**Intel® NUC**
**BIOS Settings Glossary**

The BIOS Setup program can be used to view and change the BIOS settings for the computer. BIOS Setup is accessed by pressing **F2** after the Power-On Self-Test (POST) memory test begins and before the operating system boot begins.
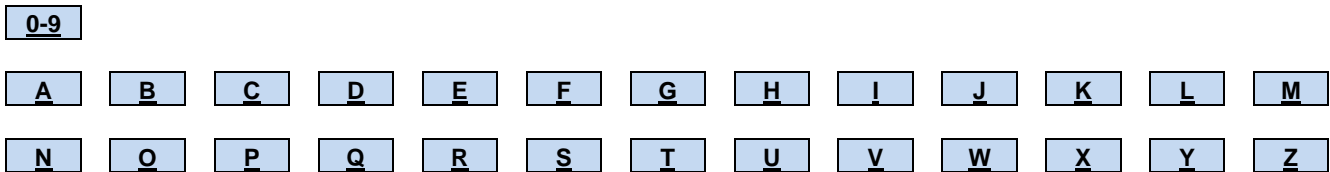
**The presence of menus and BIOS settings are dependent on your Intel NUC model, hardware components installed, and the BIOS version.**

If any problems occur (poor performance, intermittent issues) after making BIOS settings changes, reset the BIOS to default values:

1. During boot, enter the BIOS setup by pressing **F2**.
2. Press **F9** to set defaults.
3. Press **F10** to save and exit.

If the system locks or won't boot after making BIOS settings changes, perform a BIOS recovery as described at http://support.intel.com/support/motherboards/desktop/sb/CS-023360.htm.


**Find BIOS settings (Ctrl+Click)**


| 0-9 |
|-----|

| A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|

| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|

**0 – 9**

| BIOS Setting | Appears on BIOS Screen… | Options | Description / Purpose |
|---|---|---|---|
| +3.3V | Configuration > Fan Control & Real-Time Monitoring | Information only | Displays the voltage of the power supply +3.3V rail. |
| +3.3v Standby | Configuration > Fan Control & Real-Time Monitoring | Information only | Displays the voltage of the power supply +3.3V Standby rail. |
| +5v | Configuration > Fan Control & Real-Time Monitoring | Information only | Displays the voltage of the power supply +5V rail. |

**A**

| BIOS Setting | Appears on BIOS Screen… | Options | Description / Purpose |
|---|---|---|---|
| Active Processor Cores | Main | • All<br>• 1 | Allows you to select the number of cores to enable in each processor package. |
| After Power Failure | Power | • Stay Off<br>• Last State<br>• Power On | Determines the mode of operation after power is restored if a power loss occurs.<br><br>**Stay Off:** after power is restored, the system stays off until the power button is pressed.<br>**Last State:** after power is restored, the system returns to the last power state before power was lost.<br>**Power On:** after power is restored, the system automatically powers on. |
| Audio | Configuration > Onboard Devices | • Enabled<br>• Disabled | Enables or disables onboard audio. |

**B**

| BIOS Setting | Appears on BIOS Screen… | Options | Description / Purpose |
|---|---|---|---|
| BIOS Setup Auto-Entry | Boot | • Enabled<br>• Disabled | If set to Enable, the BIOS will halt and prompt to boot normally or enter Setup.  This must be set to Disable to allow OS boot without user intervention.<br><br>This feature cannot be enabled if Fast Boot USB Optimization is enabled. |
| BIOS Version | Main | Information only | Displays the version of the BIOS currently installed. |
| Blacklisted Signature Database (dbx) | Boot > Secure Boot > Secure Boot Config | Information only | Displays **Installed** or **Not Installed** based on the presence of the UEFI dbx variable. |
| Blink LEDs | Configuration > Intel x Gigabit Network Connection | Range 0 - 15 seconds | Blink LEDs for the specified duration (in seconds) |
| Boot Device Priority | Boot | • Optical Drives<br>• Removable Drive<br>• Hard Disk Drives<br>• Network | Specifies the boot sequence from the available devices. The list of options may vary depending on board model and hardware configuration. |

| Boot Drive Order | Boot | Dependent on installed bootable devices | Allows you to specify the boot sequence from the available types of boot devices.<br><br>All detected bootable devices will be included in the list. The user can change the order of devices.  The BIOS will attempt to boot to each device in the order of this list. |
|---|---|---|---|
| Boot Menu Type | Boot | • Normal<br>• Advanced | Select how the boot menu is displayed.<br>**Normal:** displays boot devices by category.<br>**Advanced:** displays individual boot devices. |
| Boot to Network | Boot | • Enabled<br>• Disabled | Enables or disables the ability to boot from network devices. |
| Boot to Optical Devices | Boot | • Enabled<br>• Disabled | Enables or disables booting from optical devices (CD/DVD). |
| Boot to Removable Devices | Boot | • Enabled<br>• Disabled | Enables or disables booting from removable devices. |
| Boot USB Devices First | Boot | • Enabled<br>• Disabled | **Enable:** the BIOS will attempt to boot to supported USB devices before any other devices.<br>**Disable:** the normal boot order will be used. |
| Burst Mode Power Limit (Watts) | Performance > Processor Overrides | Numeric | Intel Turbo Boost Technology will use this power limit for a very short duration. After that, the Sustained Mode Power Limit will be used. |

