Intel® Desktop Boards
BIOS Settings Dictionary – By Menu

The BIOS Setup program can be used to view and change the BIOS settings for the computer. The BIOS Setup program is accessed by pressing the <F2> key after the Power-On Self-Test (POST) memory test begins and before the operating system boot begins. The following menus are available:

Menu Title	Purpose
Maintenance	Clears passwords and displays processor information. *The maintenance menu is displayed only when the Desktop Board is in Configure Mode.*
Main	Displays processor and memory configuration.
Configuration	Configures advanced features available through the chipset.
Performance	Allows for advanced configuration of CPU, memory and bus settings.
Security	Sets passwords and security features.
Power	Configures power management features and power supply controls.
Boot	Selects boot options.
Intel® ME	Configures options for the Intel® Management Engine and Intel® Active (or Standard) Management Technology.
Exit	Saves or discards changes to Setup program options.

The presence of menus and BIOS settings are dependent on your board model, hardware components installed, and the BIOS version. BIOS menu titles may differ.

If any problems occur after making BIOS settings changes (poor performance, intermittent issues, etc.), reset the desktop board 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.

Boot

BIOS Setting	Options	Description / Purpose
Boot Device Priority	• Removable Devices • Optical Drive • Hard Disk Drive • Ethernet	Specifies the boot sequence from the available devices. The list of options may vary depending on board model and hardware configuration.
Boot Drive Order	Dependent on installed bootable devices	Allows you to specify the boot sequence from the available types of boot devices. 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	• Normal • Advanced	**Normal:** allows you to set boot priority based on type of device. **Advanced:** allows you to set boot priority for each device regardless of category
Boot to Network	• Enable • Disable	Enables or disables booting from the network (PXE).
Boot to Optical Devices	• Enable • Disable	Enables or disables booting from optical devices (CD/DVD).
Boot to Removable Devices	• Enable • Disable	Enables or disables booting from removable devices.
Boot USB Devices First	• Enable • Disable	**Enable:** the BIOS will attempt to boot to supported USB devices before any other devices. **Disable:** the normal boot order will be used.
Hard Drive Order	Lists all installed hard drive devices	Allows you to set the boot order of hard drives (used when Boot Menu type is set to normal) All detected hard drives will be included in the list. You can change the order of devices. When attempting to boot to hard drives, the BIOS will attempt to boot to each device in the order of this list.
Optical Drive Order	Lists all installed optical drive devices (CD/DVD)	Select the boot order for optical drives. All detected optical devices will be included in the list. The user can change the order of devices. When attempting to boot to optical drives, the BIOS will attempt to boot to each device in the order of this list.
Removable Drive Order	Lists all installed removable devices	Allows you to set the boot order of removable devices (floppy drives, USB thumb drives, etc) - used when Boot Menu type is set to normal. All detected removable devices will be included in the list. The user can change the order of devices. When attempting to boot to removable drives, the BIOS will attempt to boot to each device in the order of this list.

UEFI boot	• Enable • Disable	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). **Enable**: BIOS will attempt to boot via UEFI before using the legacy boot sequence. **Disable**: BIOS will use the legacy boot sequence. *For information on UEFI, refer to http://www.uefi.org/home*
USB Boot	• Enable • Disable	Enables or disables booting from USB boot devices.

Boot > Boot Display Options

BIOS Setting	Options	Description / Purpose
Display F10 to Enter Boot Menu	• Enable • Disable	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	• Enable • Disable	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	• Enable • Disable	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	• Enable • Disable	If enabled, BIOS will display “F7 to Update BIOS” prompt. F7 key input will still be accepted if this prompt is disabled.
Display F9 for Remote Assistance	• Enable • Disable	If set to Enable, BIOS will display “F9 for Remote Assistance” prompt. F9 key input will still be accepted if this prompt is disabled. *This BIOS setting is present only when the board supports Remote Assistance.*
Expansion Card Text	• Disable • Enable • Hide all	**Disable**: BIOS will display text only from mass-storage PCI option ROMs during POST. **Enable:** BIOS will display text from any PCI option ROMs during POST. **Hide All:** BIOS will display no text from PCI option ROMs during POST.
POST Code Routing	• Onboard • PCI	Routing for Ports 80h, 84-86h, 88h, 8C-8Eh. **Onboard:** sends BIOS POST codes to the onboard POST code LED display **PCI:** sends BIOS POST codes to the PCI bus (POST card in PCI slot)
POST Function Hotkeys Displayed	• Enable • Disable	If enabled, BIOS will display function key prompts during POST. Function key input will still be accepted even if prompts are disabled.

Configuration > Event Log

BIOS Setting	Options	Description / Purpose
Clear Event Log	• Disable • Enable or • Yes • No	**Enable (Yes)** discards all events in the event log and will reset the option to **Disable (No)** upon exiting BIOS.
Event Logging	• Enable • Disable	Enable or disable event logging. If enabled, BIOS will log POST errors in NVRAM.

Configuration > Fan Control & Real-Time Monitoring

BIOS Setting	Options	Description / Purpose
All-On Temperature	Numeric	Defines temperature that the fan control subsystem takes fan(s) to full speed.
Control Mode	• Minimum • Off • Manual	Select how the fan connected to this header is to be controlled. **Minimum**: sets a minimum duty cycle that the fan will never go below. **Off:** sets the duty cycle to 0. **Manual**: specifies an exact duty cycle.
Control Temperature	Numeric	Defines temperature that the fan control subsystem attempts to maintain for this device.
Current Duty Cycle	Information only	Displays the current fan duty cycle.
Current Fan Speed	Information only	Displays the current fan speed.
Current Reading	Information only	For temperature sensors: Displays the current temperature. For voltage sensors: Displays the current voltage.
Damping	• Low • Normal • High	Helps to reduce oscillation in fan speed response. Higher settings will produce fewer changes, but could slow temperature response.
Fan Type	Information only	Displays the detected fan type.

