BIOS Setup User Guide for 13th Generation Dell PowerEdge Servers

Wei Liu
Dell Server BIOS Development
September 2014

Revisions

Date	Description
August 2014	Initial draft

Table of contents

Executive summary

The 13th generation of Dell PowerEdge servers provides a System Setup utility to help manage different settings and features of your system without booting to the operating system. Using System Setup, you can configure the **System BIOS** settings, **iDRAC Settings,** and **Device Settings** of your system. This document is intended to mainly cover the usage of the System BIOS settings.

There are two user interfaces for System Setup, GUI-mode and text-mode. By default, the standard graphical mode (GUI) browser is enabled (Fig.1). In this mode, the user can use a mouse to help select settings and navigate through different pages.

Note: The use of mouse is optional in the graphical mode browser.

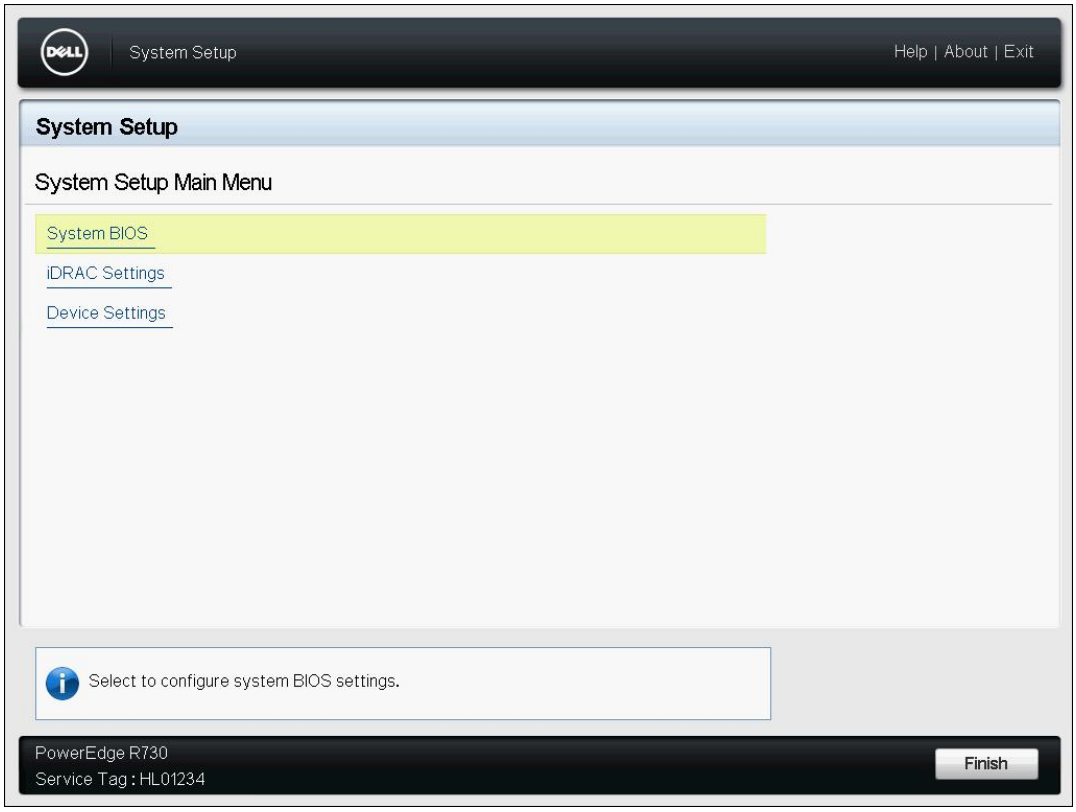


Fig. 1, Graphical Browser mode of System Setup

The text mode browser (Fig. 2) is enabled when serial console redirection is active. This mode does not support mouse interface.

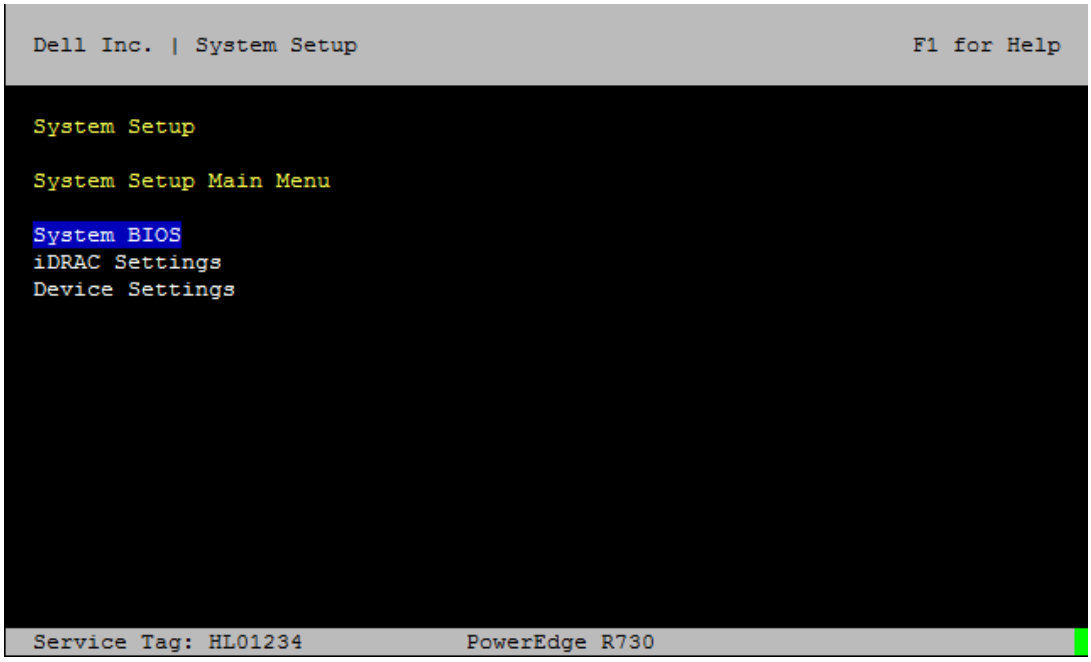


Fig.2 Text Browser mode of the System Setup

Note: You can also modify the BIOS setup options remotely using the WS-MAN and RACADM script methods.

1. Entering System Setup

There are multiple ways to enter the System Setup utility:

- Press <F2> immediately after you see the message **F2 = System Setup** during system start up.
- Press <F11> to launch the Boot Manager. On the Boot Manager screen, select **Boot Manager** -> **Launch System Setup**.
- For iDRAC remote users, System Setup can be initiated in the next reboot by selecting the **Next Boot** drop down list (Fig. 3) of the virtual console.

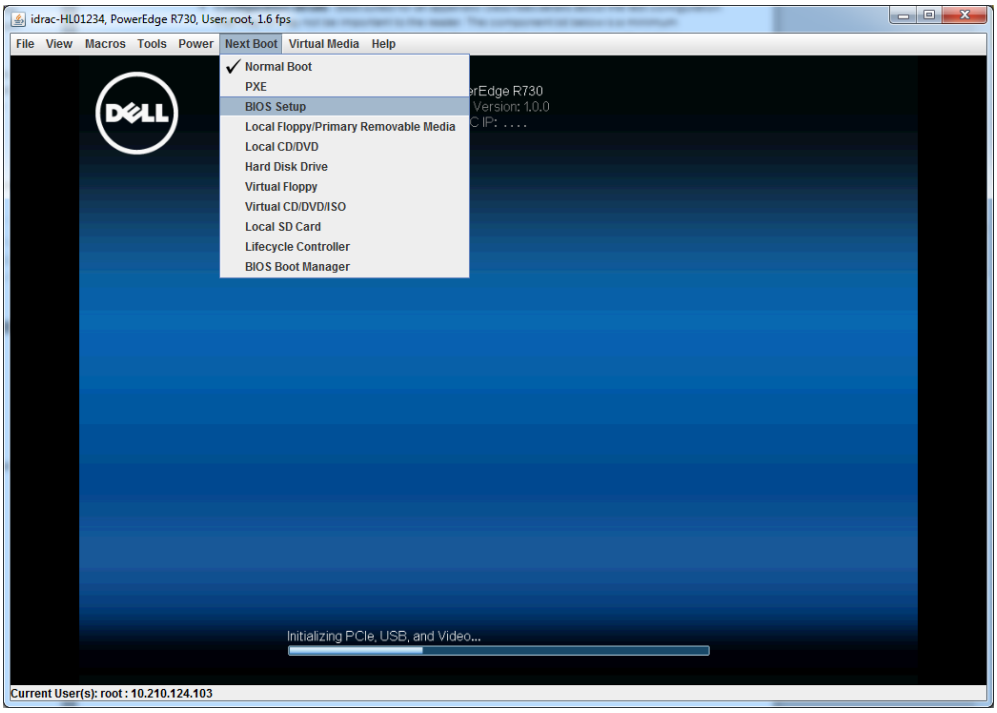


Fig. 3 Launch System Setup from iDRAC virtual console

- Lifecycle Controller users can launch System Setup by selecting the System Setup tab (Fig. 4).