## C

| BIOS Setting | Appears on BIOS Screen… | Options | Description / Purpose |
|---|---|---|---|
| Chassis Information | Main > System Identification Information | Information only | Displays SMBIOS information for:<br>• Manufacturer<br>• Version<br>• Serial Number<br>• Asset Tag<br>• SKU Number |
| Chipset-SATA Mode | Configuration > SATA Drives | • IDE<br>• AHCI | **IDE:** Compatibility mode disables AHCI support.<br>**AHCI:** Supports advanced SATA features such as Native Command Queuing.<br><br>Warning: operating system may not boot if this setting is changed after the operating system installation. |
| Clear BIOS Passwords | Maintenance | Continue? (Y/N) | When selected, the BIOS Supervisor Password and User Password will be cleared.  The hard disk drive password, if set, will remain intact. |
| Clear Event Log | Configuration > Event Log | • Enabled<br>• Disabled | **Enable** to clear the Event Log at next boot. |
| Clear Secure Boot Data | Boot > Secure Boot > Secure Boot Config | • Enabled<br>• Disabled | Clears Secure Boot databases (Pkpub, KEK, db, and dbx) during the next boot, placing the system in Custom Mode.<br>Required to install a trusted operating system not supported by the factory default Secure Boot database. |
| Clear Trusted Platform Module | Maintenance | • No<br>• Yes | Erases all stored encryption keys and clears the TPM owner.  Used to clear the TPM if you are transferring ownership of the platform to a new owner.<br><br>*This BIOS setting is present only on systems that include support for Trusted Platform Module (TPM) and have TPM enabled.* |

**D**

| BIOS Setting | Appears on BIOS Screen… | Options | Description / Purpose |
|---|---|---|---|
| Deep S4/S5 | Power | • Enabled<br>• Disabled | Enable or disable deep S4/S5.<br><br>Enabling this setting will use less power in S4/S5 sleep states, but will only wake from S4/S5 via the power button or RTC alarm. |
| Desktop Board Information | Main > System Identification Information | Information only | Displays SMBIOS information for:<br>• Manufacturer<br>• Product Name<br>• Version<br>• Serial Number<br>• Asset Tag |
| DIMM x | Main | Information only | Displays the installed system memory size in DIMM slot x in Gigabytes. |
| Discard Changes | Exit | Continue? (Y/N) | Discards changes without exiting Setup. The option values present when the computer was turned on are used. |
| Display F10 to Enter Boot Menu | Boot > Boot Display Options | • Enabled<br>• Disabled | If enabled, BIOS will display "F10 to Enter Boot Menu" prompt. F10 key input will still be accepted if this prompt is disabled. |
| Display F12 for Network Boot | Boot > Boot Display Options | • Enabled<br>• Disabled | If enabled, BIOS will display "F12 for Network Boot" prompt. F12 key input will still be accepted if this prompt is disabled. |
| Display F2 to Enter Setup | Boot > Boot Display Options | • Enabled<br>• Disabled | If enabled, BIOS will display "F2 to Enter Setup" prompt. F2 key input will still be accepted if this prompt is disabled. |
| Display F7 to Update BIOS | Boot > Boot Display Options | • Enabled<br>• Disabled | If enabled, BIOS will display "F7 to Update BIOS" prompt. F7 key input will still be accepted if this prompt is disabled. |
| Duty cycle increment (%/°C) | Configuration > Fan Control & Real-Time Monitoring | Information only | Fan speed increases by this percentage for each degree over the minimum temperature. |

**E**

| BIOS Setting | Appears on BIOS Screen… | Options | Description / Purpose |
|---|---|---|---|
| Enhanced Intel SpeedStep® Technology | Power | • Enabled<br>• Disabled | Enable or disable Enhanced Intel SpeedStep® Technology (EIST) which allows the system to dynamically adjust processor voltage and core frequency, which can result in decreased average power consumption, decreased average heat production, and a quieter system.<br><br>For information on SpeedStep, refer to http://en.wikipedia.org/wiki/Speedstep |
| Event Logging | Configuration > Event Log | • Enabled<br>• Disabled | Enable or disable event logging. If enabled, BIOS will log POST errors in NVRAM. |

