DELL Technologies

Technical White Paper

# Setting up BIOS on 15th Generation (15G) Dell EMC PowerEdge Servers


## Abstract

This Dell EMC technical white paper describes the BIOS attributes that you can use to manage and customize your Dell EMC 15G PowerEdge servers. It also defines the fields used in configuring these attributes and best practices for defining values in each field, where appropriate.



August 2021

# Revisions

| Date | Description |
|---|---|
| March 2018 | Initial release by Wei Liu, Mark Shutt, and Paul Rubin |
| July 2018 | Added info about the Persistent Memory feature |
| August 2021 | Added 15G system setup items |

# Authors

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

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 © 2021 Dell Inc. or its subsidiaries. All Rights Reserved. Dell Technologies, Dell, EMC, Dell EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners. [8/24/2021] [Technical White Paper] [508]

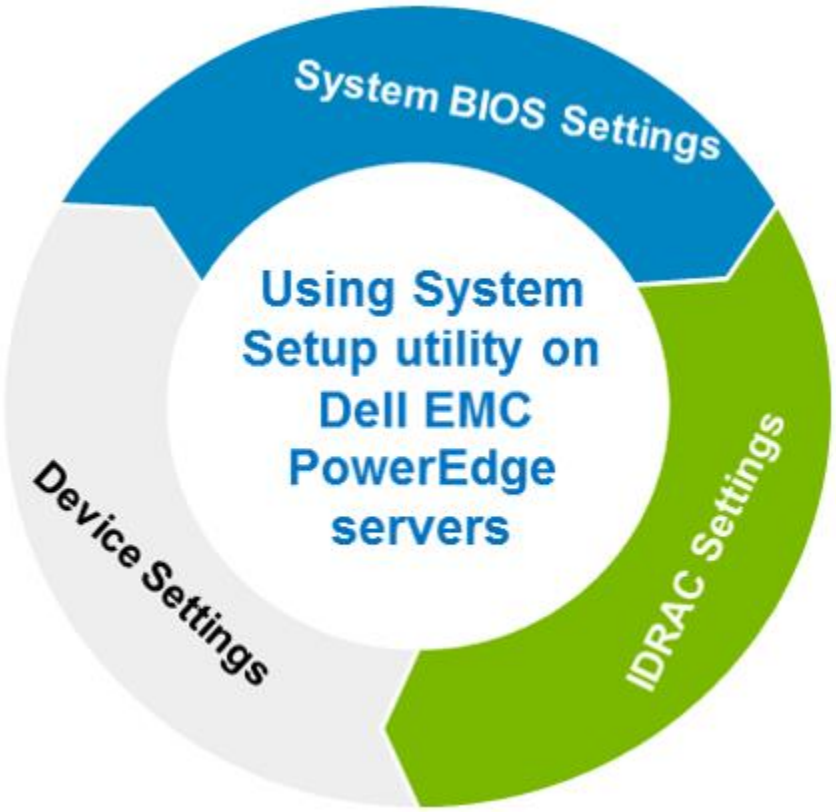
# Table of contents

# Acronyms

| Acronym | Expanded form |
|---|---|
| **ACPI** | Advanced Configuration and Power Interface |
| **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 |
| **Intel PMEM** | Intel Persistent Memory |
| **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 15th generation (15G) 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.