Fan Usage	• Unknown • CPU • System • MCH • VREG • Chassis • Inlet • Outlet • PSU • PSU In • PSU Out • HDD • Video • Aux • IOH • PCH • Memory	Select how the fan connected to this header is to be used.
Maximum Duty Cycle	Numeric	Selects the maximum duty cycle that the fan will never go above during normal usage.
Minimum Duty Cycle	Numeric	Selects the minimum duty cycle that the fan will never go below.
Over-Temperature Threshold	Numeric	Defines the temperature at or above which run-time applications can generate an alert.
Over-Voltage Threshold	User Defined	Defines the voltage at or above which run-time applications can generate an alert.
Responsiveness	• Slow • Normal • Aggressive	Defines how quickly fan speed changes based upon changes in temperature.
Restore Default Configuration	Continue? (Y/N)	When this question is selected, the BIOS Fan Control configuration is erased and defaults are loaded. This does not affect any other BIOS Setup questions.
Under-Speed Threshold	Numeric	Sets a threshold to allow an alert to be generated if speed in RPM goes below the set value. A monitoring utility is required to see this alert.
Under-Voltage Threshold	User Defined	Defines the voltage at or below which run-time applications can generate an alert.

Configuration > On-Board Devices

BIOS Setting	Options	Description / Purpose
1394	• Enable • Disable	Enables or disables IEEE 1394 support *This BIOS setting is present only on Intel® Desktop Boards that include IEEE 1394.* *For information on IEEE 1394, refer to http://en.wikipedia.org/wiki/IEEE_1394*
Audio	• Enable • Disable	Enables or disables onboard audio.

Bluetooth Wireless	• Enable • Disable	Enables or disables the on-board bluetooth wireless controller. *This BIOS setting is present only on Intel® Desktop Boards that include Bluetooth.*
Enhanced Consumer IR	• Enable • Disable	Enables or disables consumer infrared communication feature.
Floppy Controller	• Automatic • Enable • Disable	Configures the floppy drive controller. Only 1.44MB floppy drives are supported. **Automatic:** enables the onboard floppy controller if a floppy drive is connected.
Internal LED Brightness Level	• Off • Low • Med • High	Sets the brightness level for the board's power switch. *This BIOS setting is present only on certain Extreme Series Intel® Desktop Boards.*
LAN	• Enable • Disable	Enables or disables the on-board LAN controller.
Numlock	• Off • On	If Numlock is on, the keypad defaults to numeric functionality.
Parallel Port	• Enable • Disable	Enables or disables the parallel port.
PCI Latency Timer	• 32 • 64 • 96 • 128 • 160 • 192 • 224 • 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 Legacy PCI devices.
Secondary LAN	• Enable • Disable	Enables or disables the onboard secondary LAN controller.
Serial Port	• Enable • Disable	Enables or disables the serial port.
Serial Port 2	• Enable • Disable	Enables or disables the second serial port. *This BIOS setting is present only on Intel® Desktop Boards that include two serial ports.*
Skull Backlighting	• Enable • Disable	Enable or disable backlighting on the onboard skull. *This BIOS setting is present only on certain Extreme Series Intel® Desktop Boards.*
Trusted Platform Module	• Enable • Disable	Enables or disables Trusted Platform Module (TPM). *This BIOS setting is present only on Intel® Desktop Boards that include support for Trusted Platform Module (TPM).* *For information on TPM, refer to http://en.wikipedia.org/wiki/Trusted_Platform_Module*

Configuration > On-Board Devices > Audio

BIOS Setting	Options	Description / Purpose
Front Panel Audio	• Auto • High Definition Front Panel • Legacy Front Panel • Disable	Automatically or manually select the type of audio front panel installed. **Auto**: attempts to detect the presence and type of Audio Front Panel installed **High Definition Front Panel**: configures Front Panel Audio in High Definition Mode **Legacy Front Panel**: configures Front Panel Audio in Legacy Mode **Disable**: disables Front Panel Audio
HDMI/Display Port Audio	• Enable • Disable	**Enable:** HDMI/Display port output includes both audio and video. **Disable:** HDMI/DisplayPort output is video only.

Configuration > On-Board Devices > Parallel Port

BIOS Setting	Options	Description / Purpose
Mode	• Output only • Bi-directional • EPP • ECP	Allows you to select the mode for the parallel port. This option is available only when the parallel port is enabled. **Output Only:** operates in AT*-compatible mode. **Bi-directional:** operates in PS/2-compatible mode. **EPP:** Enhanced Parallel Port mode, a high-speed bi-directional mode for non-printer peripherals. **ECP:** Enhanced Capability Port mode, a high-speed bi-directional mode for printers and scanners.

Configuration > On-Board Devices > Skull Backlighting

BIOS Setting	Options	Description / Purpose
Skull Eye Hard Drive Activity	• Enable • Disable	Sets the skull's eyes to light up matching hard drive activity. *This BIOS setting is present only on certain Extreme Series Intel® Desktop Boards.*

Configuration > On-Board Devices > USB

BIOS Setting	Options	Description / Purpose
USB 3.0 Controller	• Enable • Disable	Enables or disables all USB 3.0 ports and the USB 3.0 controller. USB 3.0 ports are colored blue on the back panel and are designated as USB* in the illustration.
USB Legacy	• Enable • Disable	Enables or disables USB Legacy support. 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 Port x	• Enable • Disable	Allows you to enable or disable individual USB ports. 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. 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.

Configuration > PCI/PCIe Add-In Slots

BIOS Setting	Options	Description / Purpose
FLR Capability	• Enable • Disable	Enables or disables Function Level Reset (FLR), allowing PCH devices to be reset individually.
PCI/PCIe Slot Information	Information only	For each slot on the motherboard, a line is displayed that lists: • Slot Number (must match board silkscreen) • Slot Type (PCI or PCIe) • PCIe Slot Electrical Width • PCIe Slot Negotiated Width • Data Transfer Speed

Configuration > SATA Drives

BIOS Setting	Options	Description / Purpose
Chipset-SATA Mode	• IDE • RAID • AHCI	**IDE:** Compatibility mode disables AHCI support. **AHCI:** Supports advanced SATA features such as Native Command Queuing. **RAID:** Allows multiple drives to be merged into larger volumes for increased performance and/or reliability. Always enables AHCI. Warning: operating system may not boot if this setting is changed after the operating system installation.
Detected Discrete-SATA Device	Information only	Displays the device identification string, capacity in gigabytes, and negotiated speed (1.5 Gb/s, 3.0 Gb/s, or 6.0 Gb/s) for a device attached to a discrete SATA port.
Detected SATA Drive	Information only	Displays the device identification string, capacity in gigabytes, and negotiated speed (1.5 Gb/s, 3.0 Gb/s, or 6.0 Gb/s) for a device attached to a SATA port.
Discrete SATA	• Enable • Disable	Enables or disables the Discrete SATA Controller. Additional help text within the BIOS screen will be board-specific.