| Event Type | Configuration > Event Log | Information only | Displays list of logged events with the date and time of occurrence. |
|---|---|---|---|
| Execute Disable Bit | Security | • Enabled<br>• Disabled | Enable to implement Execute Disable Technology.<br><br>*For more information, refer to*<br>*http://en.wikipedia.org/wiki/NX_bit* |
| Exit Discarding Changes | Exit | Continue? (Y/N) | Exits BIOS setup without saving any changes made. |
| Exit Saving Changes | Exit | Continue? (Y/N) | Saves all changes and exits BIOS setup. |
| Expansion Card Text | Boot > Boot Display Options | • Disabled<br>• Enabled<br>• Hide all | **Disable**: BIOS will display text only from mass-storage PCI option ROMs during POST.<br>**Enable:** BIOS will display text from any PCI option ROMs during POST.<br>**Hide All:** BIOS will display no text from PCI option ROMs during POST. |

## F

| BIOS Setting | Appears on BIOS Screen… | Options | Description / Purpose |
|---|---|---|---|
| Failsafe Watchdog | Performance | • Enabled<br>• Disabled | Enables or disables Failsafe Watchdog.<br><br>When the failsafe watchdog is enabled, after a boot failure, the system will reboot back into BIOS Setup with the last values set by the user. |
| Fast Boot | Boot | • Enabled<br>• Disabled | Enable or disable Fast Boot features.<br><br>In order to disable Fast Boot without entering BIOS setup, power down the system for 5 seconds, then power it back on while holding the power button for 2 seconds (the system will beep). |
| Fixed Disk Boot Sector | Maintenance | • Normal<br>• Write Protect | **Write Protect** provides some Master Boot Record protection.<br>Set to **Normal** while installing an operating system.<br>Only applicable to Legacy IDE Mode. |
| Flash Update Sleep Delay | Power | • Enabled<br>• Disabled | If enabled, the system will sleep for 20 seconds during the flash update power cycle.  Enabling this feature may increase compatibility with power supplies. |
| Force Secure Boot Defaults | Boot > Secure Boot > Secure Boot Config | • Enabled<br>• Disabled | Restores factory default Secure Boot databases during the next boot, placing the system in Standard Mode. |

## G

| BIOS Setting | Appears on BIOS Screen… | Options | Description / Purpose |
|---|---|---|---|
| General Optimization | Boot | • Enabled<br>• Disabled | **Enable**: BIOS will boot faster, however the following features will be disabled: Boot to Network, Boot to Optical Devices, and Boot to Removable Devices. |
| Graphics Max Multiplier | Performance | Numeric | Selects Graphics Dynamic Frequency: Host Clock Frequency x 0.5 x Graphics Max Multiplier = Graphics Dynamic Frequency |
| Graphics Voltage Offset (mV) | Performance | Numeric | Changing this setting may allow for graphics overclocking. |

**H**

| BIOS Setting | Appears on BIOS Screen… | Options | Description / Purpose |
|---|---|---|---|
| Hard Disk Drive Password | Security | Information only | Reports if there is a hard disk drive password set. |
| Hard Disk Drive Password Prompt | Security | • Enabled<br>• Disabled | **Enable**: BIOS will always prompt for a hard disk drive password if a User HDD Password is installed.<br>**Disable**: BIOS will never prompt for a hard disk drive password unless attempting to boot to a drive with a User HDD Password installed. |
| Hard Disk Pre-Delay | Configuration > SATA Drives | 0 to 30 seconds (changeable in 5 second increments) | Delay (in seconds) before hard drives are initialized.  This can be used to increase the amount of time that the BIOS Splash Screen displays.<br><br>To increase or decrease, use the + and: keys on the keypad. |
| Hibernation Timer | Power | • Immediate<br>• 1 minute<br>• 2 minutes<br>• 5 minutes<br>• 10 minutes<br>• 15 minutes<br>• 1 hour<br>• 2 hours | When the system is put to sleep, it will temporarily wake up when the timer expires, and then hibernate to an SSD. |
| High Precision Event Timers | Configuration > Onboard Devices | • Enabled<br>• Disabled | High precision event timers are integrated into chipset hardware and are available for use by operating systems. They can be disabled if incompatible with an OS or application. |
| Host Clock Frequency | Main | Information only | Displays the default host clock frequency (in MHz) |