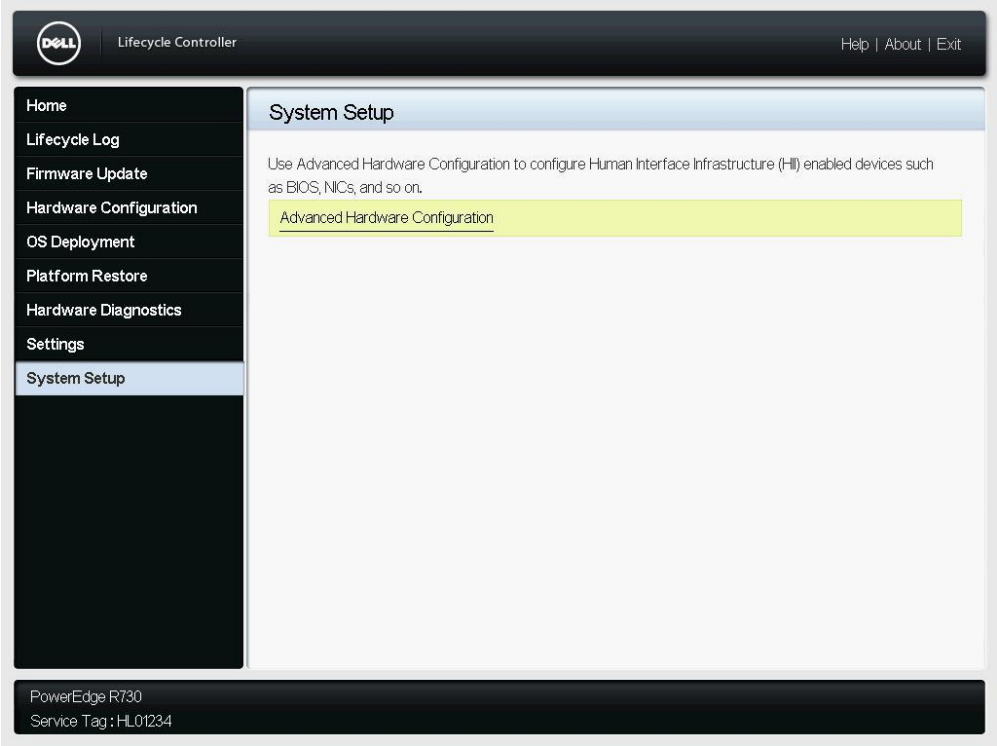


Fig. 4, Launch System Setup from Lifecycle Controller

2. System BIOS

In the main page of the System BIOS Setup (Fig. 5), the following menu items are presented.

Menu Item	Description
System Information	Displays information about the system such as system model name, BIOS version, Service Tag, and so on. This page is read-only.
Memory Settings	Displays information and options related to the installed memory.
Processor Settings	Displays information and options related to the processor such as speed, cache size, and so on.
SATA Settings	Display options related to the integrated SATA controller and ports.
Network Settings	Displays options to modify network devices features such as PXE. This option is available only in the UEFI boot mode.
Boot Settings	Displays options to specify the boot mode (BIOS vs UEFI). Enables you to modify UEFI and BIOS boot settings such as boot sequence.
Integrated Devices	Displays options to enable or disable integrated device controllers and ports, to specify related features and options.
Serial Communication	Displays options to enable or disable the serial ports and specify serial communication related features and options.
System Profile Settings	Displays options to change the system profile settings such as power management, memory frequency, and so on.
System Security	Displays options to configure the system security settings like, system password, setup password, TPM security, Secure Boot, and so on. It also enables or disables support for the power and NMI buttons on the system.
Miscellaneous Settings	Displays miscellaneous options to change the system date, time and so on.

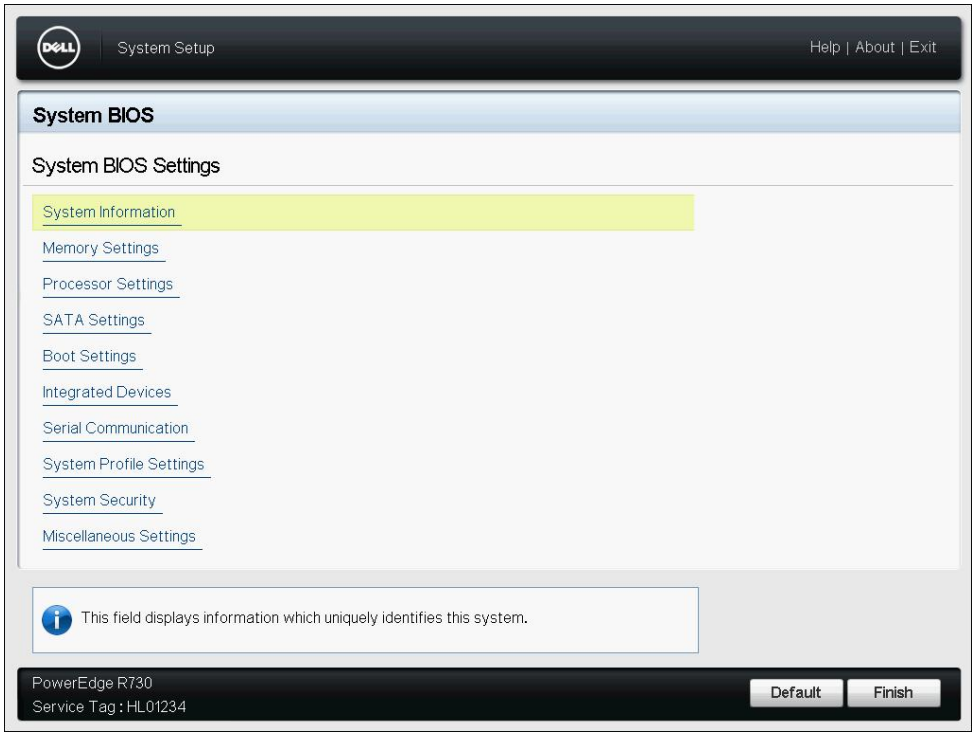


Fig. 5 Main Page of the System BIOS Settings

2.1 System Information

The **System Information** page lists some of the system properties such as Service Tag, BIOS revision, and so on. This page is read-only.

