Setting up BIOS on 14th Generation (14G) Dell EMC PowerEdge Servers

This Dell EMC technical white paper describes the BIOS attributes that you can use to manage and customize your Dell EMC 14G PowerEdge servers. It also defines the fields used in configuring these attributes and best practices for defining values in each field, where appropriate.

April 2018

Authors

Wei Liu — Distinguished Engineer (Dell EMC Server BIOS Engineering)
Mark Shutt — Member Technical Staff (Dell EMC Server BIOS Engineering)
Paul Rubin — Senior Product Manager (Dell EMC Systems Management Marketing)

A Dell EMC Technical White Paper

Revisions

Date	Description
March 2018	Initial release by Wei Liu, Mark Shutt, and Paul Rubin

The information in this publication is provided “as is.” Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any software described in this publication requires an applicable software license.

Copyright © 2018 Dell Inc. or its subsidiaries. All Rights Reserved. Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be the property of their respective owners. Published in the USA [4/16/2018] [Technical White Paper]

Dell believes the information in this document is accurate as of its publication date. The information is subject to change without notice.

.

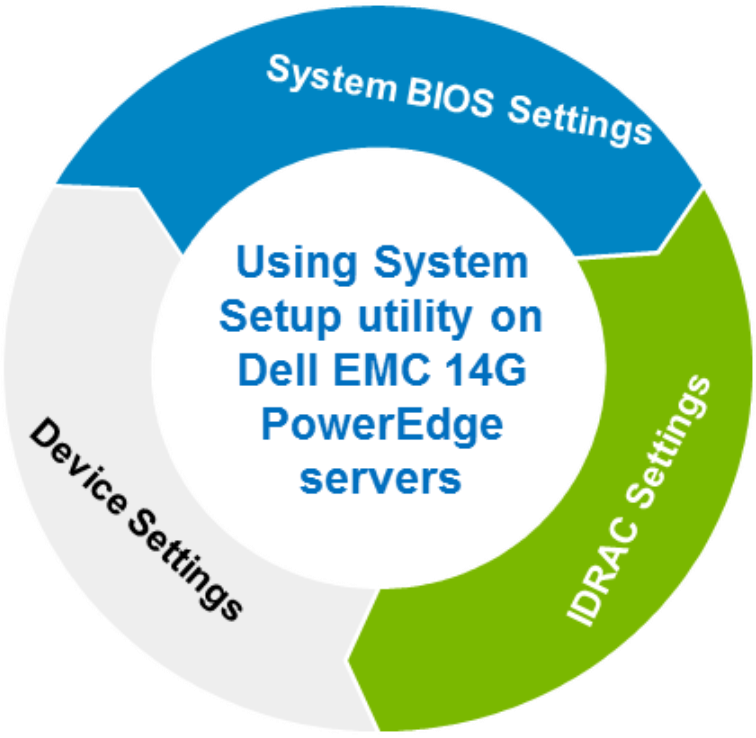
Contents

Acronyms

ACPI	Advanced Configuration and Power Interface
Acronym	Expanded form
AHCI	Advanced Host Controller Interface
ASPM	Advanced State Power Management
BIOS	Basic Input/Output System
DAPC	Dell Active Power Control
DBPM	Demand Based Power Management
DCU	Data Cache Unit
Dell EMC iDRAC	Dell EMC Integrated Dell Remote Access Controller
DPAT	Dell Processor Acceleration Technology
ECC	Error-Correction Code
GUI	Graphical User Interface
I/OAT	I/O Acceleration Technology
IMC	Integrated Memory Controllers
iSCSI	Internet Small Computer Systems Interface
KEK	Key Exchange Key
ME	Management Engine
NDC	Network Daughter Card
NUMA	Non-Uniform Memory Access
PERC	Dell PowerEdge RAID Card
PK	Platform Key
PPI	Physical Presence Interface
PXE	Preboot eXecution Environment
SNC	Sub NUMA Clustering
SOL	Serial Over LAN
SR-IOV	Single Root I/O Virtualization
TCG	Trusted Computing Group
TPM	Trusted Platform Module
TUI	Text User Interface
TXT	Trusted Execution Technology
UEFI	Unified Extensible Firmware Interface
UPI Prefetch	Ultra Path Interconnect

Executive summary

The 14th generation (14G) of Dell EMC PowerEdge servers provides a System Setup utility to help manage different settings and features of your server without booting to the operating system (OS). Using System Setup, you can configure the System BIOS settings, iDRAC settings, and Device Settings of your server. This technical white paper provides an overview of the usage of System BIOS settings.



There are two user interfaces for System Setup—Graphical User Interface (GUI) and Text User Interface (TUI). By default, the standard GUI browser is enabled. In this mode, you can use a mouse device to help select settings and navigate through different pages.

Note: The use of a mouse device is optional in case of GUI.

It is assumed that the reader of this technical white paper has prior working knowledge of system management applications and is familiar with some of the commonly used technologies and acronyms. A list of frequently used Acronyms is also given on the previous page.

Screen shots and architecture diagrams are used to reduce the reading and comprehension on the part of audience. Tabulated data is aimed at helping you quickly understand the features and execute your business-critical functions with less effort.

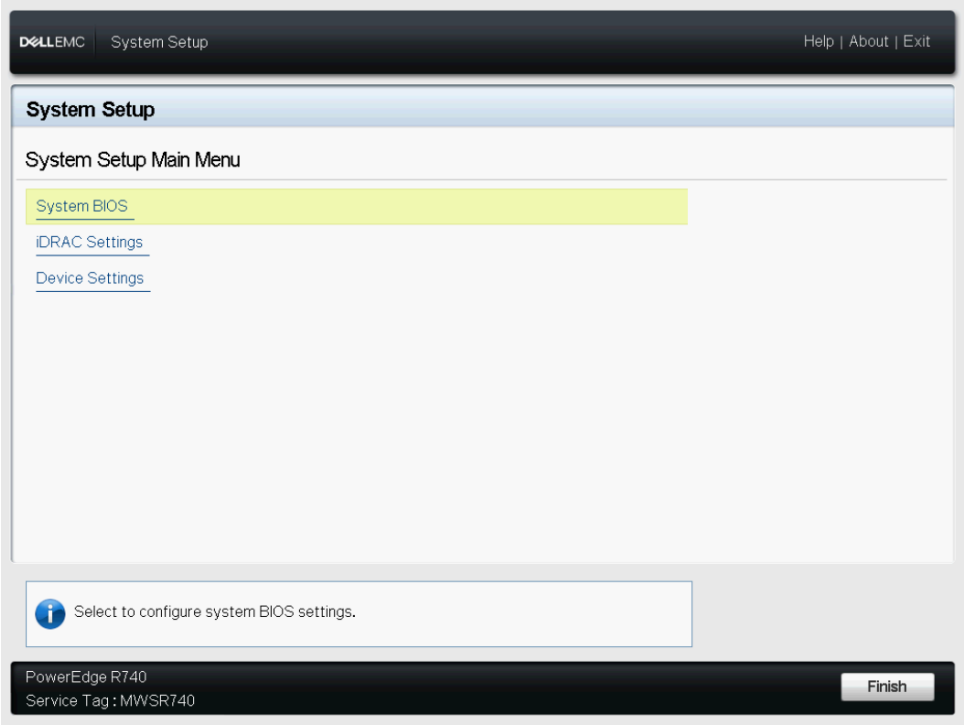


Figure 1 Graphical Browser mode of System Setup

The TUI (Fig. 2) is enabled when serial console redirection is active. This mode does not support the GUI.