**I**

| BIOS Setting | Appears on BIOS Screen… | Options | Description / Purpose |
|---|---|---|---|
| IGD Current Limit (Amps) | Performance > Processor Overrides | Numeric | Integrated Graphics Dynamic Frequency will be controlled based on this current limit. |
| IGD DVMT Memory | Configuration > Video | • 128 MB<br>• 256 MB<br>• 512 MB<br>• Maximum DVMT | Dynamic Video Memory Technology (DVMT): Allows you to select the amount of system memory allocated to the integrated graphics device (IGD) video. |
| IGD Primary Video Port | Configuration > Video | • Auto<br>• HDMI<br>• HDMI 1<br>• HDMI 2<br>• Mini DisplayPort 1<br>• Mini DisplayPort 2 | Allows you to select your preference for the Integrated Graphics Device (IGD) display interface used when system boots.<br><br>**Auto:** attempts to detect connected monitors, and will display video on a maximum of two ports.<br><br>*The options available can vary, depending on system model.* |
| Install Intel Platform Key | Boot > Secure Boot > Secure Boot Config | • Enabled<br>• Disabled | Generates a new Secure Boot Platform Key during next boot. The private half of the Platform Key is discarded. |
| Intel x Gigabit Network Connection | Configuration | Opens sub-menu for LAN settings | Displays the MAC Address of the onboard LAN device in hexadecimal. |

| | | | |
|---|---|---|---|
| Intel® Anti-Theft Technology | Security | Information only | Displays the status of Intel Anti-Theft Technology<br><br>*For information on Intel® Anti-Theft Technology, refer to http://antitheft.intel.com/welcome.aspx* |
| Intel® Dynamic Power Technology | Power | • Energy Efficient Performance<br>• Off<br>• Custom | Configures processor power management features.<br><br>**Energy Efficient Performance:**<br>Sets these options:<br>• Enhanced Intel SpeedStep® Technology = Enabled<br>• OS ACPI C2 Report = Enabled<br>• OS ACPI C3 Report = Disabled<br>• PCIe ASPM Support = Enabled<br>Hides these options:<br>• Enhanced Intel SpeedStep® Technology<br>• OS ACPI C2 Report<br>• OS ACPI C3 Report<br><br>**Off:**<br>Hides these options:<br>• Enhanced Intel SpeedStep® Technology<br>• OS ACPI C2 Report<br>• OS ACPI C3 Report<br>• Enhanced Intel SpeedStep® Technology to Disable<br>• PCIe ASPM Support to Disable<br><br>**Custom:**<br>Unhides these options:<br>• Enhanced Intel SpeedStep® Technology<br>• OS ACPI C2 Report<br>• OS ACPI C3 Report |
| Intel® Graphics Performance Analyzers | Configuration > Video | • Enabled<br>• Disabled | This feature is intended only for software developers. If GPA support is enabled, hardware acceleration of Blu-ray Disc playback may be disabled. |
| Intel® Hyper-Threading Technology | Main | • Enabled<br>• Disabled | Enables or disables Hyper-Threading Technology.<br><br>When disabled, only one thread per active core will be available.<br><br>*For information on Hyper-Threading, refer to http://en.wikipedia.org/wiki/Hyperthreading* |
| Intel® Rapid Start Technology | Power | • Enabled<br>• Disabled | If enabled, the system will wake up faster. Requires a correctly configured SSD.<br><br>*For more information on Intel Rapid Start Technology, refer to http://www.intel.com/support/motherboards/desktop/sb/CS-033913.htm* |
| Intel® Smart Connect Technology | Power | • Enabled<br>• Disabled | When enabled, Intel® Smart Connect technology can be configured to periodically wake up the system briefly to retrieve data from the network (email, etc.)<br><br>*For more information on Intel Rapid Start Technology, refer to http://www.intel.com/support/motherboards/desktop/sb/CS-033913.htm* |
| Intel® Turbo Boost Technology | Performance > Processor Overrides | • Enabled<br>• Disabled | **Enable**: Allows processor cores to run faster than the base operating frequency when running below power, current, and temperature limits.<br>**Disable**: Uses Maximum Non-Turbo Ratio |

| Intel® Virtualization Technology | Security | • Enabled<br>• Disabled | Enables or disables Virtualization Technology.  Takes affect only after power cycling.<br><br>*For more information refer to*<br>*http://www.intel.com/technology/virtualization/index.htm* |
|---|---|---|---|
| Intel® VT for Directed I/O (VT-d) | Security > Intel® VT for Directed I/O (VT-d) | • Enabled<br>• Disabled | Enables or Disables Intel® VT for Directed I/O (VT-d) which provides additional hardware support for managing I/O virtualization.  If Enabled, BIOS will publish a DMA Remapping ACPI table.<br><br>*For information on Intel® VT, refer to*<br>*http://www.intel.com/technology/virtualization/index.htm* |

**J**

There currently are no BIOS settings that begin with the letter J.