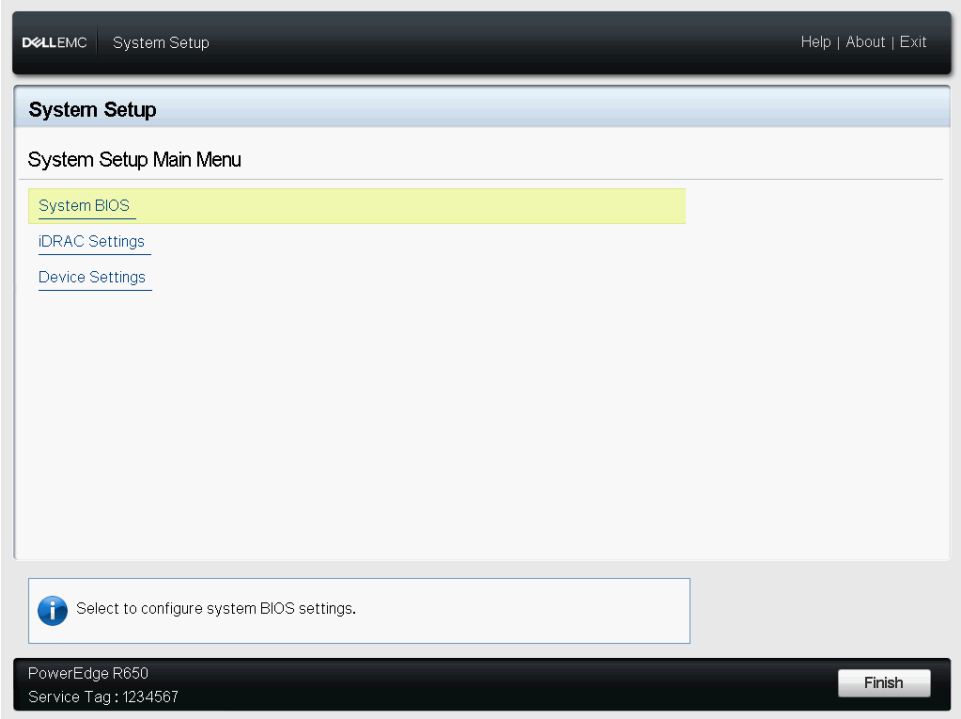



Figure 1 Graphical Browser mode of System Setup

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

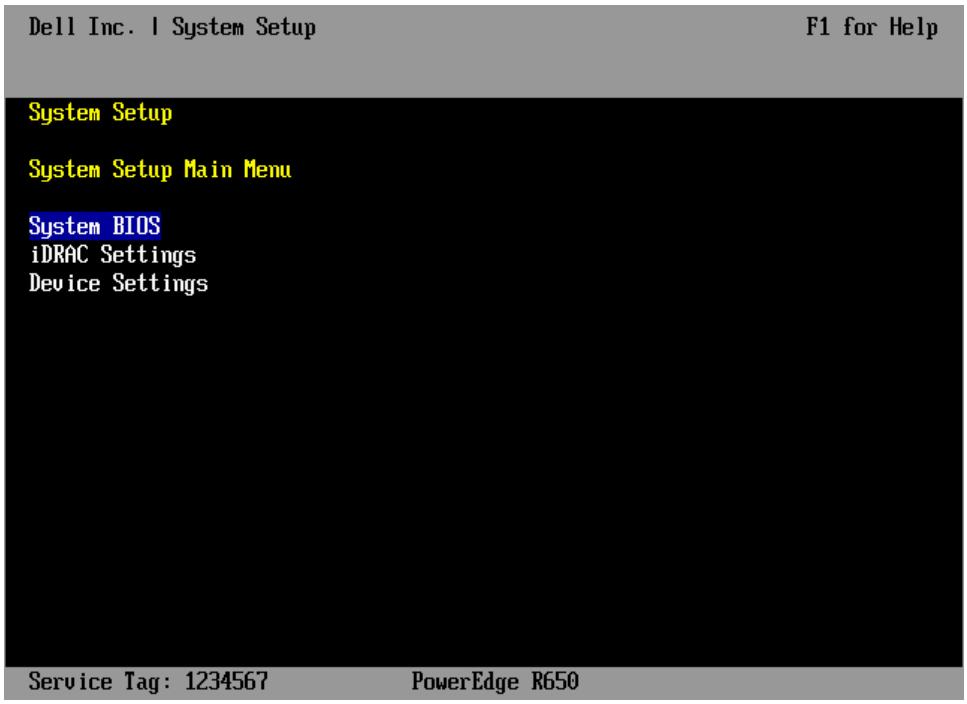



Figure 2 Text Browser mode of the System Setup

# Starting System Setup

There are multiple ways to start the System Setup utility:

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

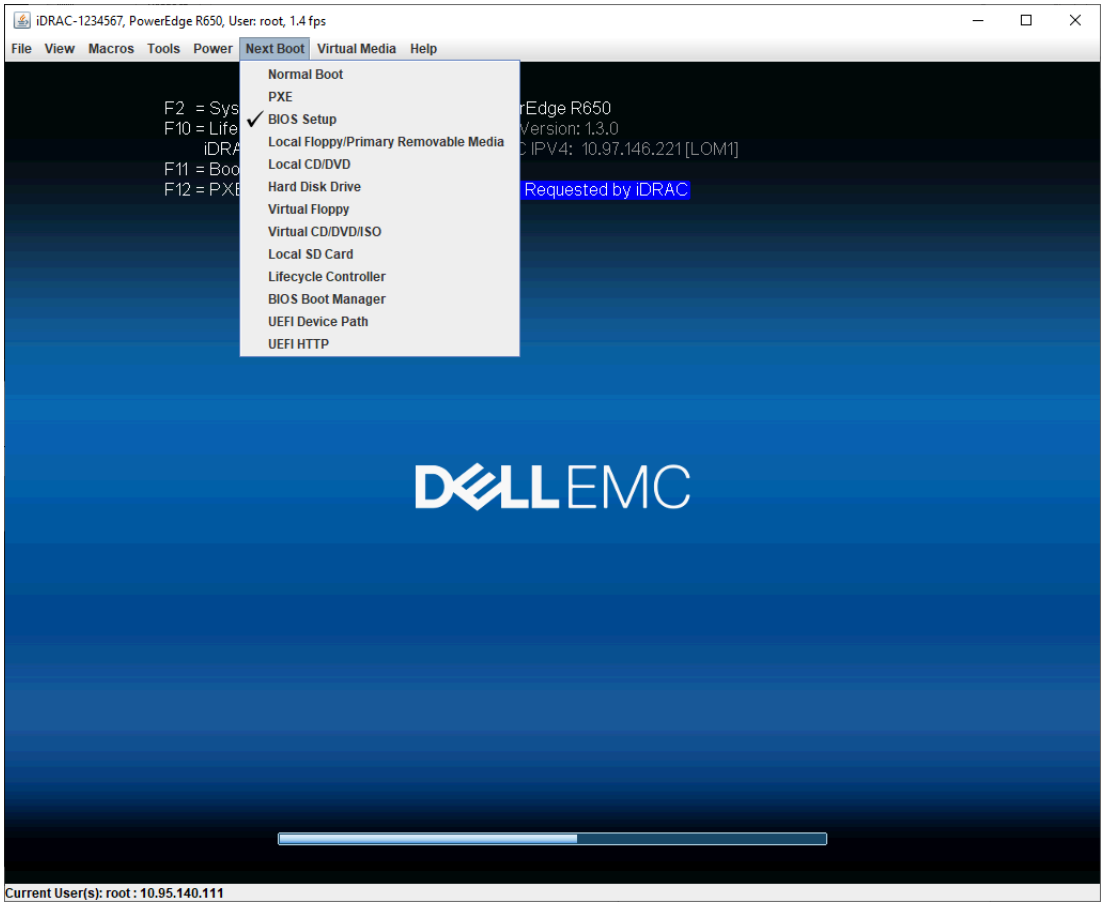



Figure 3 Start System Setup from iDRAC virtual console

- To open System Setup by using Lifecycle Controller, select **System Setup** in the Lifecycle Controller interface page.