Discrete SATA Mode	• IDE • RAID	**IDE:** Compatibility mode disables RAID support. **RAID**: Allows multiple drives to be merged into larger volumes for increased performance and/or reliability. **Warning**: operating system may not boot if this setting is changed after the operating system installation.
eSATA Ports	• Enable • Disable	Enable or disable the external SATA (eSATA) ports. *For information on eSATA, refer to http://en.wikipedia.org/wiki/Esata#External_SATA*
Hard Disk Pre-Delay	• Disable • 3 Seconds • 6 Seconds • 9 Seconds • 12 Seconds • 15 Seconds • 21 Seconds • 30 Seconds	Delay (in seconds) before hard drives are initialized. This can be used to increase the amount of time that the BIOS Splash Screen displays. Time options available may vary by board.
No SATA Devices Detected	Information only	This appears when Discrete-SATA is enabled, but no devices are detected on a Discrete-SATA port.
S.M.A.R.T.	• Auto • Disable • Enable	Enable or disable support for the hard disk's S.M.A.R.T. (Self Monitoring Analysis And Reporting Technology) capability. S.M.A.R.T. is supported by all current hard disks and allows the early prediction and warning of impending hard disk failures. You should enable it if you want to use S.M.A.R.T.-aware utilities to monitor the hard disk's condition. *For information on S.M.A.R.T., refer to http://en.wikipedia.org/wiki/Self-Monitoring,_Analysis,_and_Reporting_Technology*
SATA Port x	Information only	Displays the device identification string, capacity in gigabytes, and negotiated speed (1.5 Gb/s, 3.0 Gb/s, or 6.0 Gb/s) for the device attached to the SATA port. If no device is attached, the string [Not Installed] is displayed.

Configuration > Video

BIOS Setting	Options	Description / Purpose
Detected Video Device Priority	Detected video devices are listed	When the Primary Video Adaptor is set to Manual, each detected video device is listed here and you can select the order of preference for the video device used during boot.

IGD DVMT Memory	• 32 MB • 64 MB • 128 MB • 256 MB • Maximum DVMT	Dynamic Video Memory Technology (DVMT) - Allows you to select the amount of system memory allocated to the integrated graphics device (IGD) video. Intel Dynamic Video Memory Technology 3.0 (DVMT 3.0) allows additional memory to be allocated for graphics usage based on application need. Once the application is closed, the memory that was allocated for graphics usage is then released and made available for system use. The options available may vary by board. *For information on DVMT, refer to the Intel® Graphics Media Accelerator 900 White Paper at http://www.intel.com/design/chipsets/applnots/30262403.pdf*
IGD Primary Video Port	• Auto • VGA Analog • DVI-I (Blue) • Analog DVI-I (Blue) • Digital DVI-D (White) • HDMI • LVDS • DisplayPort	Allows you to select your preference for the Integrated Graphics Device (IGD) display interface used when system boots. **Auto:** attempts to detect connected monitors, and will display video on a maximum of two ports.
IGD Secondary Video Port	• None • VGA Analog • DVI-I (Blue) • Analog DVI-I (Blue) • Digital DVI-D (White) • HDMI • LVDS • DisplayPort	Allows you to select your preference for the mirrored Integrated Graphics Device (IGD) display interface used when system boots.
Integrated Graphics Device	• Enable if Primary • Always Enable • Always Disable	**Enable if Primary**: Integrated Graphics Device (IGD) is disabled if not selected as the Primary Video Adaptor **Always Enable**: IGD is always enabled, even if not selected as the Primary Video Adaptor. **Always Disable**: IGD is always disabled, even if there are no other video devices installed.
No Video Detected Error Beeps	• Enable • Disable	Enable or disable motherboard speaker beeps when video is not detected.
PAVP	• Lite • Disable	Protected Audio-Video Path (PAVP) protects content when using hardware-accelerated audio/video decoding. It requires a processor/chipset that supports PAVP. This BIOS setup item is not displayed in BIOS Setup and is only accessible via the Intel® Integrator Toolkit (ITK).

Primary Video Adapter	• Auto • Int Graphics (IGD) • Ext PCIe Graphics (PEG) • Ext PCI Graphics • Manual	Allows selecting a specific video controller as the display device that will be active when the system boots. Options may vary depending on your configuration.

Configuration > Video > LVDS Settings

BIOS Setting	Options	Description / Purpose
Maintain Aspect Ratio	• Yes • No	Allows you to select the Aspect Ratio before the graphics driver initialization. **Yes:** Native Ratio **No:** Full Screen *This BIOS setting is present only on Intel® Desktop Boards that support LVDS.*
Screen Brightness	• Enable • Disable	Enable or disable setting the amount of panel backlight illumination. *This BIOS setting is present only on Intel® Desktop Boards that support LVDS.*

Exit

BIOS Setting	Options	Description / Purpose
Discard Changes	Continue? (Y/N)	Discards changes without exiting Setup. The option values present when the computer was turned on are used.
Exit Discarding Changes	Continue? (Y/N)	Exits BIOS setup without saving any changes made.
Exit Saving Changes	Continue? (Y/N)	Saves all changes and exits BIOS setup.
Load Custom Defaults	Continue? (Y/N)	The BIOS will load Setup defaults. If User Custom defaults are present, they are used.
Load Optimal Defaults	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.
Save Custom Defaults	Continue? (Y/N)	The BIOS will save the existing Setup configuration as a User Custom default.

Intel® ME

BIOS Setting	Options	Description / Purpose
Change Intel® Management Engine Password	User defined	Intel® ME password must be changed from the default password prior to gaining access to other ME options. The system owner should document the new Intel ME password, store it in a secured location (a vault, safe deposit box, or off-site storage), and have it available for future use. This document should be updated after any password change is made.
Enter Intel® Management Engine Password	User input	Intel® ME password must be entered prior to gaining access to other options on the Intel® ME page.