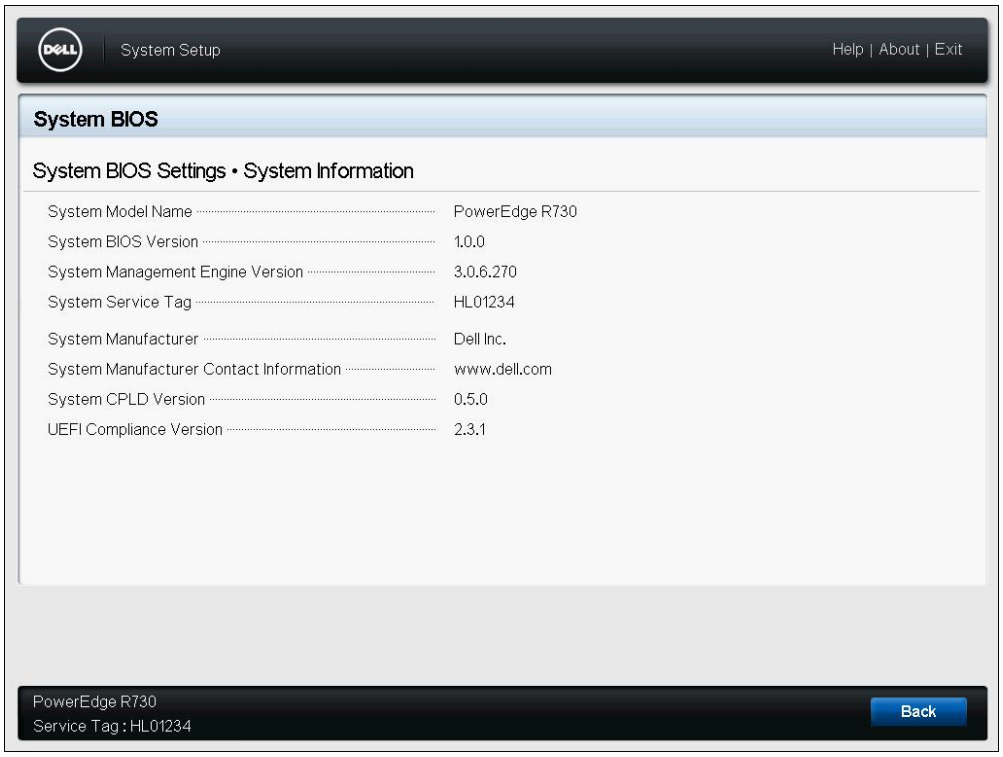


Fig. 6 System Information page

2.2 Memory Settings

The **Memory Settings** page allows you to view some of the properties of the installed memory in the system, as well as enable or disable specific memory features. Detailed descriptions are listed in the table table.

Note: Dell reserves the rights to change the defaults.

Menu Item	Options	Description
System Memory Size	N/A	Displays the amount of memory installed in the system.
System Memory Type	N/A	Displays the type of memory installed in the system.
System Memory Speed	N/A	Displays the system memory speed.
System Memory Voltage	N/A	Displays the system memory voltage.
Video Memory	N/A	Displays the amount of video memory. On 13th generation PowerEdge servers this value is 16MB, reflecting the video memory size of the embedded Matrox video.
System Memory Testing	- Enabled	Specifies whether the BIOS software-based system memory tests

	- Disabled	are conducted during POST. When set to **Enabled**, the memory tests are performed, and test results will be displayed on the screen. By default, **System Memory Testing** is set to **Disabled**. **NOTE**: Enabling this field will result in a longer boot time. The extend of the increase depends on the amount of memory installed in the system. **NOTE**: This memory test is different from the hardware-based memory test which is built-in in the chipset (MBIST). MBIST is performed on every boot.
Memory Operating Mode	- Optimizer Mode - Advanced ECC Mode - Mirror Mode - Spare Mode - Spare with Advanced ECC Mode - Dell Fault Resilient Mode	Allows you to select the memory operating mode. Certain options are active only if a valid memory configuration is detected. By default, **Memory Operating Mode** is set to **Optimizer Mode.** When **Optimizer Mode** is enabled, the DRAM controllers operate independently in 64-bit mode and provide optimized memory performance. When **Advanced ECC Mode** is enabled, the two DRAM controllers are combined in 128-bit mode and provide optimized reliability. Memory that cannot be teamed by the controllers is not reported to the Operating System. When **Mirror Mode** is enabled, the system maintains two identical copies of data in the memory. This feature provides maximum reliability, allows the system to continue running even during a catastrophic memory failure. **NOTE**: In **Mirror Mode**, only half of the installed memory size is reported to the Operating System. When **Spare Mode** is enabled, the BIOS reserves a rank of memory as a spare. At runtime the memory controller can move a rank that exhibits a large number of correctable errors to the spare rank. **NOTE**: In **Spare Mode**, the memory size reported to the Operating System does not include the spare portion. **Spare with Advanced ECC Mode** operates similar to the **Spare Mode**. When this mode is enabled, system runs under **Advanced ECC mode** with a spare rank reserved in each channel. **NOTE**: In **Spare with Advanced ECC Mode**, the memory size reported to the Operating System does not include the spare portion. When **Dell Fault Resilient Mode** is enabled, the BIOS establishes an area of memory that is fault resilient. This mode can be used by an Operating System that supports the feature to load critical applications or enables the Operating System kernel to maximize system availability.
Node Interleaving	- Enabled - Disabled	If **Enabled**, memory interleaving is supported if a symmetric memory configuration is installed. If Disabled, the system

		supports Non-Uniform Memory Access (NUMA) (asymmetric) memory configurations. By default, **Node Interleaving** is set to **Disabled** Operating Systems that are NUMA-aware understand the distribution of memory in a particular system and can intelligently allocate memory in an optimal manner. Operating Systems that are not NUMA aware could allocate memory to a processor that is not local resulting in a loss of performance. Node Interleaving should only be enabled for Operating Systems that are not NUMA aware.
Snoop Mode	- Early Snoop - Home Snoop - Cluster on Die	The Snoop Modes are provided to tune memory performances under different memory bandwidths. Users are given these options to select different mode with their specific system configuration and workloads to optimize the system performance. Snoop functions keep cache coherency across QPI. The difference between **Early Snoop** and **Home Snoop** is the way snoops are generated. **Cluster on Die** arranges the cores/LLC slices to have MLC miss served locally therefore reducing LLC latencies. By default, **Snoop Mode** is set to **Early Snoop.** **NOTE**: The option is only available when **Node Interleaving** is set to **Disabled**.

2.3 Processor Settings

The **Processor Settings** page allows you to control processor-related features.

NOTE: Dell reserves the rights to change the defaults.

Menu Item	Options	Description
Logical Processor	- Enabled - Disabled	Allows you to enable or disable the logical processors (Hyper-Threading Technology). By default, **Logical Processor** is set to **Enabled.**
Alternate RTID (Requestor Transaction ID) Setting	- Enabled - Disabled	Allow you to manipulates Requestor Transaction IDs (RTIDs), which are QPI resources. If **Enabled**, more RTIDs are allocated to the remote socket, increasing cache performance between the sockets. By default, **Alternate RTID (Requestor Transaction ID) Setting** is set to **Disabled.**
Virtualization Technology	- Enabled - Disabled	Allows you to enable or disable the virtualization features.When set to **Enabled**, BIOS enables the processor virtualization features. By default, **Virtualization Technology** is set to **Enabled.**
Address Translation	- Enabled	Allows you to define the **Address Translation Cache** (ATC) for

Services (ATS)	- Disabled	devices to cache the DMA transactions. This field provides an interface to a chipset's Address Translation and Protection Table to translate DMA addresses to host addresses. By default, **Address Translation Services (ATS)** is set to **Enabled.**
Adjacent Cache Line Prefetch	- Enabled - Disabled	Allows you to optimize the system for applications that require high utilization of sequential memory access. You can disable this option for applications that require high utilization of random memory access. By default, **Adjacent Cache Line Prefetch** is set to **Enabled.**
Hardware Prefetcher	- Enabled - Disabled	allows you to enable or disable the Hardware Prefetcher. When enabled, the processor is able to prefetch extra cache lines for every memory request. This setting can affect performance, depending on the application and workloads running on the system and memory bandwidth utilization. By default, **Hardware Prefetcher** is set to **Enabled.**
DCU Streamer Prefetcher	- Enabled - Disabled	Allows you to enable or disable the Data Cache Unit (DCU) streamer prefetcher. This setting can affect performance, depending on the application and workloads running on the system. Recommended for High Performance Computing applications. By default, **DCU Streamer Prefetcher** is set to **Enabled.**
DCU IP Prefetcher	- Enabled - Disabled	Allows you to enable or disable the Data Cache Unit (DCU) IP prefetcher. This setting can affect performance, depending on the application and workloads running on the system. Recommended for High Performance Computing applications. By default, **DCU IP Prefetcher** is set to **Enabled.**
Execute Disable	- Enabled - Disabled	Allows you to enable or disable the Execute Disable Memory Protection Technology that is used in the processors to segregate areas of memory for use by either storage of code instructions or for storage of data. Enable this feature to prevent malicious software and viruses from taking over the system by inserting malicious code into non-executable memory locations. By default, **Execute Disable** is set to **Enabled.**
Logical Processor Idling	- Enabled - Disabled	Allows you to enable or disable the OS capability to put logical processors in the idling state in order to reduce power consumptions. This option is related to Power Capping, and should only be enabled if the operating system supports it. It uses the operating system core parking algorithm and parks some of the logical processors in the system which in turn allow the corresponding processor cores transition into a lower power idle state. By default, **Logical Processor Idling** is set to **Disabled.**
Configurable TDP	- Normal - Level 1 - Level 2	Allows you to reconfigure the processor Thermal Design Power (TDP) levels during POST based on the power and thermal delivery capabilities of the system. TDP refers to the maximum amount of power the cooling system is required to dissipate. By default, **Configurable TDP** is set to **Normal.** **NOTE**: This option is only available on certain SKUs of the processors, and the number of alternative levels varies as well.