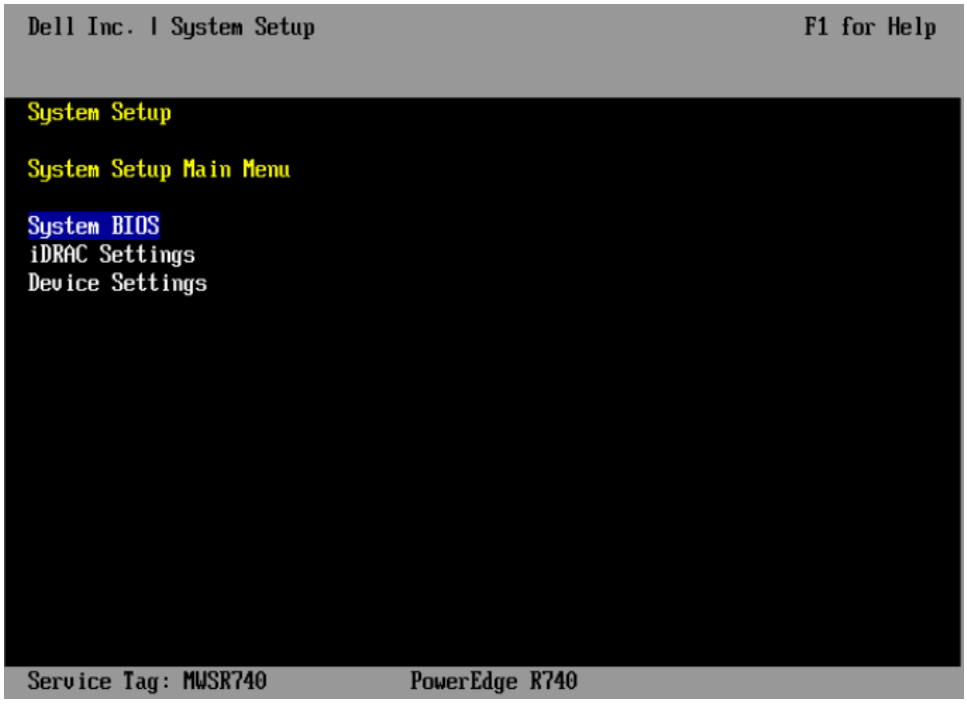


Figure 2 Text Browser mode of the System Setup

Starting System Setup

There are multiple ways to start the System Setup utility:

1. Press F2 immediately when **F2 = System Setup** is displayed during system startup.
2. Else, press F11 to open the Boot Manager page. You can open System Setup by clicking **Boot Manager → Launch System Setup**.
3. For iDRAC virtual console users, initiate the System Setup during the next reboot by selecting from the **Boot** drop-down menu of the virtual console.