Intel® ME > Intel® Active (or Standard) Management Technology Configuration

BIOS Setting	Options	Description / Purpose
Partial Intel® AMT Reset	Continue? (Y/N)	Resets all Intel® AMT configuration settings to their factory defaults except Intel® ME password, PSKs (PID/PPS), domain name, and host name.
Set PRTC	User defined	Sets the Intel® AMT PRTC (Protected Real Time Clock). Enter PRTC in Greenwich Mean Time (GMT) format: YYYY:MM:DD:HH:MM:SS
Setup and Configuration Mode	• Local • Remote	**Local:** AMT configuration is performed without communicating with a server **Remote**: AMT configuration is performed by communicating with a server

Intel® ME > Intel® Active (or Standard) Management Technology Configuration > KVM Configuration

BIOS Setting	Options	Description / Purpose
Enable KVM	• Enable • Disable	**Enable**: allows Keyboard-Video-Mouse redirection over IP. Video is redirected from local client to remote console. Keyboard and Mouse are redirected from remote console to local client. **Disable**: does not allow KVM functionality.
Remote Control of Opt-in Policy	• Enable • Disable	**Enable**: allows a remote user to set the User Opt-in policy. **Disable:** prevents a remote user from setting the User Opt-in policy.
User Consent for Opt-in Session	• Required • Not Required	**Required**: local user consent is required for remote establishment of KVM session. **Not Required:** allows remote establishment without local user consent.

Intel® ME > Intel® Active (or Standard) Management Technology Configuration > Local Setup and Configuration

BIOS Setting	Options	Description / Purpose
Computer Name	User defined	Sets the computer name.
Domain Name	User defined	Sets the domain name (name of the network the computer is connected to).
Dynamic DNS TTL	Numeric	When Dynamic DNS Update is enabled, this sets the DDNS (Dynamic DNS) Time-To-Live value. If set to zero, the value will be the internal default of 15 minutes or 1/3 DHCP lease time.
Dynamic DNS Update	• Enable • Disable	**Enable:** Intel® ME attempts to register its IP address and FQDN in DNS (Domain Name System) using the Dynamic DNS Update protocol. **Disable:** Intel® ME will make no attempt to update DNS. IPv6 requires dedicated FQDN for DDNS (Dynamic DNS).
Periodic Update Interval	Numeric	When Dynamic DNS Update is enabled, this sets the interval at which DDNS (Dynamic DNS) updates will be sent
Shared/Dedicated FQDN	• Shared • Dedicated	**Shared:** Intel® ME shares FQDN (Fully Qualified Domain Name) with the Host Operating System **Dedicated:** FQDN is dedicated to the Intel® ME.

Intel® ME > Intel® Active (or Standard) Management Technology Configuration > Local Setup and Configuration > IPv4 TCP/IP Configuration

BIOS Setting	Options	Description / Purpose
Alternate DNS Address	User defined	Enter address in dot-decimal notation (for example: 255.255.255.0)
Default Gateway Address	User defined	Enter address in dot-decimal notation (for example: 255.255.255.0)
DHCP	• Enable • Disable	Enables or disables DHCP (Dynamic Host Configuration Protocol) for Intel® ME.

IPv4 Address	User defined	Enter address in dot-decimal notation (for example: 192.168.0.10). If DHCP is disabled then the IP address should be different from the Host Operating System IP address.
Preferred DNS Address	User defined	Enter address in dot-decimal notation (for example: 255.255.255.0)
Subnet Mask	User defined	Enter address mask in dot-decimal notation (for example: 255.255.255.0)

Intel® ME > Intel® Active (or Standard) Management Technology Configuration > Local Setup and Configuration > IPv6 TCP/IP Configuration

BIOS Setting	Options	Description / Purpose
Alternate DNS IPv6 Address	User defined	Enter valid address (for example: 1122:3344:5566:7788:99AA:BBCC:DDEE:FF00)
Enable IPv6	• Enable • Disable	**Enable:** Intel® ME IPv6 addresses are dedicated and not shared with the Host Operating System. **Disable:** Intel ® ME IPv6 addresses are shared with the host operating system.
IPv6 Address	User defined	Enter valid address (for example: 1122:3344:5566:7788:99AA:BBCC:DDEE:FF00)
IPv6 Default Router	User defined	Enter valid address (for example: 1122:3344:5566:7788:99AA:BBCC:DDEE:FF00)
IPv6 Interface ID	• Random ID • Intel ID • Manual ID	**Random ID**: the ID is randomly generated. **Intel ID**: the ID is generated using the MAC address. **Manual ID**: allows you to enter 64-bit valid value.
IPv6 Manual Interface ID	User defined	If IPv6 Interface ID is set to Manual ID, allows you to enter valid 64-bit value (for example: 1122:3344:5566:7788).

Preferred DNS IPv6 Address	User defined	Enter valid address (for example: 1122:3344:5566:7788:99AA:BBCC:DDEE:FF00)

Intel® ME > Intel® Active (or Standard) Management Technology Configuration > Remote Setup and Configuration

BIOS Setting	Options	Description / Purpose
Delete TLS Pre-Shared Key (PSK) PID/PPS	Continue? (Y/N)	Deletes TLS Pre-Shared Key (PSK) PID/PPS so they can be reprogrammed.
Fully Qualified Domain Name (FQDN)	User defined	The fully qualified domain name (FQDN) for a specific provisioning server. The FQDN must contain both a hostname and a domain name.
PKI DNS Suffix	User defined	Domain Name System Suffix for PKI (Public Key Infrastructure). This value is used to validate the FQDN in the provisioning server's certificate (for example: name.com).
Provisioning Mode	Information only	Displays the current Provisioning Mode: either **PKI** or **PSK**.
Provisioning Server Address IPv4/IPv6	User defined	Enter IP address in dot-decimal notation. For example, 192.168.0.10
Provisioning Server Mode	• OTC uses TLS-PSK • Remote Configuration uses TLS-PKI	Select between One Touch Configuration (using Transport Layer Security with Pre-Shared Key) or Remote Configuration (using Transport Layer Security with Public Key Infrastructure) based on Intel® AMT deployment policy.
Provisioning Server Port	Numeric	Enter the port of the Provisioning Server. Port number range 0 - 65535.
TLS Pre-Shared Key (PSK) PID	User defined	The PID (Provisioning Identifier) is an 8-character alpha-numeric string in dash-separated format (for example: ABCD-123K). Both PID and PPS (Provisioning Passphrase) must be set to establish a secure TLS-PSK session.