x2APIC Mode	-Enabled -Disabled	Allows you to enable or disable the x2APIC mode. Compared to the traditional xAPIC architecture, x2APIC extends the processor addressability and enhances performance of interrupt delivery. By default, **x2APIC Mode** is set to **Disabled.**
Dell Controlled Turbo	- Enabled - Disabled	This field helps with controlling the turbo engagement. It sets the maximum turbo ratio limit based on the number of active cores. This option is active only when the CPU Power Management is set to Maximum Performance and Turbo Boost is Enabled. By default, **Dell Controlled Turbo** is set to **Disabled.**
Number of Cores per Processor	- All - 1 - 2 - 4 - 6 ...	This field controls the number of enabled cores in each processor. Under certain circumstances, limited performance improvements to Intel Turbo Boost Technology and potentially larger shared caches may benefit some workloads. Most computing environments tend to benefit more from larger number of processing cores, so disabling cores to gain nominal performance enhancements must be carefully weighed prior to changing this setting from the default. By default, **Number of Cores per Processor** is set to **All.**
Processor 64-bit Support	N/A	Displays whether the processor(s) support 64-bit extensions.
Processor Core Speed	N/A	Displays the maximum non-turbo core frequency of the processor.
Family-Model-Stepping	N/A	Displays the family, model and stepping of the processor.
Brand	N/A	Displays the brand name provided by the processor manufacturer.
Level 2 Cache	N/A	Displays the total size of L2 cache.
Level 3 Cache	N/A	Displays the total size of L3 cache.
Number of Cores	N/A	Displays the number of cores per processor.

2.4 SATA Settings

The **SATA Settings** page is only available on certain systems that support SATA devices. It allows you to change the SATA controller modes and view each port settings.

Note: Dell reserves the rights to change the defaults.

Menu Item	Options	Description
Embedded SATA	- ATA Mode - AHCI Mode - RAID Mode - Off	Allows setting different modes for the embedded SATA controller(s). By default, **Embedded SATA** is set to **AHCI Mode.** **Note**: Exercise caution when making changes to this field. The operating system previously installed on the SATA hard disk under a particular mode may not boot after the SATA

		controller(s) is changed to a different mode.
Security Freeze Lock	- Enabled - Disabled	Specifies whether BIOS sends Security Freeze Lock command to the embedded SATA drives during POST or not. This option is only applicable to ATA and AHCI mode, not RAID mode. Enabling this feature will prevent changes to all SATA security states until a following system reset. This feature is useful to stop virus and malware from erasing your drive or setting up a password attack. By default, **Security Freeze Lock** is set to **Enabled.**
Write Cache	- Enabled - Disabled	Allows you to enable or disable Write Cache on SATA drives during POST. By default, **Write Cache** is set to **Disabled.**
Port A (B, C....)	- Auto - Off	For Embedded SATA settings in ATA mode, set this field to Auto to enable BIOS support. Set it to Off to turn off the port. By default, **Port A (B,C..F)** is set to **Auto.** **Note**: In case of AHCI mode and RAID mode, this field is grayed out because BIOS enables the port.
Model	N/A	Displays the drive model of the selected device.
Drive Type	N/A	Displays the type of drive attached to the SATA port.
Capacity	N/A	Displays the capacity of the hard drive. This field is undefined for removable media devices like optical drives.

2.5 Boot Settings

The **Boot Settings** page allows you to set the boot modes (BIOS vs UEFI), and specify the boot order.

Note: Dell reserves the rights to change the defaults.

Menu Item	Options	Description
Boot Mode	- BIOS - UEFI	Allows you to set the boot mode. BIOS boot mode is used to boot devices installed with legacy operating systems which do not follow the Unified Extensible Firmware Interface (UEFI) standard. If the operating system supports UEFI, you can set this option to **UEFI**. By default, **Boot Mode** is set to **BIOS**. **Note**: Switching the boot mode may prevent the system from booting if the operating system is not installed in the same boot mode.
Boot Sequence Retry	- Enabled - Disabled	Allows you to enable or disable the boot sequence retry feature. If this field is enabled and system fails to boot, the system BIOS will keep re-attempting the boot sequence every 30 seconds. By default, **Boot Sequce Retry** is set to **Enabled.**
Hard Disk Failover	-Enabled -Disabled	Allows you to enable or disable the hard disk failover. If this set to Enabled, when attempting to boot the "Hard drive C:" boot option, BIOS exhausts every hard disk controller in the Hard-disk

		Drive Sequence instead of just the first one in the list, before falling to the next boot option. By default, **Hard Disk Failover** is set to **Disabled.** **Note**: This option is applicable to BIOS boot mode only.
Boot Option Settings	N/A	Allows you to configure the boot sequence and the boot devices.

2.6 Network Settings

The **Network Settings** menu allows you to modify the UEFI PXE device settings. Modifying UEFI iSCSI device settings may be available in a future BIOS release. BIOS will only connect the UEFI drivers and create corresponding boot options for those network devices that have been enabled and configured in this interface.

Note: Network Settings menu is only available in UEFI boot mode. For BIOS boot mode, the network settings are handled by the network controllers option ROM (either via the configuration utility during option ROM initialization phase, or from the Device Settings menu inside System Setup).

Note: Dell reserves the rights to change the defaults.

Menu Item	Options	Description
PXE Device 1	-Enabled -Disabled	Allows you to enable or disable the PXE device. When enabled, a UEFI boot option is created for the device. By default, **PXE Device 1** is set to **Enabled.**
PXE Device 2(3,4)	-Enabled -Disabled	Allows you to enable or disable the PXE device. When enabled, a UEFI boot option is created for the device. By default, **PXE Device 2(3,4)** is set to **Disabled.**
PXE Device 1 (2,3,4) Settings	N/A	Allows you to control the configuration of the PXE device in UEFI boot mode. You can select the network interface, the protocol (IPv4 vs IPv6), and VLAN settings.

2.7 Integrated Devices

The **Integrated Devices** page allows you to view and configure the settings of all integrated devices in the system.

Note: Dell reserves the rights to change the defaults.

Menu Item	Options	Description
USB3.0 Setting	-Disabled -Enabled -Auto (only on	Allows you to enable the USB 3.0 support. By default, **USB3.0 Setting** is set to **Disabled.**