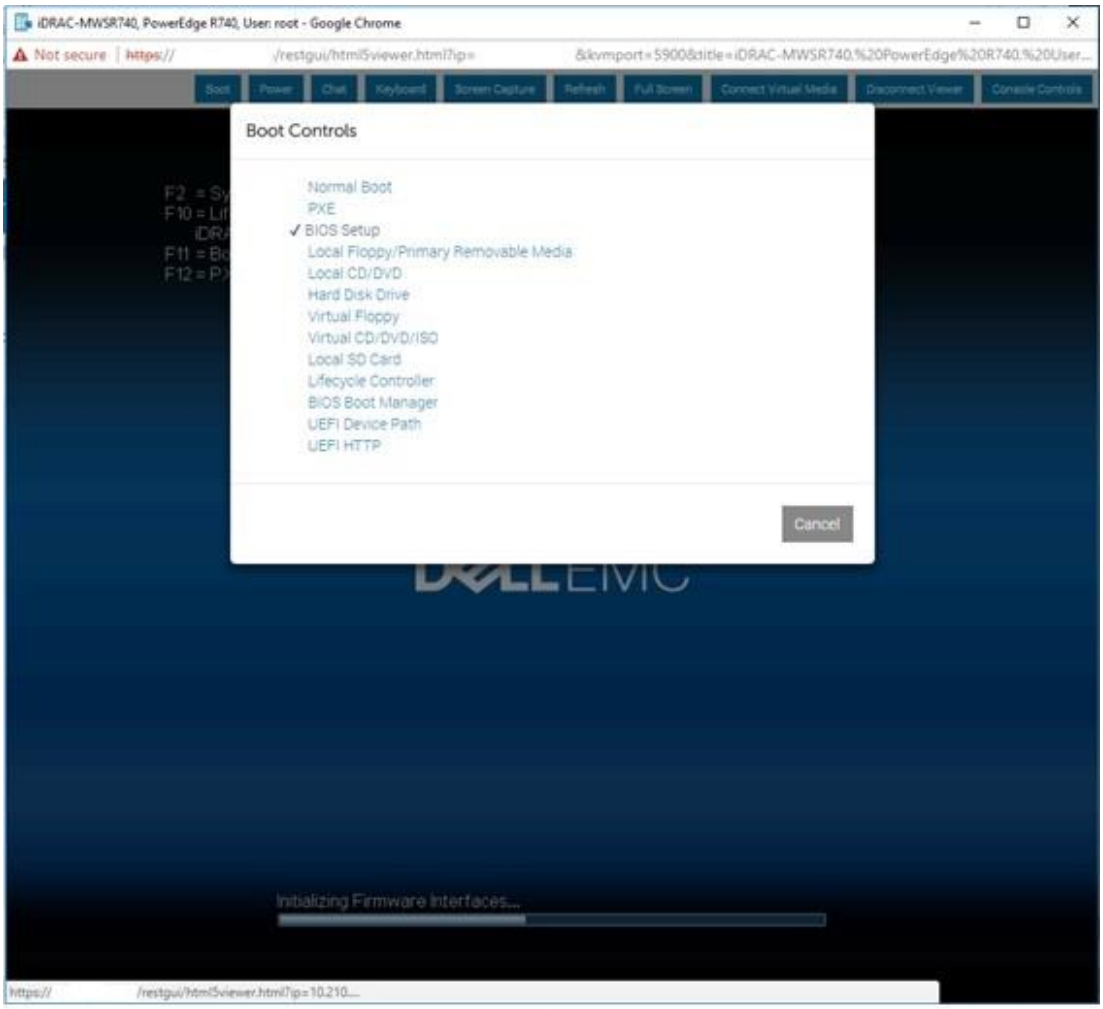


Figure 3 Start System Setup from iDRAC virtual console

4. To open System Setup by using Lifecycle Controller click **System Setup**.

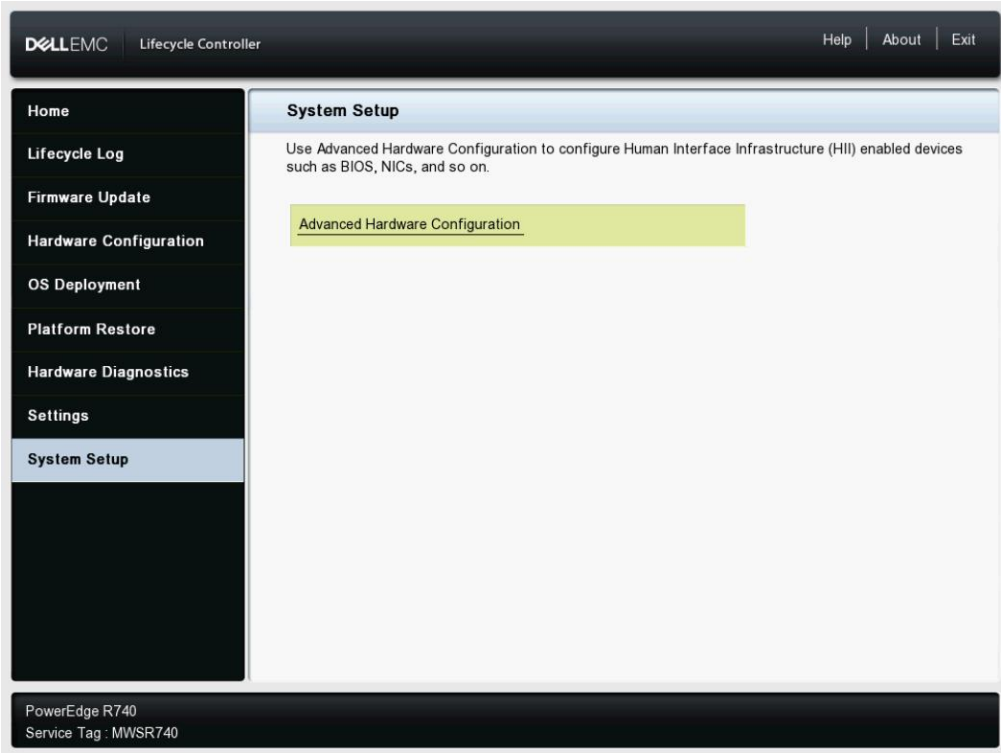


Figure 4 Start System Setup from Lifecycle Controller

1. System BIOS

On the System BIOS Setup page, the following links are displayed:

Menu Item	Description
System Information	Read-only. Displays information about the system such as system model name, BIOS version, and Service Tag.
Memory Settings	Displays information and options related to installed memory.
Processor Settings	Displays information and options related to the processor such as speed and cache size.
SATA Settings	Displays options related to the integrated SATA controller and ports.
NVMe Settings	Displays options related to NVMe drive settings.
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.
Network Settings	Only available in the UEFI boot mode. Displays options to modify network devices features such as PXE, iSCSI, and HTTP Boot.
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 power management and memory frequency.
System Security	Displays options to configure the system security settings such as system password, setup password, TPM security, and Secure Boot. It also enables or disables support for the power and NMI buttons on the server.
Redundant OS Control	Displays options to configure the Redundant OS feature, which allows a redundant OS to be placed on a drive and have it hidden under normal operating conditions.
Miscellaneous Settings	Displays miscellaneous options to change the system date, time, and so on.

1.1 System Information

Lists system properties such as Service Tag and BIOS revision. This page is read-only.

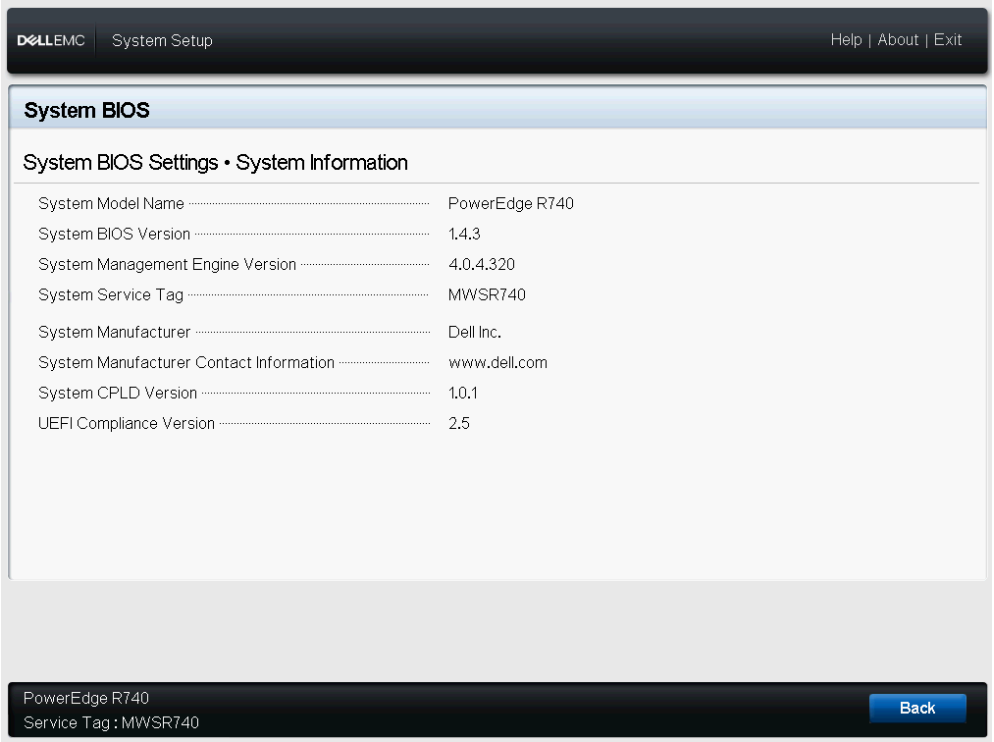


Figure 5 The System Information page

1.2 Memory Settings

Enables you to view some of the properties of the installed memory in the system, and enable or disable specific memory features.

Note: The default option setting is depicted in **boldface**. Dell EMC reserves the rights to change the default properties.

Menu Item	Options	Description
System Memory Size	N/A	Displays the size 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 volume of video memory. On the 14G PowerEdge servers, this value is 16 MB, reflecting the video memory size of the embedded Matrox video.

System Memory Testing	• **Enabled** • Disabled	Specifies whether or not the BIOS software-based system memory tests are conducted during POST. When set to Enabled, the memory tests are performed, and test results are displayed on the screen. **Note**: Enabling results in a longer boot time. The extent 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	Selects the memory operating mode. Certain options are active only if a valid memory configuration is detected. • **Optimizer Mode**—If enabled, the DRAM controllers operate independently in the 64-bit mode and provide optimized memory performance. • Advanced ECC Mode—If enabled, the two DRAM controllers are combined in 128-bit mode and provide optimized reliability. Memory that cannot be grouped by the controllers is not reported to the OS. • Mirror Mode—If enabled, the system maintains two identical copies of data in memory. This feature provides maximum reliability and enables 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 OS. • Spare Mode—If 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 OS does not include the spare portion. • Spare with Advanced ECC Mode—Operates similar to Spare Mode. When this mode is enabled, system runs under Advanced ECC mode with a spare rank reserved in each channel.

		Note: In the Spare with Advanced ECC Mode, the memory size reported to the OS does not include the spare portion. • Dell Fault Resilient Mode—If enabled, the BIOS creates an area of memory that is fault resilient. This mode can be used by an OS that supports the feature to load critical applications or enables the OS kernel to maximize system availability.
Current State of Memory Operating Mode		Read-only. Indicates the current state of the memory operating mode. This can differ from the Memory Operating Mode field if the requested mode cannot be achieved.
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. OSs that detect NUMA detect the distribution of memory in a particular system and can intelligently allocate memory in an optimal manner. OSs that detect NUMA could allocate memory to a processor that is not local, resulting in a loss of performance. Node Interleaving should only be enabled for OSs that are not NUMA aware.
Opportunistic Self-Refresh	• Enabled • **Disabled**	When set to Enabled, the Integrated Memory Controllers (IMCs) may go into self-refresh when it is idled for a period of time.