TLS Pre-Shared Key (PSK) PPS	User defined	The PPS (Provisioning Passphrase) is a 32-character alpha-numeric string in dash-separated format (for example: EGET-GZFF-C6A6-ORRR-HQXP-C9JI-RJGB-KBS8). Both PID (Provisioning Identifier)and PPS must be set to establish a secure TLS-PSK session.

Intel® ME > Intel® Active (or Standard) Management Technology Configuration > Remote Setup and Configuration > Manage Permanent Certificates

BIOS Setting	Options	Description / Purpose
Active Certificate	• Yes • No	Determines if the certificate hash is active or not. Active certificates can be used in the Remote Configuration PKI process. **Yes:** active **No:** inactive
Certificate Algorithm	Information only	Displays the certificate algorithm: either **SHA1**, **SHA256**, or **SHA384**.
Hash Value	Information only	Displays the hash value of the permanent certificate or the user define certificate.
Permanent Certificate Name	Information only	Displays the permanent certificate name.

Intel® ME > Intel® Active (or Standard) Management Technology Configuration > Remote Setup and Configuration > Manage User Defined Certificates

BIOS Setting	Options	Description / Purpose
Active Certificate	• Yes • No	Determines if the certificate hash is active or not. Active certificates can be used in the Remote Configuration PKI process. **Yes:** active **No:** inactive

Certificate Algorithm	• Empty • SHA1 • SHA256 • SHA384	Algorithm type must match the generated certificate hash
Hash Value	Information only	Displays the hash value of the permanent certificate or the user define certificate.
User Hash Certificate #x	User Defined	A readable unique identifier that is used to track the certificate hash. An alpha numeric entry is supported.

Intel® ME > Intel® Active (or Standard) Management Technology Configuration > SOL/IDER Configuration

BIOS Setting	Options	Description / Purpose
Redirection Mode	• Enable • Disable	Enable or disable redirection mode. Redirection mode must be enabled when using a legacy SMB Redirection Console which was intended for AMT 5.0 or earlier.
SOL/IDER Authentication Mode	• Enable • Disable	Selects how IDER and SOL operation verify and secure interfaces on LAN. **Enable:** requires Kerberos. **Disable**: allows user name and password authentication.

Intel® ME > Intel® Active (or Standard) Management Technology Configuration > View Provisioning Record

BIOS Setting	Options	Description / Purpose
Cert. Serial Number	Information only	Displays the certificate serial number.
Cert. Type	Information only	Displays the certificate type: either **User Defined**, **Permanent Default**, or **Not Defined**.
Date	Information only	Displays the provisioning date.

Hash Data	Information only	Displays the hash data.
Hash Type	Information only	Displays the hash type: either **MD5**, **SHA1**, **SHA256**, **SHA512**, or **Not Defined**.
Host Initiated	Information only	Displays the host initiated status: either **Yes**, **No**, or **Invalid**.
Mode	Information only	Displays the provisioning mode: either **TLS-PSK**, **TLS-PKI**, or **Not Defined**.
Provisioning Record Details	Information only	Displays the provisioning information, including the following: • Mode • Server IP Address • Server FQDN • Date • Time Validity Pass • Secure DNS • Host Initiated • Hash Data • Hash Type • Cert. Serial Number • Cert. Type
Secure DNS	Information only	Displays the secure DNS: either **Yes**, **No**, or **Invalid**.
Server FQDN	Information only	Displays the provisioning server FQDN.
Server IP Address	Information only	Displays the provisioning server IP address.
Time Validity Pass	Information only	Displays the time validity pass: either **Yes**, **No**, or **Invalid**.

Intel® ME > Intel® Management Engine Configuration

BIOS Setting	Options	Description / Purpose
Deep S4/S5	• Enable • Disable	Enable or disable deep S4/S5. 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.
Idle Timeout	User defined	A value between **0** and **65535**. Sets the number of minutes of idle time before Intel® ME will sleep. Default value is 0. With this setting, Intel® ME will not sleep, with no power savings. *This option is present only if "Turn on Intel® ME in Sleep States" is enabled.*
Manageability Feature	• None • Intel® AMT • Intel® Standard Manageability	**None:** The default value; with this setting, you are allowed to enable/disable onboard LAN. **Intel® AMT:** enables Intel® Active Management Technology - for more information, refer to http://www.intel.com/technology/platform-technology/intel-amt/ **Intel® Standard Manageability**: enables Standard Manageability. AMT or Standard Manageability options are dependent on the installed processor/chipset.
ME Wake from S3, S4, S5	• Enable • Disable	Determines the state of Intel® ME during system sleep states. **Enable**: allows ME to wake during S3, S4 or S5. **Disable:** prevents ME from waking during S3, S4 or S5.

Main

BIOS Setting	Options	Description / Purpose
Active Processor Cores	• All • 1 • 2	Allows you to select the number of cores to enable in each processor package. *This BIOS setting is present only when a multi-core processor is installed.*
BIOS Version	Information only	Displays the version of the BIOS currently installed.
Host Clock Frequency	Information only	Displays the default host clock frequency (in MHz)