	Workstations)	When set to **Disabled**, BIOS disables USB 3.0 mode for all the USB3.0 ports. The USB devices operate at USB2.0 speed. When set to **Enabled**, BIOS operates all USB3.0 ports at USB2.0 speed mode during POST, and switches them to USB3.0 mode right after the operating system boots. You must select this option only if the operating system (such as. Windows Server 2012) has a native USB 3.0 driver. Otherwise none of the USB devices will work after boot. The **Auto** option is available only on workstation servers. If this option is selected, the BIOS leaves all USB 3.0 ports at USB 2.0 speed mode, and a special OS switching driver is required to set the USB3.0 port to USB3.0 mode. Microsoft Windows 7 has switching driver capability.
User Accessible USB Ports	- All Ports On - Only Back Ports On - All Ports Off	Allows you to configure the User Accessible USB Ports. Selecting **Only Back Ports On,** disables the front USB ports; selecting **All Ports Off** disables all front and back USB ports. The USB keyboard and mouse will still function in certain USB ports during the boot process, depending on the selection. After the boot process is complete, the USB ports will be enabled or disabled as per the setting of the field. By default, **User Accessible USB Ports** is set to **All Ports On.** **Note**: Selecting **Only Back Ports On** and **All Ports Off** will disable the USB management port and restrict access to the iDRAC USB management port features.
Internal USB Port	- Enabled - Disabled	Allows you to enable or disable the internal USB port. By default, **Internal USB Port** is set to **Enabled.**
Integrated RAID Controller	- Enabled - Disabled	Allows you to enable or disable the integrated RAID controller. By default, **Integrate RAID Controller** is set to **Enabled.**
Integrated Network Card 1 (2)	- Enabled - Disabled	Allows you to enable or disable the integrated network card (NDC). This option is only available to systems that support NDC. By default, **Integrated Network Card 1(2)** is set to **Enabled.** **Note**: If set to **Disabled**, the NIC interface may still be available for shared network access by iDRAC.
Embedded NIC1 and NIC2	- Enabled - Disabled	Allows you to enable or disable the embedded NIC1 and NIC2. This option is only available on systems that do not support NDC. By default, **Embedded NIC1 and NIC2** is set to **Enabled.** **Note**: If set to **Disabled**, the NIC interface may still be available for shared network access by iDRAC.
I/OAT DMA Engine	- Enabled - Disabled	Allows you to enable or disable the I/O Acceleration Technology (I/OAT) option. I/OAT is a set of DMA features designed to accelerate network traffic and lower CPU utilization. This feature should be enabled only if the hardware and software support I/OAT. By default, **I/OAT DMA Engine** is set to **Disabled.**
Embedded Video Controller	-Enabled -Disabled	Allows you to enable or disable the use of the Embedded Video Controller as the primary display. By default, **Embedded Video Controller** is set to **Enabled.** If **Enabled**, the Embedded Video Controller will be the primary

		display even if add-in graphics cards are installed. If **Disabled**, an add-in graphics card will be used as the primary display. BIOS will output displays to both the primary add-in video and the embedded video during POST and pre-boot environment. The embedded video will then be disabled right before the operating system boots. **Note**: When there are multiple add-in graphics cards installed in the system, the first card discovered during during PCI enumeration is selected as the primary video. You may have to re-arrange the cards in the slots in order to control which card is the primary video controller.
Current State of Embedded Video Controller	N/A	Displays the the current state for the Embedded Video Controller. This is a read-only field. If the Embedded Video Controller is the only display capability in the system (that is, no add-in graphics card is installed), then the Embedded Video Controller is automatically used as the primary display even if the **Embedded Video Controller** setting is **Disabled**.
SR-IOV Global Enable	-Enabled -Disabled	Allows you to enable or disable the BIOS configuration of Single Root I/O Virtualization (SR-IOV) devices. Enable this feature if you are booting to a virtualization operating system that recognize SR-IOV devices. By default, **SR-IOV Global Enable** is set to **Disabled.**
OS Watchdog Timer	- Enabled - Disabled	Allows you to enable or disable the operating system watchdog timer. If your system stops responding, this watchdog timer aids in the recovery of your operating system. When set to **Enabled**, the operating system is allowed to initialize the timer. When set to **Disabled** , the timer will have no effect on the system. By default,**OS Watchdog Timer** is set to **Disabled.**
Memory Mapped I/O above 4GB	- Enabled - Disabled	Allows you to enable support for PCIe devices that require large amount of MMIO resources. Enable this option only for 64-bit operating systems. By default, **Memory Mapped I/O above 4GB** is set to **Enabled.**
Slot Disablement	- Enabled - Disabled - Boot Drive Disabled	Allows you to enable or disable PCIe slots on your system. The **Slot Disablement** feature controls the configuration of PCIe cards installed in the specified slot. Slot disablement must be used only when the installed peripheral card is preventing booting into the operating system or causing delays or lockups in system startup. By default, **Slot Disablement** is set to **Enabled.** If the slot is disabled, both the Option ROM and UEFI driver are disabled. The card is not enumerated on the PCI bus and will notbe available to the operating system. If the boot drive is disabled, then the Option ROM or UEFI driver from that slot will not run during POST. As a result,the system will not boot from the card, and its pre-boot services will not be available. However, the card is available to the operating system. **Note**: This option is not available if the slot contains a Dell

		PowerEdge RAID card (PERC). **Note**: Some PCIe device manufacturers implement a master boot driver that can initialize and manage all the similar devices in the system. In this case, to make sure that the Option ROM and UEFI driver do not run, you must select Boot Driver Disabled for all the cards from the same manufacturer (including its integrated device versions such as NDCs).

2.8 Serial Communication

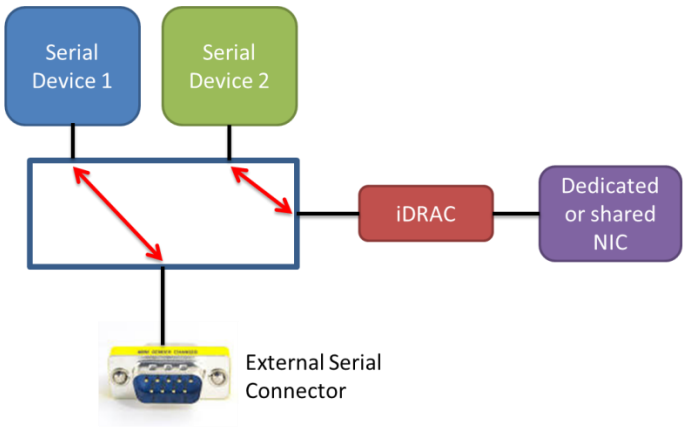
The **Serial Communication** page allows you to view and change the properties of the serial communication settings.

Note: Dell reserves the rights to change the defaults.

Menu Item	Options	Description
Serial Communication	- On without Console Redirection - Auto - On with Console Redirection via COM1 - On with Console Redirection via COM2 - Off	This fields configures the BIOS serial console redirection feature, and determines which serial port address would be used (COM1 = 0x3F8, COM2 = 0x2F8). Auto option will turn on BIOS console redirection for the selected device and port address if a terminal is detected during system startup. By default, **Serial Communication** is set to **Auto.**
Serial Port Address	-Serial Device1=COM1,Serial Device2=COM2 -Serial Device1=COM2,Serial Device2=COM1	Allows you to set the port address for serial devices. By default, **Serial Port Address** is set to **Serial Device1=COM2,Serial Device2=COM1.** **Note**: Only Serial Device 2 can be used for Serial Over LAN (SOL) feature. To use console redirection by SOL, configure the same port address for console redirection and the serial device.
External Serial Connector	- Serial Device 1 - Serial Device 2 - Remote Access Device	Use this field to associate the External Serial Connector to Serial Device 1, Serial Device 2, or the Remote Access Device. By default, **External Serial Connector** is set to **Serial Device1.** **Note**: Only Serial Device 2 can be used for Serial Over LAN (SOL) feature. To use console redirection by SOL, configure the same port address for console redirection and the serial device (refer to Fig 7, 8, 9 for details). **Note**: This serial MUX setting is saved inside iDRAC. The iDRAC can independently change the setting too. The BIOS will sync up the serial MUX setting with the iDRAC on every boot, therefore, loading BIOS default from within the BIOS setup utility may not always revert this setting to the default – "Serial Device 1".
Failsafe Baud Rate	- 115200 - 57600 - 19200 - 9600	Allows you to set the failsafe baud rate for the console redirection. The BIOS attempts to negotiate and determine the serial baud rate automatically during POST. In case of SOL, BIOS retrieves the baud rate value directly from iDRAC. This failsafe

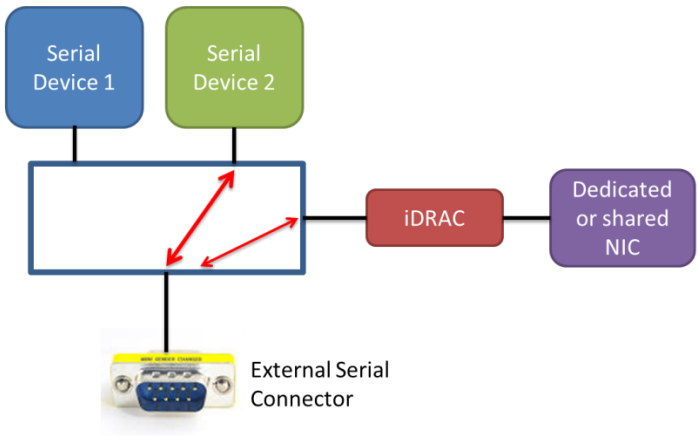
		baud rate is used only if the BIOS was not able to determine the baud rate through either method, auto baud operation or iDRAC. By default, **Failsafe Baud Rate** is set to **115200.**
Remote Terminal Type	- VT100/VT220 - ANSI	Allows you to select the remote console terminal type. This must match the emulation mode type in your serial terminal program (for example, Putty or HyperTerminal). By default, **Remote Terminal Type** is set to **VT100/VT220.**
Redirection After Boot	- Enabled - Disabled	Allows you to enable or disable the BIOS console redirection after the operating system is loaded. By default, **Redirection After Boot** is set to **Enabled.**

The following figure depict the different serial MUX modes for serial communications.