**K**

| BIOS Setting | Appears on BIOS Screen… | Options | Description / Purpose |
|---|---|---|---|
| Key Exchange Key (KEK) | Boot > Secure Boot > Secure Boot Config | Information only | Displays **Installed** or **Not Installed** based on the presence of the UEFI KEK variable. |

**L**

| BIOS Setting | Appears on BIOS Screen… | Options | Description / Purpose |
|---|---|---|---|
| L2 Cache RAM | Main | Information only | Displays the total L2 cache memory of the installed processor in megabytes. |
| L3 Cache RAM | Main | Information only | Displays the total L3 cache memory of the installed processor in megabytes. |
| LAN | Configuration > Onboard Devices | • Enabled<br>• Disabled | Enables or disables the onboard LAN controller. |
| Link Speed | Configuration > Intel x Gigabit Network Connection > NIC Configuration | • AutoNeg<br>• 10 Mbps Half<br>• 10 Mbps Full<br>• 100 Mbps Half<br>• 100 Mbps Full | Changes the link speed and duplex for the LAN port. |
| Load Custom Defaults | Exit | Continue? (Y/N) | The BIOS will load Setup defaults.  If User Custom defaults are present, they are used. |
| Load Optimal Defaults | Exit | Continue? (Y/N) | The BIOS will load Setup defaults.  If OEM custom defaults are present, they are used.  This item is equivalent to the F9 BIOS Setup hotkey.  This item does not affect BIOS Passwords, HD Passwords or anything under the Intel® ME menu. |

**M**

| BIOS Setting | Appears on BIOS Screen… | Options | Description / Purpose |
|---|---|---|---|
| Master Key Hard Disk Drive Password | Security | Information only | Reports if there is a master key hard disk drive password set. |

| Maximum Non-Turbo Ratio | Performance > Processor Overrides | Numeric | Maximum Non-Turbo Processor Speed = Maximum Non-Turbo Ratio x Host Clock Frequency<br><br>This parameter along with Host Clock Frequency determines the maximum processor speed when Intel® Turbo Boost Technology is not engaged. |
|---|---|---|---|
| Memory Configuration Interface | Performance > Memory Overrides | • Basic<br>• Advanced | **Basic:** provides access to commonly modified memory parameters.<br>**Advanced:** provides access to additional memory parameters. |
| Memory Speed | Main | Information only | Displays the current memory speed. Defined as current host clock frequency x memory multiplier. |
| Memory Voltage (V) | Performance > Memory Overrides > Performance Memory Profiles | Multiple voltage values | Changing memory voltage may allow for overclocking and/or improve memory compatibility. Options include:<br>• **tCL:** CAS latency<br>• **tRCD**: RAS-to-CAS Delay<br>• **tRP**: RAS Pre-Charge<br>• **tRASmin**: Minimum RAS Active Time<br>• **tRFC:** RAS Refresh<br>• **tRRD:** RAS to RAS Delay<br>• **tWR:** Write Recovery<br>• **tWTR:** Write to Read<br>• **tRTP**: Read to Precharge Delay<br>• **tRC:** Row Cycle Delay<br>• **tFAW:** Four Active Window<br>• **tCWL**: CAS Write Latency<br>• **Command Rate** |
| Minimum Duty Cycle (%) | Configuration > Fan Control & Real-Time Monitoring | Information only | Fan speed never goes below this value. |
| Minimum Temperature (°C) | Configuration > Fan Control & Real-Time Monitoring | Information only | Fan speed increases if the processor temperature exceeds this value. The value is calculated by Tcontrol minus a fixed value. |
| Motherboard Temperature | Configuration > Fan Control & Real-Time Monitoring | Information only | Displays the current system ambient temperature. |

## N

| BIOS Setting | Appears on BIOS Screen… | Options | Description / Purpose |
|---|---|---|---|
| Native ACPI OS PCIe Support | Power | • Enabled<br>• Disabled | Enable for power savings and performance improvements. Note: not all PCIe devices are compatible with this feature. |
| Numlock | Configuration > Onboard Devices | • Enabled<br>• Disabled | If Numlock is enabled, the keypad defaults to numeric functionality. |

## O

| BIOS Setting | Appears on BIOS Screen… | Options | Description / Purpose |
|---|---|---|---|
| OS ACPI C2 Report | Power | • Enabled<br>• Disabled | Enable or disable OS ACPI C2 Report. If enabled, BIOS will report ACPI C2 State (mapped to processor C3 state). |
| OS ACPI C3 Report | Power | • Enabled<br>• Disabled | Enable or disable OS ACPI C3 Report. If enabled, BIOS will report ACPI C3 State (mapped to processor C6 state). |

| | | | |
|---|---|---|---|
| Overridden Processor Speed | Main | Information only | Displays the maximum processor speed at current settings.  Defined as current host clock frequency x maximum  non-turbo ratio. |