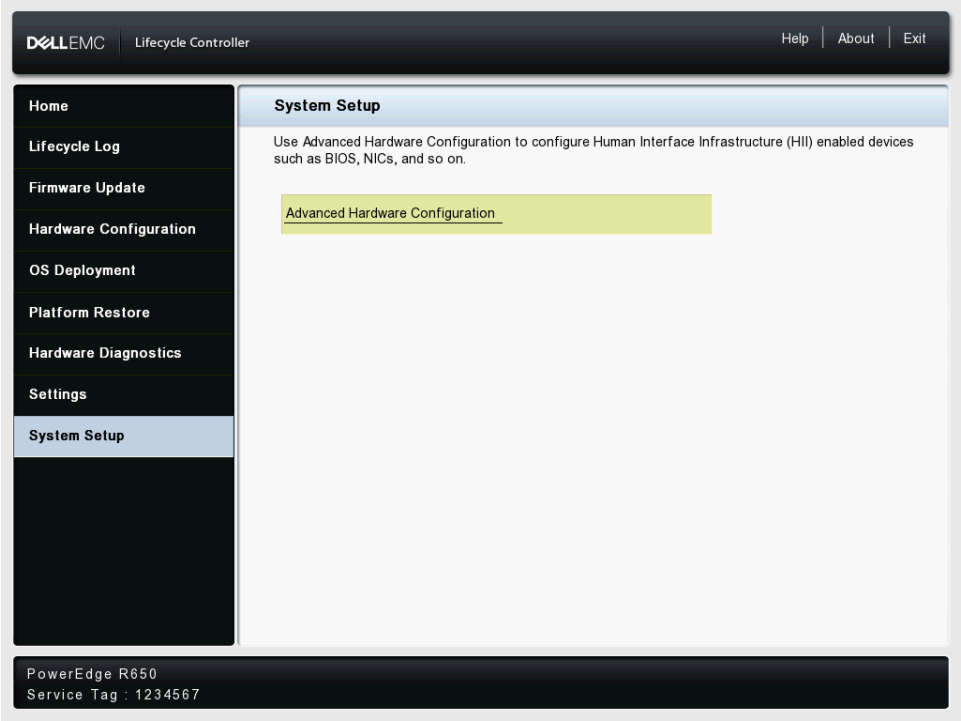



Figure 4 Start System Setup from Lifecycle Controller

# 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. |
| **Persistent Memory** | Enables the Persistent Memory when the Non-Volatile DIMM is selected. |
| **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 BIOS—System Information

The System information page lists system properties such as Service Tag and BIOS revision. This page is read-only.

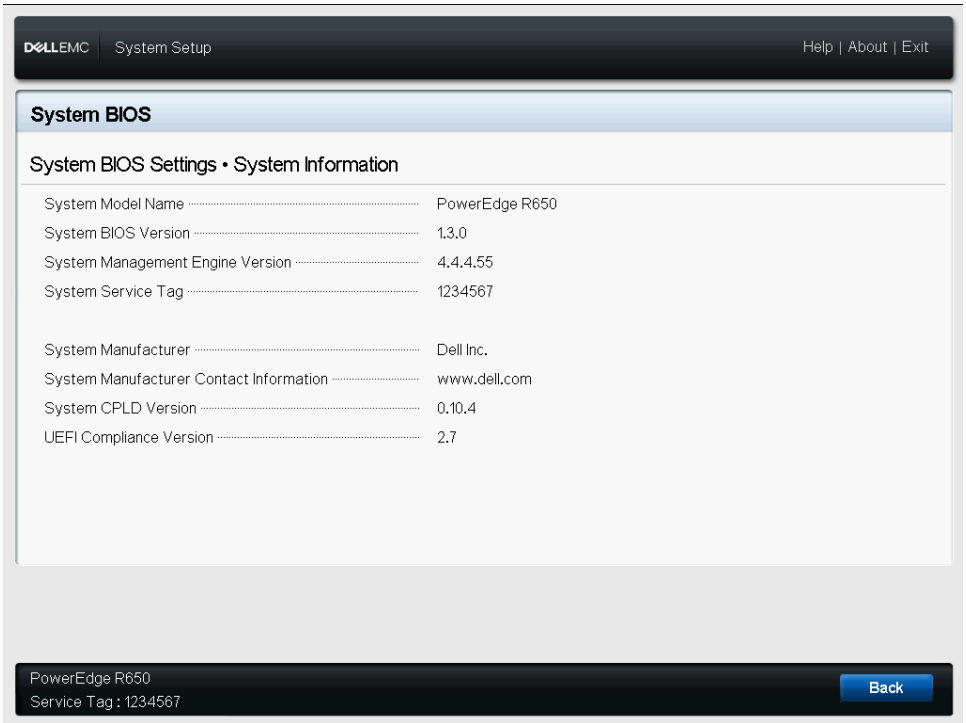



Figure 5 The System Information page

## 1.2 System BIOS—Memory Settings

The Memory Settings page 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. |