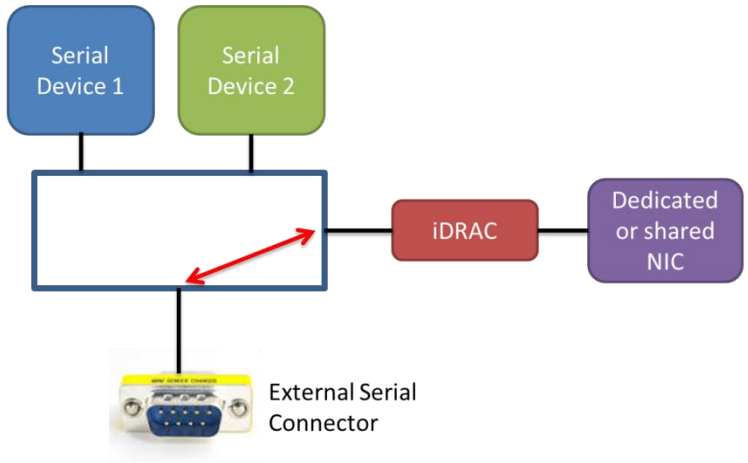
External Serial Connector is set to Serial Device 1. The serial MUX enables concurrent Serial over LAN (SOL) access and external serial connector access to host.

Fig. 7 External Serial Connector set to Serial Device 1



External Serial Connector is set to Serial Device 2. Under this mode the Remote Access Device can snoop for Break Sequence between the external serial connector and the host.

Fig. 8 External Serial Connector set to Serial Device 2



External Serial Connector is set to Remote Access Device. The serial MUX enables Serial Emergency Management Port Mode.

Fig. 9 External Serial Connector set to Remote Access Device.

After console redirection is enabled and active, the BIOS Setup utility interface turns into text mode.

The following screen shot list the key mappings for some special keys in console redirection:

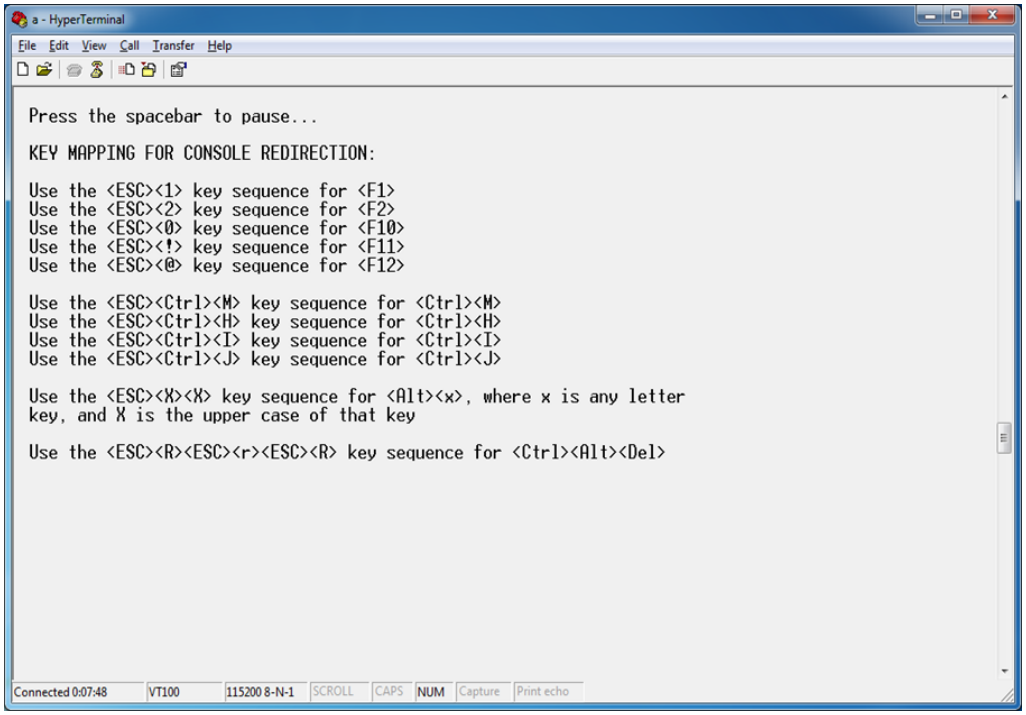


Fig. 10 Key mapping for console redirection

2.9 System Profile Settings

The **System Profile Settings** menu provides various system profiles to target for performance, performance-per-watt, or RAS for dense configurations to facilitate different customer workloads.

Note: Dell reserves the rights to change the defaults.

<table>
<tr><th>Menu Item</th><th>Options</th><th>Description</th></tr>
<tr><td>System Profile</td><td>- Performance per Watt (DAPC)
- Performance per Watt (OS)
- Performance
- Dense Configuration
- Custom</td><td>Allows you to set the system profile. When set to a mode other than Custom, BIOS presets each option accordingly. When set to Custom, you can change the setting of each option. By default, System Profile is set to Performance per Watt (DAPC).

• Performance Per Watt Optimized (DAPC)
This mode allows the BIOS to manage the processor power states in order to achieve Performance/Watt maximized at all utilization levels and workload types while still meeting performance requirements. BIOS also manages system Power Capping in this mode.

<table>
<tr><th>Settings</th><th>DAPC</th></tr>
<tr><td>CPU Power Management</td><td>System DBPM (DAPC)</td></tr>
<tr><td>Memory Frequency</td><td>Maximum Performance</td></tr>
<tr><td>Turbo Boost</td><td>Enabled</td></tr>
<tr><td>Energy Efficient Turbo</td><td>Enabled</td></tr>
</table>
</td></tr>
</table>

C1E	Enabled
C States	Enabled
Collaborative CPU Performance Control	Disabled
Memory Patrol Scrub	Standard
Memory Refresh Rate	1x
Uncore Frequency	Dynamic
Energy Efficient Policy	Balanced Performance
Number of Turbo Boost Enabled Cores for Processor x	All
Monitor/Mwait	Enabled

• **Performance Per Watt Optimized (OS)**
Under this mode, the CPU Power Management field is set to OS DBPM. This means that the operating system (OS) controls the processor's power management. The main controls are the processor frequency or performance states (P-states, P0, P1...Pn), and the processor clock throttling (T-states, T0, T1...Tn). The OS modifies the power states to achieve the best operating performance, based on the Node Manager inputs and the processor utilization.

Settings	OS control
CPU Power Management	OS DBPM
Memory Frequency	Maximum Performance
Turbo Boost	Enabled
Energy Efficient Turbo	Enabled
C1E	Enabled
C States	Enabled
Collaborative CPU Performance Control	Disabled
Memory Patrol Scrub	Standard
Memory Refresh Rate	1x
Uncore Frequency	Dynamic
Energy Efficient Policy	Balanced Performance
Number of Turbo Boost Enabled Cores for Processor x	All
Monitor/Mwait	Enabled

• **Performance**
Under this mode, the CPU Power Management field is set to Performance and allows the BIOS to program the processor for the maximum performance state.

Settings	Performance
CPU Power Management	Maximum Performance
Memory Frequency	Maximum Performance
Turbo Boost	Enabled
Energy Efficient Turbo	Disabled
C1E	Disabled
C States	Disabled
Collaborative CPU Performance Control	Disabled

<table>
<tr><td></td><td></td><td>
<table>
<tr><td>Memory Patrol Scrub</td><td>Standard</td></tr>
<tr><td>Memory Refresh Rate</td><td>1x</td></tr>
<tr><td>Uncore Frequency</td><td>Maximum</td></tr>
<tr><td>Energy Efficient Policy</td><td>Performance</td></tr>
<tr><td>Number of Turbo Boost Enabled Cores for Processor x</td><td>All</td></tr>
<tr><td>Monitor/Mwait</td><td>Enabled</td></tr>
</table>

• Dense Configuration Optimized
Under this mode, settings are optimized to achieve maximum level of reliability. This mode istypically selected for systems with high DIMM count configurations where reliability is prioritized over power savings or performance considerations.