**P**

| BIOS Setting | Appears on BIOS Screen… | Options | Description / Purpose |
|---|---|---|---|
| PCI Latency Timer | Configuration > PCI/PCIe Add-In Slots | • 32<br>• 64<br>• 96<br>• 128<br>• 160<br>• 192<br>• 224<br>• 248 | Sets PCI Latency Timer for Bus Mastering.  Limits the time in clock cycles that a PCI device can hold the PCI bus.  Only applies to conventional PCI devices. |
| PCIe ASPM Support | Power | • Disabled<br>• Enabled<br>• PEG Only | **Disable**: ASPM support is disabled for all PCIe devices.<br>**Enable**: ASPM support is enabled for all PCIe devices.<br>**PEG Only**: ASPM is only enabled for devices installed in PCI Express Graphics (PEG) slots. |
| Performance Memory Profiles | Performance > Memory Overrides | • Automatic<br>• Manual – User Defined | Use default memory settings from DIMM SPD or manually override memory settings.<br><br>**Automatic**: BIOS configures all memory parameters automatically<br>**Manual – User Defined:** Allows user to have full control over the memory parameters |
| Platform Key (PKpub) | Boot > Secure Boot > Secure Boot Config | Information only | Displays **Installed** or **Not Installed** based on the presence of the UEFI PKpub variable. |
| Port Configuration Information | Configuration > Intel x Gigabit Network Connection | Information only | Displays information for:<br>• UEFI Driver<br>• Adapter PBA<br>• Chip Type<br>• PCI Device ID<br>• PCI Bus:Device:Function<br>• Link Status<br>• Factory MAC Address |
| POST Function Hotkeys Displayed | Boot > Boot Display Options | • Enabled<br>• Disabled | If enabled, BIOS will display function key prompts during POST.  Function key input will still be accepted even if prompts are disabled. |
| Processor Family | Main > System Identification Information | Information only | Displays the processor family, mode and stepping (including extended family/model) in hexadecimal. These are derived from the EAX register output from the CPUID instruction when EAX is set to 1. |
| Processor Idle State | Performance > Processor Overrides | • High Performance<br>• Low Power | **High Performance** forces the operating system to use the Maximum Multiplier at all times.<br>**Low Power** allows the operating system to adjust the multiplier down. |
| Processor Power Efficiency Policy | Power | • High Performance<br>• Balanced<br>• Low Power | Configures processor bias for power efficiency vs. performance.<br><br>**High Performance**: Set MSR 1B0h Bits 3:0 to 0h<br>**Balanced**: Set MSR 1B0h Bits 3:0 to 5h<br>**Low Power:** Set MSR 1B0h Bits 3:0 to 7h |
| Processor Signature | Main > System Identification Information | Information only | Displays the 32-bit processor signature in hexadecimal; copied from EAX register output from the CPUID instruction when EAX is set to 1. |

| Processor Temperature | Configuration > Fan Control & Real-Time Monitoring | Information only | Displays the current processor temperature. |
|---|---|---|---|
| Processor Type | Main | Information only | Displays the processor brand string obtained from the CPUID instruction. |
| Processor Vcc | Configuration > Fan Control & Real-Time Monitoring | Information only | Displays the voltage of the processor Vcc. |

## Q

There currently are no BIOS settings that begin with the letter Q.

## R

| BIOS Setting | Appears on BIOS Screen… | Options | Description / Purpose |
|---|---|---|---|
| Reset Intel® AMT to default factory settings | Maintenance | Continue? (Y/N) | Resets all Intel® AMT configuration settings to their factory defaults. When selected, the BIOS will unprovision AMT and load default Intel® ME settings. |

## S

| BIOS Setting | Appears on BIOS Screen… | Options | Description / Purpose |
|---|---|---|---|
| S3 State Indicator | Power | • Off<br>• Blink<br>• On<br>• Alternate Color | Determines front panel power LED behavior during S3 system power state. |
| Save Custom Defaults | Exit | Continue? (Y/N) | The BIOS will save the existing Setup configuration as a User Custom default. |
| Secure Boot | Boot > Secure Boot > Secure Boot Config | • Enabled<br>• Disabled | If enabled, BIOS will only boot to trusted operating system images.  Secure Boot is supported only via UEFI Boot.<br><br>When UEFI Secure Boot is enabled, attempts to boot non-UEFI OS will fail. |
| Secure Boot Mode | Boot > Secure Boot > Secure Boot Config | Information only | Displays the Secure Boot Mode based on the SecureBootCustomMode Boolean UEFI variable.<br><br>Displays **Standard** if the value is false.<br>Displays **Custom** if the value is true. |
| Set Hard Disk Drive Password | Security | User defined | Sets the Hard Disk Drive password<br><br>If a HDD Password is created, it must be entered each boot before operating system access. HDD Passwords are not recoverable and cannot be removed without the original password. The drive will remain inaccessible unless the HDD or Master Key HDD password is entered. |
| Set Master Key Hard Disk Drive Password | Security | User defined | Sets the Master Key Hard Disk Drive password<br><br>The Master Key HDD password is only used to unlock a drive if the HDD password is forgotten.  It does not lock a drive by itself. HDD Passwords are not recoverable and cannot be removed without the original password. The drive will remain inaccessible unless the HDD or Master Key HDD password is entered. |