1.3 Processor Settings

Enables you to control the processor-related features.

Note: The default option setting is depicted in **boldface**. Dell EMC reserves the rights to change the default properties.

Menu Item	Options	Description
Logical Processor	• **Enabled** • Disabled	Allows you to enable or disable the logical processors (Hyper-Threading Technology).
CPU Interconnect Speed	• **Maximum data rate** • 10.4 GT/s • 9.6 GT/s	This setting governs the frequency of the communication links among the CPUs in the system. Note that standard and basic bin processors support lower link frequencies than the advanced parts do. Maximum Data Rate indicates that the BIOS will run the communication links at the maximum frequency supported by the processors. You can also select specific frequencies that the processors support, which can vary.

		For best performance, you must select the Maximum Data setting. Any reduction in the communication link frequency will affect the performance of non-local memory accesses and cache coherency traffic. In addition, it can reduce access speed to non-local I/O devices from a particular CPU. However, if power saving considerations outweigh performance, you may want to reduce the frequency of the CPU communication links. If you do this, you must localize memory and I/O accesses to the nearest NUMA node to minimize the impact to system performance.
Virtualization Technology	• **Enabled** • Disabled	When this option is Enabled, BIOS will enable the processor virtualization features.
Adjacent Cache Line Prefetch	• **Enabled** • Disabled	Enables 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.
Hardware Prefetcher	• **Enabled** • Disabled	When enabled, the processor is able to prefetch extra cache lines for every memory request. This setting can affect performance based on the application and workloads running on the system and memory bandwidth utilization.
DCU Streamer Prefetcher	• **Enabled** • Disabled	Allows you to enable or disable the Data Cache Unit (DCU) streamer prefetcher. This setting can affect performance based on the application and workloads running on the system. Recommended for High Performance Computing applications.
DCU IP Prefetcher	• **Enabled** • Disabled	Allows you to enable or disable the Data Cache Unit (DCU) IP prefetcher. This setting can affect performance based on the application and workloads running on the system. Recommended for High Performance Computing applications.
Sub NUMA Cluster	• Enabled • **Disabled**	Sub NUMA Clustering (SNC) is a feature for breaking up the LLC into disjoint clusters based on address range, with each cluster bound to a subset of the memory controllers in the system. It improves average latency to the LLC.
UPI Prefetch	• **Enabled** • Disabled	UPI Prefetch is a mechanism to get the memory read started early on DDR bus, the UPI Rx path will spawn a MemSpecRd to iMC directly.
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 must only be enabled if the OS supports it. It uses the OS core parking algorithm and parks some of the logical processors in the system which in turn lets the corresponding processor cores transition into a lower power idle state.

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.
Dell Controlled Turbo	Enabled **Disabled**	Enables you to control 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. **Note**: Additional options such as "Controlled Turbo Limit Minus 1 Bin", "Controlled Turbo Limit Minus 2 Bins", and "Controlled Turbo Limit Minus 3 Bins" may be available if a valid DPAT 2.0 (Dell Processor Acceleration Technology 2.0) Enterprise license is installed on the system.
Number of Cores per Processor	• **All** • 1 • 2 • 4 • 6	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. Therefore, disabling cores to gain nominal performance enhancements must be carefully weighed prior to changing this setting from the default.
Processor Core Speed	N/A	Indicates the maximum non-turbo core frequency of the processor(s).
Processor Bus Speed	N/A	Indicates the bus speed of the processor(s).
Family-Model-Stepping	N/A	Indicates the family, model, and stepping of the processor.
Brand	N/A	Indicates the brand name provided by the processor manufacturer.
Level 2 Cache	N/A	Indicates the total size of L2 cache.
Level 3 Cache	N/A	Indicates the total size of L3 cache.
Number of Cores	N/A	Indicates the number of cores per processor.

1.4 SATA Settings

SATA Settings is available only on certain servers that support SATA devices. Enables you to change the SATA controller modes and view each port settings.

Note: The default option setting is depicted in **boldface**. Dell EMC reserves the rights to change the defaults.

Menu Item	Options	Description
Embedded SATA	• **AHCI Mode** • RAID Mode • Off	Enables you to set different modes for the embedded SATA controller(s). **Note**: Be careful when making changes to this field. The OS previously installed on the SATA hard drive 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 or not BIOS sends Security Freeze Lock command to the embedded SATA drives during POST. This option is applicable only to ATA and AHCI mode, not the RAID mode. Enabling this feature prevents 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.
Write Cache	• Enabled • **Disabled**	Allows you to enable or disable Write Cache on SATA drives during POST.
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. **Note**: In case of AHCI mode and RAID mode, this field is grayed out because the BIOS always enables the port.
Model	N/A	Indicates the drive model of the selected device.
Drive Type	N/A	Indicates the type of drive attached to the SATA port.
Capacity	N/A	Indicates the capacity of the hard drive. This field is undefined for removable media devices such as optical drives.

1.5 Boot Settings

Enables you to set the boot modes (BIOS vs UEFI) and specify the boot order.

Note: The default option setting is depicted in **boldface**. Dell EMC reserves the rights to change the default properties.

Menu Item	Options	Description
Boot Mode	• BIOS • **UEFI**	BIOS boot mode is used to boot devices installed with legacy OSs which do not follow the UEFI (Unified Extensible Firmware Interface) standard. If the OS supports UEFI, you can set this option to UEFI. **Note**: Switching the boot mode may prevent the server from booting if the OS 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 after every 30 seconds.
Hard Disk Failover	• Enabled • **Disabled**	If enabled, when attempting to boot the "Hard drive C" boot option, the BIOS will exhaust every hard drive controller in the Hard-disk Drive Sequence instead of just the first one in the list, before falling to the next boot option. **Note**: This option is applicable to BIOS boot mode only.
Boot Option Settings	N/A	Enables you to configure the boot sequence and the boot devices. Boot options can be enabled or disabled from this interface too.

1.6 Network Settings

Enables you to modify the UEFI PXE, iSCSI, and HTTP Boot device settings. 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: The Network Settings menu is available only in the UEFI boot mode. For BIOS boot mode, the network settings are handled by the network controllers option ROM (either by using the Configuration utility during option ROM initialization phase or from the Device Settings menu inside System Setup).

Note: The default option setting is depicted in **boldface**. Dell EMC 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.
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. Up to four PXE devices can be added to the UEFI boot sequence.
PXE Device (1,2,3,4) Settings	N/A	Enables you to control the configuration of the PXE device in UEFI boot mode. You can select the network interface, protocol (IPv4 vs. IPv6), and VLAN settings.
HTTP Device (1,2,3,4)	• Enabled • **Disabled**	Allows you to enable or disable the HTTP Boot device. When enabled, a UEFI HTTP boot option is created. Up to four HTTP boot devices can be added to the UEFI boot sequence.
HTTP Device (1,2,3,4) Settings	N/A	Enables you to control the configuration of the HTTP device in UEFI boot mode. You can select the network interface, the protocol (IPv4 vs. IPv6), VLAN settings, and URI.
iSCSI Initiator Name		Indicates the name of the iSCSI Initiator in IQN format.
iSCSI Device 1	• Enabled • **Disabled**	Allows you to enable or disable the iSCSI device. When enabled, a UEFI boot option is created for this device.
iSCSI Device 1 Settings	N/A	Allows you to control the configuration of iSCSI.