<table>
<tr><th>Settings</th><th>Dense Configuration</th></tr>
<tr><td>CPU Power Management</td><td>System DBPM (DAPC)</td></tr>
<tr><td>Memory Frequency</td><td>Maximum Performance - 1</td></tr>
<tr><td>Turbo Boost</td><td>Disabled</td></tr>
<tr><td>Energy Efficient Turbo</td><td>Disabled</td></tr>
<tr><td>C1E</td><td>Enabled</td></tr>
<tr><td>C States</td><td>Enabled</td></tr>
<tr><td>Collaborative CPU Performance Control</td><td>Disabled</td></tr>
<tr><td>Memory Patrol Scrub</td><td>Extended</td></tr>
<tr><td>Memory Refresh Rate</td><td>2x</td></tr>
<tr><td>Uncore Frequency</td><td>Dynamic</td></tr>
<tr><td>Energy Efficient Policy</td><td>Balanced Performance</td></tr>
<tr><td>Number of Turbo Boost Enabled Cores for Processor x</td><td>All</td></tr>
<tr><td>Monitor/Mwait</td><td>Enabled</td></tr>
</table>

• Custom
Under this mode, you can change the settings of individual options.
</td></tr>
<tr><td>CPU Power Management</td><td>- System DBPM (DAPC)
- Maximum Performance
- OS DBPM</td><td>Allows you to set the CPU power management mode. By default, CPU Power Management is set to System DBPM (DAPC).

The Dell Active Power Control (DAPC) mode allows the BIOS to manage the processor power states in order to achieve Performance/Watt maximized at all utilization levels and workload types while still meeting performance requirements.

In the OS (Demand Based Power Management (DBPM) mode, the operating system (OS) controls the processor's power management.

In the Maximun Performance mode, the processor runs at the highest frequency all the time.</td></tr>
<tr><td>Memory Frequency</td><td>- Maximum Performance
- 2133MHz</td><td>Allows you to set the speed at which the memory bus operates. The maximum possible frequency in the system may not be the maximum frequency rated on the installed DIMM. The maximum</td></tr>
</table>

	- 1866MHz ... -Maximum Reliability	memory bus frequency is dependent upon the currently selected profile, the capacity of the DIMMs, the installed DIMM configuration, the operating voltage and the capability of the processor. In most profiles except the Dense Configuration Optimized profile, the BIOS will configure the memory bus frequency to the maximum possible frequency. Under the Custom menu, a memory frequency can be selected to the desired value. However, the selected frequency can never exceed the maximum possible frequency for the system which is limited by the capabilities and configuration of the system as noted above. By default, **Memory Frequency** is set to **Maximum Performance.**
Turbo Boost	- Enabled - Disabled	Allows the processor to engage to a higher frequency than the nominal or rated frequency if the current operating environment allows it. This results in a higher system performance. Turbo Boost is engaged on a per socket basis. If some of the cores of a socket are idle then other cores of the same socket can go to a higher processor performance state. By default, **Turbo Boost** is set to **Enabled.**
Energy Efficient Turbo	-Enabled -Disabled	Allows the user to enable or disable the **Energy Efficient Turbo** (EET) setting of the processor. EET is a mode of operation where a processor's core frequency is adjusted within the turbo range by the Power Control Unit (PCU). When the PCU detects high utilization on a core, the turbo frequency is increased. This feature is intended to save power under less intensive processor utilization workloads. With EET enabled, the PCU identifies an optimal P0 frequency which is tuned by the PCU. The PCU monitors the core memory stall counter to assess efficiency of core frequency increases to remain performance/power efficient. By default, **Energy Efficient Turbo** is set to **Enabled.**
C1E	- Enabled - Disabled	Allows you to enable or disable the processor to switch to C1E (Enhanced Halt State) when it is idle. By default, **C1E** is set to **Enabled.**
C States	- Enabled - Disabled	Allows you to enable or disable the processor to operate in all available power states. By default, **C States** is set to **Enabled.**
Collaborative CPU Performance Control	- Enabled - Disabled	Allows youto enable or disable the **Collaborative CPU Performance Control (CCPC**), a feature that defines an abstracted and flexible mechanism for OS Power Management (OSPM) to collaborate with an entity in the platform to manage the performance of the processors. Without CCPC, the firmware-based power management (that is DAPC) and OS-based power management (that is OSBPM) are mutually exclusive. By default, **Collaborative CPU Performance Control** is set to **Enabled.**
Memory Patrol Scrub	- Extended - Standard - Disabled	Searches the memory for errors and repairs correctable errors to prevent the accumulation of memory errors. By default, **Memory Patrol Scrub** is set to **Standard.** When set to **Disabled**, Patrol Scrubbing does not occur. When set to **Standard** , the entire memory array is scrubbed once

		in a 24 hour period. When set to **Extended**, the entire memory array is scrubbed every 4 hours to further increase system reliability.
Memory Refresh Rate	- 1x - 2x	Allows you to set the memory refresh rate. The memory controller periodically refreshes the data in the memory. The frequency at which memory is normally refreshed is referred to as 1x refresh rate. When memory modules are operating at a higher than normal temperature or to further increase system reliability, the refresh rate can be set to 2x. By default, **Memory Refresh Rate** is set to **1x.**
Uncore Frequency	- Dynamic - Maximum	Allows you to select the processor Uncore Frequency. Dynamic mode allows the processor to optimize power resources across the cores and uncore during runtime. The optimization of the uncore frequency to either save power or optimize performance is influenced by the setting of the **Energy Efficient Policy**. By default, **Uncore Frequency** is set to **Dynamic.**
Energy Efficient Policy	- Performance - Balanced Performance - Balanced Energy - Energy Efficient	Allows you to select the **Energy Efficient Policy**. The CPU uses the setting to manipulate the internal behavior of the processor and determines whether to target higher performance or better power savings. By default, **Energy Efficient Policy** is set to **Balanced Performance.**
Number of Turbo Boost Enabled Cores for Processor 1(2,3,4)	-All	Allows you to control the number of turbo boost enabled cores for processor 1 (2,3,4). By default, the maximum number of cores is enabled.
Monitor/Mwait	- Enabled - Disabled	Allows you to enable or disable the Monitor/Mwait instructions of the processor. When set to **Disabled** the Monitor/Mwait instructions are not supported by the processor. By default, **Monitor/Mwait** is set to **Enabled.** **Note**: Monitor/Mwait can be disabled only when C state is disabled in Custom mode. When C state is enabled in Custom mode, changing this setting does not impact system power/performance.

2.10 System Security

The **System Security** page allows you to perform specific security-related functions such as setting passwords, enable or disable power/NMI buttons, and so on.

Note: Dell reserves the rights to change the defaults.

Menu Item	Options	Description
Intel AES-NI	N/A	Displays the current status of Intel Processor AES-NI feature. This feature improves the speed of applications by performing encryption and decryption using the Advenced Encryption Standard Instruction Set.