| Set Supervisor Password | Security | User defined | Sets the Supervisor password.<br><br>The supervisor password gives unrestricted access to view and change all Setup options. If only the supervisor password is set, pressing <Enter> at the password prompt of Setup gives the user restricted access to Setup. If both the supervisor and user passwords are set, you must enter either the supervisor password or the user password to access Setup. Setup options are then available for viewing and changing depending on whether the supervisor or user password was entered. |
|---|---|---|---|
| Set User Password | Security | User defined | Sets the User password.<br><br>Setting a user password restricts who can boot the computer. The password prompt is displayed before the computer is booted. If only the supervisor password is set, the computer boots without asking for a password. If both passwords are set, you can enter either password to boot the computer. |
| Signature Database (db) | Boot > Secure Boot > Secure Boot Config | Information only | Displays **Installed** or **Not Installed** based on the presence of the UEFI db variable. |
| Supervisor Password | Security | Information only | Reports if there is a supervisor password set. |
| Suspend | Security | • Enabled<br>• Disabled | Suspend Intel® Anti-Theft Technology starting on the next boot. |
| Sustained Mode Power Limit (Watts) | Performance > Processor Overrides | Numeric | Intel Turbo Boost Technology will control processor power usage to the Sustained Mode Power Limit over a moving average time window. |
| Sustained Mode Time (Seconds) | Performance > Processor Overrides | 1 - 32 seconds | Intel Turbo Boost Technology will control processor power usage to the Sustained Mode Power Limit over a moving average time window. |
| System Date | Main | Month, day, year | Displays and changes the System Date from the Real-Time Clock.<br><br>The RTC Date is displayed in the format [MM/DD/YYYY]. Each field is selectable with the Tab key.  The + and – keys are used to increment/decrement the selected field. When changed, values are immediately committed to the RTC instead of waiting for Save & Exit Setup/F10 key. The default date is only loaded when the RTC reports an invalid date, or a battery or CMOS checksum failure.  The default date is not loaded when other Setup defaults are loaded (F9 key, etc.) |
| System Fan Control | Configuration > Fan Control & Real-Time Monitoring | • Fixed<br>• Custom<br>• Cool<br>• Blended<br>• Quiet | **Fixed:** the System Fan Speed will be fixed.<br>**Custom:**  Allows you to manually set temperature and duty cycle options.<br>**Cool:** Preloads specific settings for cool operation.<br>**Blended:** Preloads specific settings to blend cool and quiet operation.<br>**Quiet:** Preloads specific settings for quiet operation. |
| System Fan Speed | Configuration > Fan Control & Real-Time Monitoring | Information only | Displays the current processor fan speed. |

| System Information | Main > System Identification Information | Information only | Displays SMBIOS information for:<br>• Manufacturer<br>• Product Name<br>• Version<br>• Serial Number<br>• UUID<br>• SKU Number<br>• Family |
|---|---|---|---|
| System Time | Main | Hours, minutes, seconds | Displays and changes the System Time from the Real-Time Clock.<br><br>The RTC Time is displayed in the 24-hour format [HH:MM:SS]. Each field is selectable with the Tab key. The + and – keys are used to increment/decrement the selected field. When changed, values are immediately committed to the RTC instead of waiting for Save & Exit Setup/F10 key. The default time is only loaded when the RTC reports an invalid time, or a battery or CMOS checksum failure. The default time is not loaded when other Setup defaults are loaded (F9 key, etc.) |

## T

| BIOS Setting | Appears on BIOS Screen… | Options | Description / Purpose |
|---|---|---|---|
| TDC Current Limit Override (Amps) | Performance > Processor Overrides | Numeric | Intel Turbo Boost Technology will be disengaged if the processor is operating beyond this current limit. |
| Thunderbolt™ Controller | Configuration > Onboard Devices | • Enabled<br>• Disabled | Enables or disables the onboard Thunderbolt™ Controller.<br><br>*This BIOS setting is present only on systems that include Thunderbolt.* |
| Total Memory | Main | Information only | Displays the total installed system memory size in gigabytes. |
| Trusted Platform Module Presence | Configuration > Onboard Devices | • Enabled<br>• Disabled | Controls the exposure of the onboard Trusted Platform Module (TPM) device to the operating system. |
| Trusted Platform Module | Configuration > Onboard Devices | • Enabled<br>• Disabled | Enables or disables Trusted Platform Module (TPM).<br><br>*This BIOS setting is present only on systems that include support for Trusted Platform Module (TPM).*<br><br>*For information on TPM, refer to http://en.wikipedia.org/wiki/Trusted_Platform_Module* |