1.7 Integrated Devices

Enables you to view and configure the settings of all integrated devices in the system.

Note: The default option setting is indicates in **boldface**. Dell EMC reserves the rights to change the default properties.

Menu Item	Options	Description
User Accessible USB Ports	• **All Ports On** • Only Back Ports On • All Ports Off • All Ports Off (Dynamic)	Configures 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 device will still function in certain USB ports during the boot process, based on the selection. After the boot process is complete, the USB ports will be enabled or disabled as per the setting of the field. Selecting All Ports Off (Dynamic) disables all the front and back ports during POST, while allowing the front ports to be enabled or disabled dynamically by an authorized user without resetting the system. On the iDRAC GUI, click **System Settings → Hardware Settings → Front Ports**. **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.
iDRAC Direct USB Port	• **On** • Off	The iDRAC Direct USB port is managed by iDRAC exclusively with no host visibility. When set to Off, iDRAC will not detect any USB devices installed in this managed port.
Integrated RAID Controller	• **Enabled** • Disabled	Allows you to enable or disable the integrated RAID controller.
Integrated Network Card 1(2)	• **Enabled** • Disabled	Allows you to enable or disable the integrated network card (NDC). This option is available only to systems that support NDC. **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. **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.
Embedded Video Controller	• **Enabled** • Disabled	This field enables or disables the use of the Embedded Video Controller as the primary display. • 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. The 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 OS boots. **Note**: When there are multiple add-in graphics cards installed in the system, the one being discovered first during PCI enumeration will be selected as the primary video. You might have to re-arrange the cards in the slots in order to control with card is the primary video controller.
Current State of Embedded Video Controller	N/A	This is a read-only field, indicating the current state for the Embedded Video Controller. 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**	This field enables or disables BIOS configuration of Single Root I/O Virtualization (SR-IOV) devices. Enable this feature if you are booting to a virtualization OS that recognize SR-IOV devices.
OS Watchdog Timer	• Enabled • **Disabled**	If your system stops responding, this watchdog timer aids in the recovery of your OS. When this field is set to Enabled, the OS is allowed to initialize the timer. When is set to Disabled (the default), the timer will have no effect on the system.
Memory Mapped I/O above 4GB	• **Enabled** • Disabled	This field helps in enabling support for PCIe devices that require large amount of MMIO resources. Enable this option only for 64-bit OSs.
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 OS or causing delays or lockups in system startup.

		If the slot is disabled, both the Option ROM and UEFI driver are disabled. The card is not enumerated on the PCI bus and won't be available to the OS. 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 cannot boot from the card, and its pre-boot services are also not available. However, the card is available to the OS. **Note**: This option is not available if the slot contains a Dell EMC 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 the option ROM and UEFI driver do not run, select Boot Driver Disabled for all the cards from the same manufacturer (including its integrated device versions such as NDCs).
Slot Bifurcation	N/A	Enables configuration of how the PCIe slots are bifurcated.
Auto Discovery Bifurcation Settings	• Platform Default Bifurcation • Auto Discovery of Bifurcation • Manual Bifurcation Control	Enables BIOS to dynamically scan for PCIe devices rather than relying strictly on system slot definitions. • The Platform Default setting will strictly follow the system slot definitions when configuring each PCIe slot. • The Auto Discovery setting will analyze the installed PCIe cards and determine the correct configuration for each slot. This may include bifurcation of the slot for multiple devices. • Manual Control allows the user to override bifurcation settings for each slot. CAUTION: Improper configuration of PCIe slots can prevent the system from functioning properly.

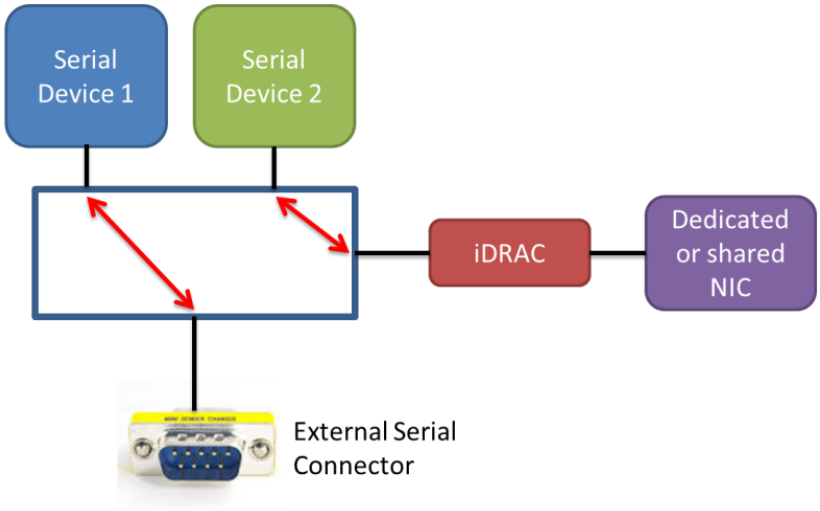
1.1 Serial Communication

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

Note: The default option setting is depicted in **boldface**. Dell EMC reserves the rights to change the default properties.

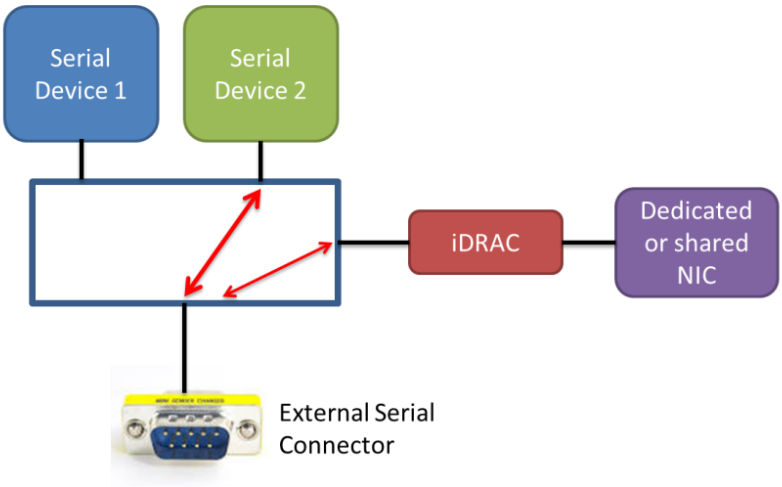
Menu Item	Options	Description
Serial Communication	• On without Console Redirection • **Auto** • On with Console Redirection via COM1 • On with Console Redirection via COM2 • Off	Configures the BIOS serial console redirection feature, and determines which serial port address would be used (COM1 = 0x3F8, COM2 = 0x2F8). Auto option will enable BIOS console redirection for the selected device and port address if a terminal is detected during system startup.
Serial Port Address	• Serial Device1=COM1,Serial Device2=COM2 • **Serial Device1=COM2,Serial Device2=COM1**	Enables you to set the port address for serial devices. **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	Associates the External Serial Connector to Serial Device 1, Serial Device 2 or the Remote Access Device. **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 6, 7, and 8).
Failsafe Baud Rate	• **115200** • 57600 • 19200 • 9600	Enables you to set the failsafe baud rate for the console redirection. BIOS attempts to negotiate and determine the serial baud rate automatically during POST. In case of SOL, BIOS gets 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.
Remote Terminal Type	• **VT100/VT220** • ANSI	Enables 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).
Redirection After Boot	• **Enabled** • Disabled	Allows you to enable or disable the BIOS console redirection after the OS is loaded.