System Password	N/A	Allows you to set the system password. The system password is the password that you must enter to allow the system to boot to an operating system. This option is read-only if the password jumper (PWRD_EN) is not installed in the system. Use the following guidelines to assign passwords: - A password can have up to 32 characters. - The password can contain the number 0 through 9 - Both lower case and upper case letters are allowed. - The following special characters are allowed: space, (”), (+), (,), (-), (.), (/), (;), ([), (\), (]), (`).
Setup Password	N/A	Allows you to set the setup password. The setup password is the password that you must enter to change any BIOS settings, with the exception of the system password, which can be changed without entering the correct setup password. This option is read-only if the password jumper (PWRD_EN) is not installed in the system. Use the following guidelines to assign passwords: - A password can have up to 32 characters. - The password can contain the number 0 through 9 - Both lower case and upper case letters are allowed. - The following special characters are allowed: space, (”), (+), (,), (-), (.), (/), (;), ([), (\), (]), (`).
Password Status	- Unlocked - Locked	Allows you to lock the system password. To prevent the system password from being modified, set this option to **Locked** and enable setup password. This field also allows you to prevent disabling the system password during a system boot. By default, **Password Status** is set to **Unlocked.**
TPM Security	-Off -On with Pre-boot Measurements -On without Pre-boot Measurements	Allows you to control the reporting of the Trusted Platform Module (TPM). By default, **TPM Security** is set to **Off.** When set to **Off**, the presence of the TPM is not reported to the operating system. When set to **On with Pre-boot Measurements**, BIOS stores the Trusted Computing Group (TCG) compliant measurements to the TPM during POST. The measurements include important platform configurations measurement which fulfills NIST SP800-155 BIOS Integrity Measurement specification. When set to **On without Pre-boot Measurements**, BIOS bypasses pre-boot measurements. The TPM chip is still visible to the operating system in this case.
TPM Information	N/A	Displays the type of TPM and its firmware version. This field shows unknown if **TPM Security** is set to **Off**.
TPM Status	N/A	Displays the current status of the TPM.
TPM Command	- None - Activate	Allows you to control the Trusted Platform Module (TPM). By default, **TPM Command** is set to **None.**

	- Deactivate - Clear	When set to **None**, no command is sent to the TPM. When set to **Activate**, the TPM is enabled and activated. When set to **Deactivate**, the TPM is disabled and deactivated. When set to **Clear**, all the contents of the TPM are cleared. **Warning**: Clearing the TPM causesloss of all the keys in the TPM. This could affect booting to the operating system. **Note**: This field is read-only when **TPM Security** is set to **Off**. The action requires an additional reboot before it can take effect.
Intel TXT	- Off - On	Allows you to enable or disable the Intel Trusted Execution Technology (TXT). To enable **Intel TXT**, Virtualization Technology must be enabled, **TPM Security** must be set to **On with Pre-boot Measurements**, and **TPM Status** must be **Enabled, Activated**. By default, **Intel TXT** is set to **Off.**
Power Button	- Enabled - Disabled	Allows you to enable or disable the power button on the front panel. By default, **Power Button** is set to **Enabled.**
NMI Button	-Enabled -Disabled	Allows you to enable or disable the NMI button on the front panel. By default, **NMI Button** is set to **Disabled.**
AC Power Recovery	- Last - On - Off	Specifies how the system reacts after AC power has been restored to the system. It is especially useful for people who turn their systems off with a power strip. By default, **AC Power Recovery** is set to **Last.** When set to **Off**, the system stays off after AC power is restored. When set to **On**, the system turns on after AC power is restored. When set to **Last**, the system turns on if the system was on at the moment when AC power was lost. The system will remain off if the system was turned off when AC power was lost. In case of an ungraceful shutdown, the system always turns on.
AC Power Recovery Delay	- Immediate - Random - User Defined	Allows you to set how the system supports staggering of power up after AC power is restored to the system. By default, **AC Power Recovery Delay** is set to **Immediate.**When set to **Immediate**, there is no delay for power-up. When set to **Random**, the system creates a random delay (60s to 240s) for power-up. When set to **User Defined**, the system delays power-up by that amount. The system supported user defined power-up delay range is from 60s to 240s.
User Defined Delay (60s to 240s)	N/A	Allows you to control the user defined **AC Recovery Delay**. Enter a delay in the range of 60s to 240s.
UEFI Variable Access	- Standard - Controlled	Provides varying degrees of securing UEFI variables. By default, **UEFI Variable Access** is set to **Standard.**

		When set to **Standard**, UEFI variables are accessible in the operating system per the UEFI specification. When set to **Controlled**, selected UEFI variables are protected in the environment and new UEFI boot option entries are forced to be appended to the end of the current boot order.
Secure Boot	- Enabled - Disabled	Allows you to enable Secure Boot, where the BIOS authenticates each component that is executed during the boot process using the certificates in the Secure Boot Policy. The following components are validated in the boot process: - UEFI drivers that are loaded from PCIe cards - UEFI drivers and executables from mass storage devices - Operating system boot loaders By default, **Secure Boot** is set to**Disabled.** **Note**: Secure Boot is not available unless the **Boot Mode** (in the **Boot Settings** menu) is set to **UEFI**. **Note**: Secure Boot is not available unless the **Load Legacy Video Option ROM** setting (in the **Miscellaneous Settings** menu) is disabled. **Note**:It is recommended to enable a setup password for Secure Boot.
Secure Boot Policy	- Standard - Custom	Allows you to select the **Secure Boot Policy**. When set to **Standard**, the BIOS uses the system manufacturer's key and certificates to authenticate pre-boot images. When set to **Custom**, the BIOS uses the user-customized key and certificates. By default, **Secure Boot Policy** is set to **Standard.** **Note**: If Custom mode is selected, the **Secure Boot Custom Policy Settings** menu will appear. **Note**: Changing the default security certificates may cause the system to fail booting from certain boot options.
Secure Boot Policy Summary	N/A	Displays the list of certificates and hashes that Secure Boot uses to authenticate images. It displays the type/issuer/subject/GUID information of the Platform Key (PK), Key Exchange Key (KEK), Authorized Signature Database (db) and Forbidden Signature Database (dbx).
Secure Boot Custom Policy Settings	N/A	Allows you to configure the **Secure Boot Custom Policy**. You can enroll and delete PK, KEK, db, and dbx entries.

2.11 Miscellaneous Settings

The **Miscellaneous Settings** page allows you to perform specific functions like updating the asset tag and changing system date and time, and so on.

NOTE: Dell reserves the rights to change the defaults.

Menu Item	Options	Description
System Time	N/A	Allows you to set the time on the system.
System Date	N/A	Allows you to set the date on the system.
Asset Tag	N/A	Displays the asset tag and allows you to modify it for security and asset tracking purposes.
Keyboard NumLock	- On - Off	Determines whether the system boots with Num Lock enabled or disabled. When Num Lock is on, the rightmost keys on the keyboard function like those on a numeric calculator. With Num Lock off, they function as cursor-control keys. By default, **Keyboard NumLock** is set to **On.**
F1/F2 Prompt on Error	- Enabled - Disabled	Allows you to specify the BIOS behavior on certain POST errors. By default F1/F2 Prompt on Error is enabled, meaning when the system will halt at the end of POST waiting for user key input after encountered an error during boot up. By default, **F1/F2 Prompt on Error** is set to **Enabled.** If set to disabled, the BIOS will just display the warning or error message on the screen and continue booting to the operating system. **Note**: For certain catastrophic errors, even if this field is set to Disabled, the BIOS may still prompt F1/F2/F10/F11 during POST.
Load Legacy Video Option ROM	- Enabled - Disabled	Determines whether the system BIOS will load the legacy video (INT10h) option ROM from the video controller or not. Select Enabled if the operating system (Windows Server 2008 is the only known UEFI-aware OS that has this limitation) does not support UEFI video output standards. Failure to enable this option before installing W2K8 will result in a no video display situation after OS boots. For other UEFI-aware operating systems, this field is recommended to be left as Disabled. By default, **Load Legacy Video Option ROM** is set to **Disabled.** **Note**: This field is for UEFI boot mode only, and has no effect when the boot mode is set to BIOS. Also this field cannot be set to Enabled if UEFI Secure Boot is enabled.
In-System Characterization	- Enabled - Disabled - Enabled – No Reboot	Allows you to enable or disable In-System Characterization (ISC). ISC executes during POST upon detecting relevant change(s) in system configuration to optimize system power and performance. ISC usually takes about 20 seconds to execute, and a system reset is required for ISC results to be applied to the components such as memory Voltage Regulators (VR). By

		default, **In-System Characterization** is set to **Enabled – No reboot.** When set to **Enabled – No reboot**, the BIOS executes ISC and continues the boot process without applying the ISC results until the next system reset occurs. When set to **Enabled**, upon executing ISC the BIOS forces an immediate system reset so that ISC results can be applied right away. As a result the boot time will be longer. When set to **Disabled**, the BIOS does not execute ISC at all. **Note**: In the initial launch of 13th generation PowerEdge servers this field by default is set to **Disabled**.