## U

| BIOS Setting | Appears on BIOS Screen… | Options | Description / Purpose |
|---|---|---|---|
| UEFI Boot | Boot | • Enabled<br>• Disabled | Enables or disables Unified Extended Firmware Interface (UEFI) Boot. UEFI Boot must be enabled in order to boot to a drive larger than 2 TB (terabytes).<br><br>**Enable**: BIOS will attempt to boot via UEFI before using the legacy boot sequence.<br>**Disable**: BIOS will use the legacy boot sequence.<br><br>*For information on UEFI, refer to http://www.uefi.org/home* |

| | | | |
|---|---|---|---|
| Unattended BIOS Configuration | Security | • Always Prompt<br>• Lock<br>• Temporarily Skip Prompt<br>• Never Prompt | Configuring the BIOS via Intel® Integrator Toolkit normally requires physical presence via a keyboard response prompt. This prompt can be disabled temporarily or permanently, or unattended BIOS configuration can be locked out entirely. |
| USB Boot | Boot | • Enabled<br>• Disabled | Enables or disables booting from USB boot devices. |
| USB Legacy | Configuration > Onboard Devices > USB | • Enabled<br>• Disabled | Enables or disables USB Legacy support.<br><br>USB Legacy allows USB support under non-USB-aware operating systems.  Disabling USB Legacy will not disable USB keyboards during BIOS POST, including BIOS SETUP and Option ROMs. |
| USB Optimization | Boot | • Enabled<br>• Disabled | **Enable**: all USB devices will be unavailable until after the operating system boots, but BIOS will boot faster.<br>**Disable**: USB devices will be available before the operating system boots, but BIOS will boot slower.<br><br>This feature cannot be enabled while a User Password or Hard Drive Password is installed. |
| USB Port x | Configuration > Onboard Devices > USB | • Enabled<br>• Disabled<br>• No Detect | Allows you to enable or disable individual USB ports.<br><br>If a USB keyboard is attached to a USB port that has been disabled in BIOS, it will be enabled during POST and Setup, but will be disabled before the operating system boot.<br><br>All non-keyboard devices will be disabled during POST, Setup and in the operating system.  This means that drives attached to disabled USB ports will not appear in the BIOS boot order in Setup.<br><br>**No Detect**: skips the USB device detection on selected ports during POST.  The operating system is still able to detect and use all USB devices plugged into the system. This gives the advantage of a faster boot while still having all USB devices available in the operating system. |
| User access Level | Security | • Full<br>• Limited<br>• View Only<br>• No Access | User Access Level determines the level of BIOS Setup access granted when the User Password is entered.<br><br>**Full:** User Password grants access to all questions except User Access Level.<br>**Limited:** User Password grants access to Time/Date/Language/User Password questions.<br>**View Only:** User Password grants access only to Language question and changes cannot be saved.<br>**No Access:** User Password cannot be used to access Setup.<br><br>*This BIOS setting is present only if a supervisor password has been set.* |
| User Password | Security | Information only | Reports if there is a user password set. |

**V**

| BIOS Setting | Appears on BIOS Screen… | Options | Description / Purpose |
|---|---|---|---|
| Video Optimization | Boot | • Enabled<br>• Disabled | **Enable**: BIOS will display text only but will boot faster.<br>**Disable**: BIOS will display the logo but will boot slower.<br><br>This feature does not affect video capabilities after the operating system boots. |

**W**

| BIOS Setting | Appears on BIOS Screen… | Options | Description / Purpose |
|---|---|---|---|
| Wake on LAN | Configuration > Intel x Gigabit Network Connection > NIC Configuration | • Enabled<br>• Disabled | Enable this option to wake the system with a magic packet. |
| Wake on LAN from S4/S5 | Power | • Stay off<br>• Power On – Normal Boot<br>• Power On – PXE Boot | Configures behavior when a Wake on LAN packet is received during S4/S5.<br><br>**Stay off**: the system will not wake from S4/S5 power state when a Wake on LAN packet is received.<br>**Power On-Normal Boot**: the system will wake from S4/S5 power state when a Wake on LAN packet is received and will follow normal boot order.<br>**Power On-PXE Boot:** the system will wake from S4/S5 power state when a Wake on LAN packet is received and will attempt boot to PXE.<br><br>Wake on LAN must also be enabled in the operating system LAN driver and is disabled if Deep S4/S5 is enabled. |
| Wake system from S5 | Power | • Enabled<br>• Disabled | Enable or disable system wake on alarm event. When enabled, system will wake on the day/hour/minute/second specified. |
| Wakeup Date | Power | Numeric range 0: 31 | Select day of each month to wake the system. Select 0 for daily wakeup. |
| Wakeup Hour | Power | Numeric range 0: 23 | Select wakeup hour in 24-hour format. For example, 15 means 3 PM. |
| Wakeup Minute | Power | Numeric range 0: 59 | Select wakeup minute. |
| Wakeup Second | Power | Numeric range 0: 59 | Select wakeup second. |

**X**

There currently are no BIOS settings that begin with the letter X.

**Y**

There currently are no BIOS settings that begin with the letter Y.

**Z**

There currently are no BIOS settings that begin with the letter Z.