Intel® Hyper-Threading Technology	• Enable • Disable	Enables or disables Hyper-Threading Technology. When disabled, only one thread per active core will be available. *This BIOS setting is present only on Intel® Desktop Boards that support Hyper-Threading Technology if a processor supporting Hyper-Threading Technology is installed.* *For information on Hyper-Threading, refer to http://en.wikipedia.org/wiki/Hyperthreading*
L3 Cache RAM	Information only	Displays the total L3 cache memory of the installed processor in megabytes. *This setting appears when the installed processor supports L3 Cache.*
Memory Channel x Slot y	Information only	Displays the installed system memory size in Channel x Slot y in gigabytes. One of these lines is displayed for each memory slot present on the motherboard. The lines are displayed in order based on the distance of the memory slot from the processor, with the slots closest to the processor first. Example: Memory Channel A Slot 0 2 GB Memory Channel B Slot 0 1 GB
Memory Speed	Information only	Displays the current memory speed. Defined as current host clock frequency x memory multiplier.
Overridden Host Clock Frequency	Information only	Displays the current host clock frequency. *This BIOS setting is present only on Intel® Desktop Boards where the Host Clock Frequency has been overridden to a non-default value.*
Overridden Memory Speed	Information only	Displays the current memory speed. Defined as current host clock frequency x memory multiplier. *This BIOS setting is present only on Intel® Desktop Boards where the Host Clock Frequency and Memory Multiplier have been overridden.*
Overridden Processor Speed	Information only	Displays the maximum processor speed at current settings. Defined as current host clock frequency x maximum non-turbo ratio. *This BIOS setting is present only on Intel® Desktop Boards where the Host Clock Frequency or Maximum Non-Turbo Ratio have been overridden.*

Overridden Processor Turbo Speed	Information only	Displays the maximum processor speed at current settings. Defined as current host clock frequency x 1-core active turbo ratio. *This BIOS setting is present only on Intel® Desktop Boards where the Host Clock Frequency or Turbo Ratios have been overridden.*
Processor Turbo Speed	Information only	Displays the maximum processor speed at current settings. Defined as current host clock frequency x 1-core active turbo ratio.
Total Memory	Information only	Displays the total installed system memory size in gigabytes.
L2 Cache RAM	Information only	Displays the total L2 cache memory of the installed processor in megabytes. If the installed processor is multi-core, it is displayed as number of cores x L2 cache per core. *This setting appears when the installed processor supports L2 Cache.*
Processor Speed	Information only	Displays the maximum processor speed at current settings. Defined as current host clock frequency x maximum non-turbo ratio.
Processor Type	Information only	Displays the processor brand string obtained from the CPUID instruction.
System Date	Month, day, year	Displays and changes the System Date from the Real-Time Clock. 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 Time	Hours, minutes, seconds	Displays and changes the System Time from the Real-Time Clock. 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.)

Main > System Identification Information

BIOS Setting	Options	Description / Purpose
Microcode Update Revision	Information only	Displays the 32-bit processor microcode update revision in hexadecimal.
Onboard LAN MAC Address	Information only	Displays the MAC Address of the onboard LAN device in hexadecimal.
Processor Family x Model y Stepping z	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 Signature	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.

Main > System Identification Information > Chassis Information

BIOS Setting	Options	Description / Purpose
Asset Tag	Information only	Displays the chassis asset tag string from SMBIOS Type 3 structure.
Manufacturer	Information only	Displays the chassis manufacturer string from SMBIOS Type 3 structure.
Serial Number	Information only	Displays the chassis manufacturer serial number string from SMBIOS Type 3 structure.
Version	Information only	Displays the chassis manufacturer string from SMBIOS Type 3 structure.

Main > System Identification Information > Desktop Board Information

BIOS Setting	Options	Description / Purpose
Manufacturer	Information only	Displays the board manufacturer string from SMBIOS Type 2 structure.
Product Name	Information only	Displays the board product name string from SMBIOS Type 2 structure.
Serial Number	Information only	Displays the board serial number string from SMBIOS Type 2 structure.
Version	Information only	Displays the board version string from SMBIOS Type 2 structure.

Main > System Identification Information > Intel® Management Engine Information

BIOS Setting	Options	Description / Purpose
Firmware Version	Information only	Displays the Intel® ME firmware version currently installed. *This BIOS setting is present only on boards supporting the Intel® Management Engine (Intel® ME).*

Main > System Identification Information > System Information

BIOS Setting	Options	Description / Purpose
Manufacturer	Information only	Displays the system manufacturer string from SMBIOS Type 1 structure.
Product Name	Information only	Displays the system product name string from SMBIOS Type 1 structure.
Serial Number	Information only	Displays the system serial number string from SMBIOS Type 1 structure.
Version	Information only	Displays the system version string from SMBIOS Type 1 structure.

Maintenance

BIOS Setting	Options	Description / Purpose
Clear BIOS Passwords	Continue? (Y/N)	When selected, the BIOS Supervisor Password and BIOS User Password will be cleared. Other BIOS-related passwords (Intel® ME, hard drive, etc.) are left intact.
Clear Trusted Platform Module	• No • 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. *This BIOS setting is present only on Intel® Desktop Boards that include support for Trusted Platform Module (TPM) and have TPM enabled.* *For more information, refer to your Trusted Platform Module Quick Reference Guide.*
DIMM n (Memory Channel x Slot y)	Information only	Displays the installed system memory size in DIMM n (Channel x Slot y) in gigabytes (for example: 2 GB). One of these lines is displayed for each memory slot present on the motherboard. The lines are displayed in order based on the distance of the memory slot from the processor, with the slots closest to the processor first. DIMM numbering is based on the suggested order of memory loading and should match the label on the board silkscreen.

Reset Intel® AMT to default factory settings	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.
Reset Intel® Standard Manageability to default factory settings	Continue? (Y/N)	Resets all Intel® Standard Manageability configuration settings to their factory defaults. When selected, the BIOS will unprovision Standard Manageability and load default Intel® ME settings.

Performance

BIOS Setting	Options	Description / Purpose
Core Max Multiplier	Information only	Displays the default, proposed and active core max multiplier.
Failsafe Watchdog	• Enable • Disable	Enables or disables Failsafe Watchdog. 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.
Host Clock Frequency (MHz)	Numeric	Host Clock Frequency x Processor Multiplier = Processor Speed Host Clock Frequency x Memory Multiplier = Memory Speed Note: To increase stability at higher base clock frequencies, reduce the Processor Multiplier or Memory Multiplier.
Host Clock Frequency Override	• Automatic • Manual	**Manual:** allows you to override the Host Clock Frequency *This BIOS setting is present only on Intel® Desktop Boards that allow the host clock frequency to be overridden.*
Intel® Turbo Boost Technology	Information only	Displays the default, proposed and active Intel® Turbo Boost Technology status.
Memory	Information only	Displays the default, proposed and active memory voltage.
Multiplier	Information only	Displays the default, proposed and active memory multiplier.
PCH Core	Information only	Displays the default, proposed and active PCH core voltage.
Processor Core	Information only	Displays the default, proposed and active processor core voltage.
Processor System Agent	Information only	Displays the default, proposed and active processor system agent voltage.