The following pictures depict the different serial MUX modes for serial communications:



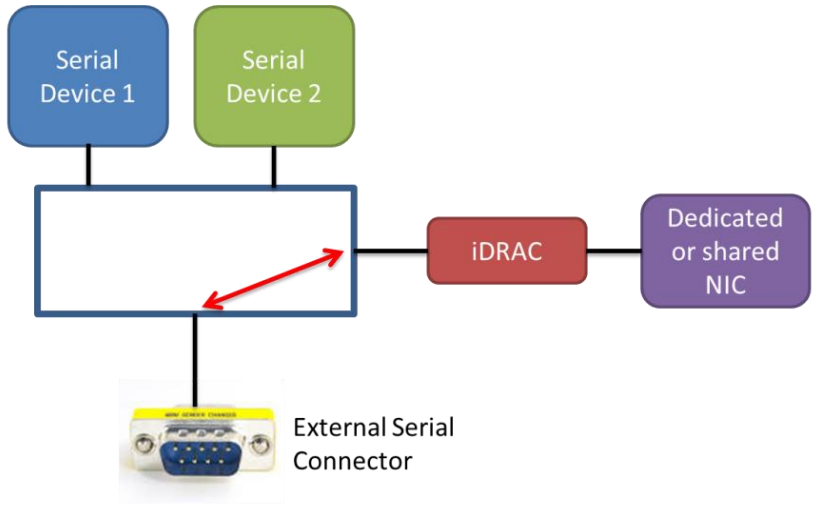
External Serial Connector is set to Serial Device 1. The serial MUX enables concurrent Serial over LAN (SOL) access and external serial connector access to host.

Figure 6 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.

Figure 7 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.

Figure 8 External Serial Connector set to Remote Access Device

Note: After console redirection is enabled and active, the BIOS Setup utility interface will operate in text mode (TUI).

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

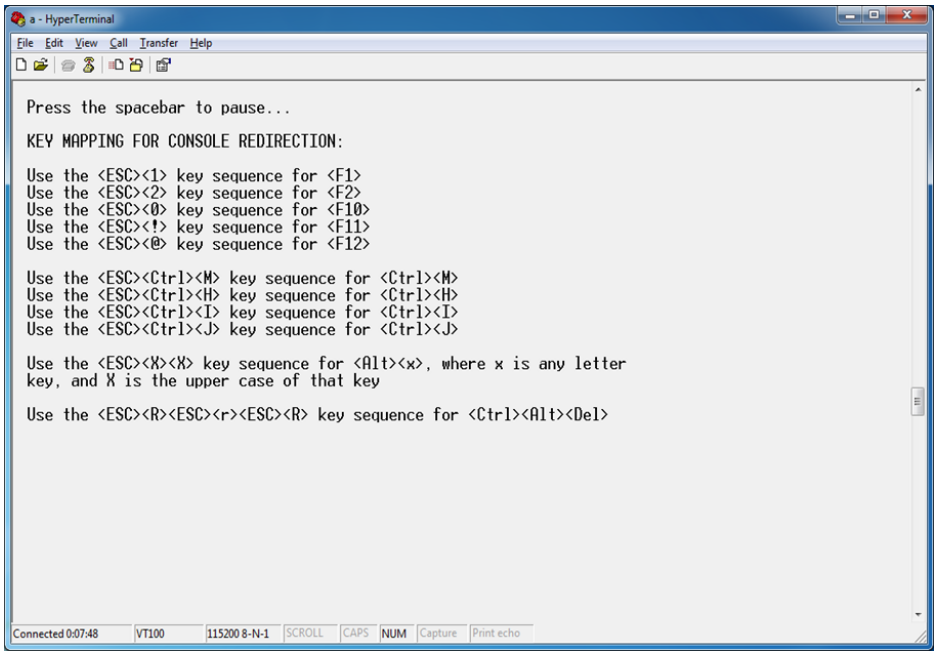


Figure 9 Key mapping for console redirection

1.8 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: The default option setting is depicted in **boldface**. Dell EMC reserves the rights to change the default properties.

Menu Item	Options	Description
System Profile	• **Performance per Watt (DAPC)** • Performance per Watt (OS) • Performance • Workstation Performance • Custom	Enables you to set the system profile. When set to a mode other than Custom, BIOS will pre-set each option accordingly. When set to Custom, you can change the setting of each option. **Performance Per Watt Optimized (DAPC)** Enables 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. The BIOS also manages system Power Capping in this mode. **Performance Per Watt Optimized (OS)** In this mode, the CPU Power Management field is set to OS DBPM. Implies that the OS controls the processor's power management. The main controls are the processor frequency or performance states (aka P-states, P0, P1…Pn), and the processor clock throttling (aka 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	DAPC
CPU Power Management	System DBPM (DAPC)
Memory Frequency	Maximum Performance
Turbo Boost	Enabled
C1E	Enabled
C States	Enabled
Write Data CRC	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
CPU Interconnect Bus Link Power Management	Enabled
PCI ASPM L1 Link Power Management	Enabled

Settings	OS control
CPU Power Management	OS DBPM
Memory Frequency	Maximum Performance
Turbo Boost	Enabled
C1E	Enabled
C States	Enabled
Write Data CRC	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
CPU Interconnect Bus Link Power Management	Enabled
PCI ASPM L1 Link Power Management	Enabled

Performance
In 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
C1E	Disabled
C States	Disabled
Write Data CRC	Disabled
Memory Patrol Scrub	Standard
Memory Refresh Rate	1x
Uncore Frequency	Maximum
Energy Efficient Policy	Performance
Number of Turbo Boost Enabled Cores for Processor x	All
Monitor/Mwait	Enabled
CPU Interconnect Bus Link Power Management	Disabled
PCI ASPM L1 Link Power Management	Disabled

<table>
<tr>
<td></td>
<td></td>
<td>Workstation Performance

<table>
<tr><th>Settings</th><th>Performance</th></tr>
<tr><td>CPU Power Management</td><td>Maximum Performance</td></tr>
<tr><td>Memory Frequency</td><td>Maximum Performance</td></tr>
<tr><td>Turbo Boost</td><td>Enabled</td></tr>
<tr><td>C1E</td><td>Disabled</td></tr>
<tr><td>C States</td><td>Enabled</td></tr>
<tr><td>Write Data CRC</td><td>Disabled</td></tr>
<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>
<tr><td>CPU Interconnect Bus Link Power Management</td><td>Disabled</td></tr>
<tr><td>PCI ASPM L1 Link Power Management</td><td>Disabled</td></tr>
</table>

Custom
In this mode, you can change the settings of individual options. The following sections will describe each option in details.</td>
</tr>
<tr>
<td>CPU Power Management</td>
<td>• System DBPM (DAPC)
• Maximum Performance
• OS DBPM</td>
<td>Enables you to set the CPU power management mode.

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

• The OS DBPM (Demand Based Power Management) means that it is the OS that controls the processor's power management.

Maximum Performance mode keeps the processor running at the highest frequency all the time.</td>
</tr>
<tr>
<td>Memory Frequency</td>
<td>• Maximum Performance
• 2133MHz
• 1866MHz

• Maximum Reliability</td>
<td>The speed at which the memory bus operates at. The maximum possible frequency in the system may not be the maximum frequency rated on the installed DIMM.

The maximum memory bus frequency depends on 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.</td>
</tr>
</table>

		Under the Custom menu, a memory frequency can be selected to the required 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.
Turbo Boost	• **Enabled** • Disabled	If the current operating environment allows, the Turbo Boost mode allows the processor to engage to a higher frequency than the processor's nominal or rated frequency. 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.
C1E	• **Enabled** • Disabled	Allows you to enable or disable the processor to switch to C1E (Enhanced Halt State) when it is idle.
C States	• **Enabled** • Disabled	Allows you to enable or disable the processor to operate in all available power states.
Write Data CRC	• **Enabled** • Disabled	When set to Enabled, DDR4 data bus issues are detected and corrected during 'write' operations. Two extra cycles are required for CRC bit generation which impacts the performance.
Memory Patrol Scrub	• Extended • **Standard** • Disabled	Patrol Scrubbing is a feature that searches the memory for errors and repairs correctable errors to prevent the accumulation of memory errors. • When set to Disabled, no Patrol Scrubbing will occur. • When set to Standard mode, the entire memory array will be scrubbed once in a 24 hour period. • When set to Extended mode, the entire memory array will be scrubbed every hour to further increase system reliability.
Memory Refresh Rate	• **1x** • 2x	The memory controller will periodically refresh the data in 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.
Uncore Frequency	• **Dynamic** • Maximum	Selects 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.
Energy Efficient Policy	• Performance • **Balanced Performance** • Balanced Energy • Energy Efficient	Selects 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.
Number of Turbo Boost Enabled	All	Enables you to control the number of Turbo Boost enabled cores for processor 1(2, 3, and 4). By default, the maximum number of cores is enabled.

Cores for Processor 1(2,3,4)		
Monitor/Mwait	• **Enabled** • Disabled	Enables you to enable/disable the Monitor/Mwait instructions of the processor. When set to disabled, these two instructions are not supported by the processor. **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 or performance.
CPU Interconnect Bus Link Power Management	• **Enabled** • Disabled	When enabled, CPU interconnect bus link power management can reduce overall system power a bit while slightly reducing system performance.
PCI ASPM L1 Link Power Management	• **Enabled** • Disabled	When enabled, PCIe Advanced State Power Management (ASPM) can reduce overall system power a bit while slightly reducing system performance. **Note**: Some devices may not perform properly (they may stop responding or cause the system to stop responding) when ASPM is enabled. Therefore, L1 will only be enabled for validated qualified cards.

1.9 System Security

System Security page allows you to perform specific security-related functions such as setting passwords, managing TPM, and enabling or disabling power or NMI buttons.

Note: The default option setting is depicted in **boldface**. Dell EMC reserves the rights to change the default properties.

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 by using the Advanced Encryption Standard Instruction Set.
System Password	N/A	Enables you to set the system password which is the password that you must enter to allow the system to boot to an OS. This option is read-only if the password jumper (PWRD_EN) is not installed in the system. A password must have up to a maximum of 32 characters.
Setup Password	N/A	Enables you to set the Setup password. The Setup password is the one 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 server. A password must have up to a maximum of 32 characters.
Password Status	• **Unlocked** • Locked	Locks the system password. To prevent the system password from being modified, set this option to locked and enable Setup password. This field also prevents the system password from being disabled by the user while the system is booting.
TPM Security (with TPM 1.2 installed)	• **Off** • On with Pre-boot Measurements • On without Pre-boot Measurements	Enables you to control the reporting of the Trusted Platform Module (TPM). • When set to Off, the presence of the TPM is not reported to the OSs. • When set to On with Pre-boot Measurements, BIOS will store 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 will bypass pre-boot measurements. The TPM chip is still visible to the OS in this case.
TPM Security (with TPM 2.0 installed)	• **Off** • On	Enables you to control the reporting of the Trusted Platform Module (TPM). When set to Off, the presence of the TPM is not reported to the OS. When set to On, BIOS will store 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.
TPM Information	N/A	Indicates the type of TPM. This field displays **Unknown** if TPM Security is set to Off.
TPM Firmware	N/A	Indicates the TPM firmware version.
TPM Status (TPM 1.2 only)	N/A	Indicates the current status of the TPM.
TPM Command (TPM 1.2 only)	• **None** • Activate • Deactivate • Clear	This field allows you to control the Trusted Platform Module (TPM). • When set to None, no command is sent to the TPM. • When set to Activate, the TPM will be enabled and activated. • When set to Deactivate, the TPM will be disabled and deactivated. • When set to Clear, all the contents of the TPM will be cleared. WARNING: Clearing the TPM will cause loss of all the keys in the TPM. This could affect booting to the OS. **Note**: This field is read-only when TPM Security is set to Off. The action requires an additional reboot before it can become effective.
TPM Hierarchy *(TPM 2.0 only)*		Allows enabling, disabling, or clearing the storage and endorsement hierarchies. • When set to Enabled, the storage and endorsement hierarchies can be used. • When set to Disabled, the storage and endorsement hierarchies cannot be used. • When set to Clear, the storage and endorsement hierarchies are cleared of any values, and then reset to Enabled.
TPM PPI Bypass Provision	• Enabled • **Disabled**	When set to Enabled, allows the OS to bypass Physical Presence Interface (PPI) prompts when issuing PPI Advanced Configuration and Power Interface (ACPI) provisioning operations.

TPM PPI Bypass Clear	• Enabled • **Disabled**	When set to Enabled, allows the OS to bypass Physical Presence Interface (PPI) prompts when issuing PPI Advanced Configuration and Power Interface (ACPI) clear operations.
TPM2 Algorithm Selection *(TPM2.0 only)*	• SHA1 • SHA256 • SM3 (if TPM supports it)	Enables or disables Trusted Execution Technology. To enable Intel(R) TXT, Virtualization Technology must be enabled, TPM Security must be On, and TPM2 Algorithm must be SHA256.
Intel TXT	• **Off** • On	Allows you to enable or disable the Intel Trusted Execution Technology (TXT). To enable Intel TXT the following must be set: TPM 1.2 • Virtualization Technology must be enabled • TPM Security must be "On with Pre-boot Measurements • TPM Status must be "Enabled, Activated" TPM 2.0 • Virtualization Technology must be enabled • TPM Security must be On • TPM2 Algorithm Selection must be set to SHA256
Power Button	• **Enabled** • Disabled	Allows you to enable or disable the power button on the front panel.
AC Power Recovery	• **Last** • On • Off	Specifies how the system will react after AC power has been restored to the system. It is especially useful for people who turn their systems off with a power strip. • When set to Off, the system will stay off after AC is restored. • When set to On, the system will turn on after AC is restored. • When set to Last, the system will turn on if the system was on when AC was lost. The system will remain off if the system was off when AC was lost. In the case of an ungraceful shutdown, the system will always turn on.
AC Power Recovery Delay	• **Immediate** • Random • User Defined	This field specifies how the system will support the staggering of power-up after AC power has been restored to the system. • When set to Immediate, there is no delay for power-up. • When set to Random, the system will create a random delay for power-up. • When set to User Defined, the system will delay power-up by that amount. The system supported user defined power-up delay.