Speed	Information only	For processor: displays the default, proposed and active processor speed. For memory: displays the default, proposed and active memory speed

Performance > Bus Overrides

BIOS Setting	Options	Description / Purpose
Allow Simultaneous PCIe x16 Video Card (PEG) and IGD	• Enable • Disable	Enable this to allow a PCIe x16 video card (PEG) installed in a x16 slot to be enabled at the same time as processor-integrated video (IGD).
PCH Core Voltage Override	Multiple voltage values	PCH Core Voltage might need to be adjusted when raising Uncore/QPI Voltage under the configuration page to achieve stable operation.
PCI Bus Frequency	Information only	Displays the PCI bus frequency
PCI Express Bus Frequency	• 110MHz • 109MHz • 108MHz • 107MHz • 106MHz • 105MHz • 104MHz • 103MHz • 102MHz • 101MHz • Default	Sets PCI Express clock frequency. Legacy PCI clock frequency is set to 1/3 of this.

Performance > Memory Overrides

BIOS Setting	Options	Description / Purpose
ECC Event Logging	• Enable • Disable	Enables or disables event logging of ECC events.
Memory Correction	• Non-ECC • ECC	Allows you to turn error reporting on or off if the system and all the memory installed supports ECC (Error Correction Code). *This BIOS setting is present only on Desktop Boards that support ECC memory when ECC DIMMs are installed.*
Performance Memory Profiles	• Automatic • Manual – User Defined • Profile x: XMP-Frequency	Use default memory settings from DIMM SPD, manually override memory settings or select an XMP profile. **Automatic**: BIOS configures all memory parameters automatically **Manual – User Defined:** Allows user to have full control over the memory parameters **Profile x: XMP-Frequency**: BIOS configures memory parameters according to selected XMP profile
Uncore Multiplier	Numeric	Uncore Multiplier affects performance and stability of processor functionality such as L3 Cache, Memory Controller, and Integrated Graphics Device.

Uncore Voltage Override	Multiple voltage values	Allows the CPU Uncore voltage to be adjusted.

Performance > Memory Overrides > Performance Memory Profiles

BIOS Setting	Options	Description / Purpose
Command Rate	• Auto • 1T • 2T	**Auto:** adjusts based on memory mode. 2T is usually more stable.
Memory Multiplier	• Auto • Multiplier: DDRx-Frequency	**Auto:** BIOS selects memory multiplier based on Host Clock Frequency, multipliers supported by installed processor, and memory frequencies supported by DIMM. **Multiplier: DDRx-Frequency:** BIOS will use specified memory multiplier. Memory will run at the frequency shown if the accompanying multiplier is selected.
Memory Voltage	Multiple voltage values	Changing memory voltage may allow for overclocking and/or improve memory compatibility.
System Agent Voltage Override	+/- to change value	Changing system agent voltage may allow for memory overclocking.
tCL	+/- to change value	CAS Latency: # of cycles between request for data and data read
tFAW	+/- to change value	Four Active Window: period of time before the 5th successive ACTIVE command to a new bank can be issued
tRASmin	+/- to change value	Minimum RAS Active Time: # cycles between precharge and bank activation
tRC	+/- to change value	Row Cycle Delay: minimum interval between successive ACTIVE commands to the same bank
tRCD	+/- to change value	RAS-to-CAS Delay: # of cycles between activating and read/write
tRFC	+/- to change value	RAS Refresh: # cycles from refresh to activation of a row
tRP	+/- to change value	RAS Pre-Charge: # cycles between closing one row and opening the next.
tRRD	+/- to change value	RAS to RAS Delay: # cycles to activate next bank in the same rank
tRTP	+/- to change value	Read to Precharge Delay: # cycles between read and precharge command to same rank
tWR	+/- to change value	Write Recovery: # cycle between write and precharge

tWTR	+/- to change value	Write to Read: # cycles between write and next read commands; related to tCL

Performance > Processor Overrides

BIOS Setting	Options	Description / Purpose
CPU Idle State	• High Performance • Low Power	**High Performance** forces the operating system to use the Maximum Multiplier at all times. **Low Power** allows the operating system to adjust the multiplier down.
CPU Voltage Override	Multiple voltage values	Sets the processor voltage. **Warning:** Changing this value from the default can shorten the life of the processor. Default value is strongly recommended.
CPU Voltage Override Type	• None • Static • Dynamic	**None:** Allows the processor to manage its own power usage with default upper limits. **Static**: Keeps the processor at a specific user specified voltage at all times. **Dynamic:** Allows the processor to manage its own voltage level, but with user-specified upper limits.
CPU VREG Droop Control	• Low V-droop (Performance) • Mid v-droop • High V-Droop (Power Saving)	Selecting a lower V-droop supplies more overall power to the CPU. This will increase heat, but may provide more CPU stability.
Intel® Turbo Boost Technology	• Enable • Disable	**Enable**: Allows processor cores to run faster than the base operating frequency when running below power, current, and temperature limits. **Disable**: Uses Maximum Non-Turbo Ratio
Maximum Non-Turbo Ratio	Numeric	Maximum Non-Turbo Processor Speed = Maximum Non-Turbo Ratio x Host Clock Frequency This parameter along with Host Clock Frequency determines the maximum processor speed when Intel® Turbo Boost Technology is not engaged.

Performance > Processor Overrides > Intel® Turbo Boost Technology

BIOS Setting	Options	Description / Purpose
1-Core Ratio Limit 2-Core Ratio Limit 3-Core Ratio Limit 4-Core Ratio Limit	Numeric	Maximum processor multiplier used by Intel® Turbo Boost Technology when x cores are active.
Long Duration Power Limit Override (Watts)	Numeric	Intel® Turbo Boost Technology will use this power limit during the Long Duration Power Limit Time Window.
Long Duration Power Limit Time Window	Numeric	Intel® Turbo Boost Technology will use the Long Duration Power Limit Override during the Long Duration Power Limit Time Window (specified in seconds).