User Defined Delay	N/A	This field controls the user-defined AC Recovery Delay. Enter a delay in the range of 60s to 240s. In the future, this may increase to 600 seconds (10 minutes).
UEFI Variable Access	• **Standard** • Controlled	This field provides varying degrees of securing UEFI variables. When set to Standard, UEFI variables are accessible in the OS based on 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.
In-Band Manageability Interface	• **Enabled** • Disabled	When set to Disabled, this setting will hide the Management Engine's (ME) HECI devices and the system's IPMI devices from the OS. This prevents the OS from changing the ME power capping settings, and blocks access to all in-band management tools. All management must be managed by using the out-of-band technique. **Note**: BIOS update requires HECI devices to be operational and DUP updates require IPMI interface to be operational. This setting needs to be set to Enabled to avoid update errors.
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 **Note**: Secure Boot is not available unless the Boot Mode (in the Boot Settings menu) is UEFI. **Note**: Secure Boot is not available unless the "Load Legacy Video Option ROM" setting (in the Miscellaneous Settings menu) is disabled. **Note**: A Setup password is recommended to be enabled for Secure Boot.
Secure Boot Policy	• **Standard** • Custom	When Secure Boot Policy is Standard, the BIOS uses the system manufacturer's key and certificates to authenticate pre-boot images. When Secure Boot Policy

		is Custom, the BIOS uses the user-customized key and certificates. **Note**: If Custom mode is selected, the Secure Boot Custom Policy Settings menu is displayed. **Note**: Changing the default security certificates may cause the system to fail booting from certain boot options.
Secure Boot Mode	• User mode • **Deploy Mode**	Configures how the BIOS uses the Secure Boot Policy Objects (PK, KEK, db, and dbx). In Setup Mode and Audit Mode, PK is not present, and BIOS does not authenticate programmatic updates to the policy objects. In User Mode and Deployed Mode, PK is present, and BIOS performs signature verification on programmatic attempts to update policy objects. Deployed Mode is the most secure mode. Use Setup, Audit, or User Mode when provisioning the system, then use Deployed Mode for normal operation. Available mode transitions depend on the current mode and PK presence. For more information about transitions between the four modes, see Figure 77 in the UEFI 2.6 specification. In Audit Mode, the BIOS performs signature verification on pre-boot images and logs results in the Image Execution Information Table, but executes the images whether they pass or fail verification. Audit Mode is useful for programmatically determining a working set of policy objects.
Secure Boot Policy Summary	N/A	View the list of certificates and hashes that Secure Boot uses to authenticate images. It shows 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	Enables you to configure the Secure Boot Custom Policy. A user can enroll and delete the PK, KEK, db, and dbx entries.

1.10 Redundant OS Control

Redundant OS Control page allows you to configure the Redundant OS feature, which allows installing an OS on a specified drive, and then hiding that drive until required.

Note: The default option setting is depicted in **boldface**. Dell EMC reserves the rights to change the default properties.

Menu Item	Options	Description
Redundant OS Location	- **None** - Internal SD Card - SATA Port A - SATA Port B - SATA Port C - SATA Port D - SATA Port E - SATA Port F - SATA Port G - SATA Port H - SATA Port I - SATA Port J - SATA Port K - SATA Port L - SATA Port M - SATA Port N - Internal M.2 Drive Slot 1 - Internal M.2 Drive Slot 2 - Internal M.2 Drive Slot 3 - Internal M.2 Drive Slot 4 - Internal M.2 Drive Slot 5 - Internal M.2 Drive Slot 6 - Internal M.2 Drive Slot 7 - Internal M.2 Drive Slot 8 - Internal M.2 Drive Slot 9 - Internal M.2 Drive Slot 10 - Internal M.2 Drive Slot 11 - Internal M.2 Drive Slot 12 - Internal M.2 Drive Slot 13 - Internal M.2 Drive Slot 14 - Internal USB - Internal M.2 Drive	Specifies the backup device for the Redundant OS Control feature. When Redundant OS Boot is set to Enabled, the BIOS will boot to this device. **Note**: In order for the devices and slots listed here to be displayed as optional backup devices, their settings must be as specified here: • SD Card Port – On • Internal USB Port – On • Embedded SATA – anything other than Off • PCIe Slot Disablement – Enabled
Redundant OS State	- **Visible** - Hidden	When set to Hidden, the device specified by Redundant OS Location is hidden. It will not be visible in the OS or the BIOS boot sequence.
Redundant OS Boot	- **Enabled** - Disabled	When set to Enabled, the BIOS will boot to the device specified by Redundant OS Location.

1.11 Miscellaneous Settings

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

Note: The default option setting is depicted in **boldface**. Dell EMC reserves the rights to change the default properties.

Menu Item	Options	Description
System Time	N/A	Enables you to set the time on the system.
System Date	N/A	Enables 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.
F1/F2 Prompt on Error	• **Enabled** • Disabled	Enables you to specify the BIOS behavior on certain POST errors. By default F1/F2 Prompt on Error is enabled, which implies that when the system will stop responding at the end of POST waiting for user input after having an error during bootup. If set to disabled, the BIOS displays the warning or error message on the screen and continues booting to the OS. **Note**: For certain catastrophic errors, even if this field is set to Disabled, BIOS may still prompt F1, F2, F10, or F11 during POST.
Load Legacy Video Option ROM	• Enabled • **Disabled**	Indicates whether or not the system BIOS will load the legacy video (INT10h) option ROM from the video controller. Select Enabled if the OS (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 OSs, this field is recommended to be left as default (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 set to Enabled if UEFI Secure Boot is enabled.
Dell Wyse P25/P45 BIOS Access	• **Enabled** • Disabled	Enables or disables Remote user to access BIOS Setup via Dell Wyse P25/P45 Portal. If P25/P45 BIOS Access is turned off, it cannot be turned back on remotely from the P25/P45. Turning this feature off will also prevent keyboard and mouse access to Diagnostics, Boot Options, and other Pre-OS functionality.

Power Cycle Request	• **None** • Full Power Cycle	Specifies how the system reacts when system transitions to S5 state. When set to None, the transition to S5 is normal. When set to Full Power Cycle, the system will temporarily be forced into a lower power state, similar to removing and replacing AC.

Conclusion

Dell EMC provides its customers with products that simplify and streamline their IT processes, freeing administrator's time to focus on activities that help grow the business. The PowerEdge System Setup utility is one such capability, speeding the configuration of BIOS, iDRAC, and device settings of your servers. System Setup provides a one-stop solution for configuring your business-critical server settings helping you achieve optimal bandwidth, power, security, memory, and processor utilization.

This technical white paper provides comprehensive information concerning the server attributes that are managed by System Setup. To maximize utilization, special notes and cautions are specified, where necessary. It provides Screen shots and architecture diagrams to enhance readability and tabulated descriptions that enable you to rapidly identify items of interest. For more information about different Dell EMC PowerEdge servers, see the brochure at http://www.dell.com/downloads/global/products/pedge/en/pedge-portfolio-brochure.pdf.

A Technical support and resources

- Dell.com/support is focused on meeting customer needs with proven services and support.
- Dell TechCenter is an online technical community where IT professionals have access to numerous resources for Dell EMC software, hardware and services.