Short Duration Power Limit Override (Watts)	Numeric	Intel® Turbo Boost Technology will use this power limit for a very short duration. After that, the Long Duration Power Limit will be honored.
TDC Current Limit Override (Amps)	Numeric	Intel® Turbo Boost Technology will be disengaged if the processor is operating beyond this current limit.
TDP Power Limit Override (Watts)	Numeric	Intel® Turbo Boost Technology will be disengaged if the processor is operating beyond this power limit.

Power

BIOS Setting	Options	Description / Purpose
After Power Failure	• Stay Off • Last State • Power On	Determines the mode of operation after power is restored if a power loss occurs. **Stay Off:** after power is restored, the system stays off until the power button is pressed. **Last State:** after power is restored, the system returns to the last power state before power was lost. **Power On:** after power is restored, the system automatically powers on.
CPU C States	• Enable • Disable	Enable or disable the CPU C State. If enabled, BIOS will report C States below C1 to the operating system. This allows the processor to be placed into lower power states when idle to reduce power consumption and heat generation.
Enhanced Halt State (C1E)	• Enable • Disable	Enable or disable Enhanced Halt State which allows the processor to consume less power and generate less heat while in the C1E (Halt) idle state.
Enhanced Intel SpeedStep® Technology	• Enable • Disable	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. *For information on SpeedStep, refer to http://en.wikipedia.org/wiki/Speedstep*
OS ACPI C2 Report	• Enable • Disable	Enable or disable OS ACPI C2 Report. If enabled, BIOS will report ACPI C2 State (mapped to processor C3 state).
PCIe ASPM Support	• Disable • Enable • PEG Only	**Disable**: ASPM support is disabled for all PCIe devices. **Enable**: ASPM support is enabled for all PCIe devices. **PEG Only**: ASPM is only enabled for devices installed in PCI Express Graphics (PEG) slots.
S1 State Indicator	• Off • Blink • On • Alternate Color	Determines front panel LED behavior during S1 system power state.

S3 State Indicator	• Off • Blink • On • Alternate Color	Determines front panel power LED behavior during S3 system power state.
Wake on LAN from S4/S5	• Stay off • Power On – Normal Boot • Power On – PXE Boot	Configures behavior when a Wake on LAN packet is received during S4/S5. **Stay off**: the system will not wake from S4/S5 power state when a Wake on LAN packet is received. **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. **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. 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	• Enable • Disable	Enable or disable system wake on alarm event. When enabled, system will wake on the day/hour/minute/second specified.
Wakeup Date	Numeric range 0 - 31	Select day of each month to wake the system. Select 0 for daily wakeup.
Wakeup Hour	Numeric range 0 - 23	Select wakeup hour in 24-hour format. For example, 15 means 3 PM.
Wakeup Minute	Numeric range 0 - 59	Select wakeup minute.
Wakeup Second	Numeric range 0 - 59	Select wakeup second.

Security

BIOS Setting	Options	Description / Purpose
Chassis Intrusion	• Disable • Enable or • Disable • Log Only • Pause POST	Enables or disables the chassis intrusion feature. **Disable:** ignores chassis intrusion and will not log the event. **Log only:** creates an entry in the BIOS event log. **Pause POST:** creates a BIOS event log entry and displays a message.
Clear User Password	Continue? (Y/N)	Clears the user password. *This BIOS setting is present only if a user password has been set.*
Hard Disk Drive Password	Information only	Reports if there is a hard disk drive password set.

Intel Trusted Execution Technology	• Enable • Disable	Enables or disables Intel® Trusted Execution Technology which provides hardware-based mechanisms that may help protect against software-based attacks and protect the confidentiality and integrity of data. If Intel® TXT is enabled, then Intel® VT, Intel® VT-d, Intel® HT, all processor cores, and the onboard TPM will also be enabled. Once Intel® TXT is enabled, it must be disabled before disabling any of these required features. *For information on Trusted Execution Technology, refer to http://www.intel.com/technology/security/*
Intel® Virtualization Technology	• Enable • Disable	Enables or disables Virtualization Technology. Takes affect only after power cycling. *For more information refer to http://www.intel.com/technology/virtualization/index.htm*
Master Key Hard Disk Drive Password	Information only	Reports if there is a master key hard disk drive password set.
Set Hard Disk Drive Password	User defined	Sets the Hard Disk Drive password 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	User defined	Sets the Master Key Hard Disk Drive password 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	User defined	Sets the Supervisor password. 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	User defined	Sets the User password. 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.
Supervisor Password	Information only	Reports if there is a supervisor password set.
User access Level	• Full • Limited • View Only • No Access	User Access Level determines the level of BIOS Setup access granted when the User Password is entered. **Full:** User Password grants access to all questions except User Access Level. **Limited:** User Password grants access to Time/Date/Language/User Password questions. **View Only:** User Password grants access only to Language question and changes cannot be saved. **No Access:** User Password cannot be used to access Setup. *This BIOS setting is present only if a supervisor password has been set.*
User Password	Information only	Reports if there is a user password set.
XD Technology	• Enable • Disable	Enables or disables XD Technology. Execute Disable Bit functionality may help prevent certain classes of malicious buffer overflow attacks when combined with a supporting operating system. *For more information, refer to http://www.intel.com/technology/xdbit/*

Security > Intel® VT for Directed I/O (VT-d)

BIOS Setting	Options	Description / Purpose
ATS	• Enable • Disable	Enables or disables Non-Isoch VT-d Engine Address Translation Services (ATS) Support
Coherency Support	• Enable • Disable	Enables or disables Non-Isoch VT-d Engine Coherency Support
Intel® VT for Directed I/O (VT-d)	• Enable • Disable	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. *For information on Intel® VT, refer to http://www.intel.com/technology/advanced_comm/virtualization.htm*
Interrupt Remapping	• Enable • Disable	Enables or disables VT-d Interrupt Remapping Support

Pass Thru DMA	• Enable • Disable	Enables or disables Isoch/Non-Isoch VT-d Engine Pass-Thru DMA Support