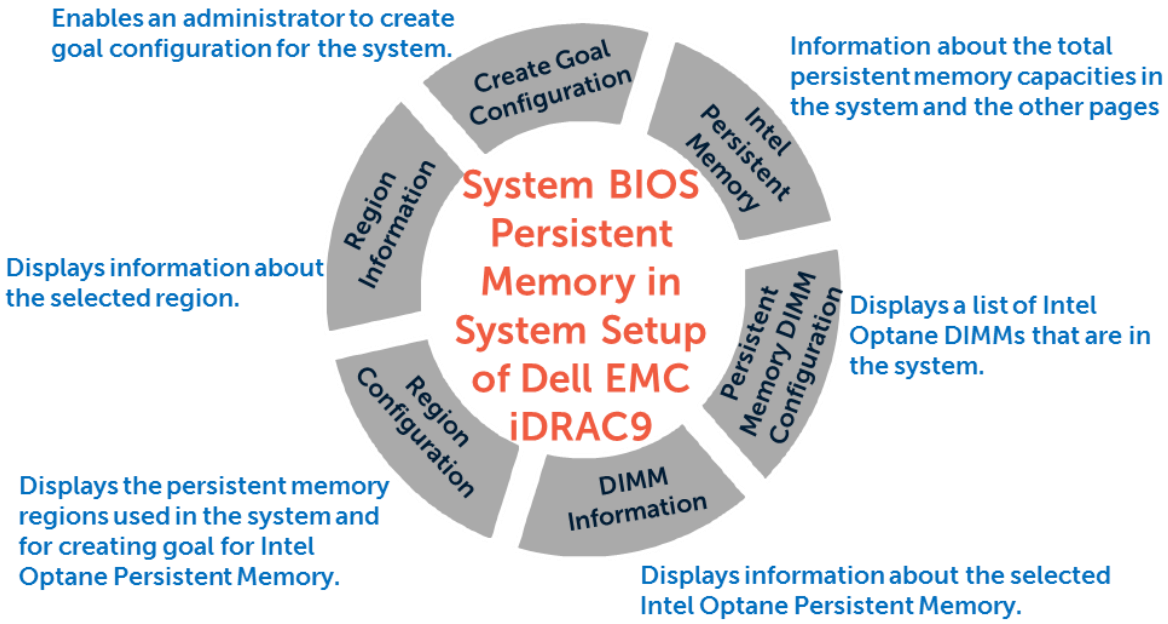
| Menu Item | Options | Description |
|---|---|---|
| **System Memory Testing** | • Enabled<br>• Disabled | Specifies whether the BIOS software-based system memory tests are conducted during POST.<br>When set to Enabled, the memory tests are performed, and test results are displayed on the screen.<br><br>Note: Enabling results in a longer boot time. The extent of the increase depends on the amount of memory installed in the system.<br><br>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. |
| **Dram Refresh Delay** | • Performance<br>• **Minimum** | By enabling the CPU memory controller to delay running the REFRESH commands, you can improve the performance for some workloads. By minimizing the delay time, it is ensured that the memory controller runs the REFRESH command at regular intervals. For Intel-based servers, this setting only affects systems configured with DIMMs which use 8 Gb density DRAMs. |
| **Memory Operating Mode** | • **Optimizer Mode**<br>• Dell Fault Resilient Mode | This field selects the memory operating mode. This feature is active only if a valid memory configuration is detected.<br>When Optimizer Mode is enabled, the DRAM controllers operate independently in 64-bit mode and provide optimized memory performance.<br>When Dell Fault Resilient Mode (FRM) is enabled, a percentage of the total installed memory is configured to create a fault resilient zone starting from lowest system memory address for use by select hypervisors for host virtualization resilience. Specify the FRM percentage by using the Fault Resilient Mode Memory Size[%] feature.<br>When Dell NUMA Fault Resilient Mode (FRM) is enabled, a percentage of the installed memory in every NUMA node is configured to create a fault resilient zone for use by select hypervisors for host virtualization resilience. Specify the FRM percentage by using the Fault Resilient Mode Memory Size[%] feature. |
| **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. |
| **Fault Resilient Mode Memory Size[%]** | • **25**<br>• 12.5 | Select to define the percent of total memory size that must be used by the fault resilient mode, when selected in the Memory Operating mode. When Fault Resilient Mode is not selected, this option is grayed out and not used by Fault Resilient Mode. |
| **Memory Interleaving** | • **Auto**<br>• Disabled | When Enabled, memory interleaving is supported if a symmetric memory configuration is installed. When set to Disabled, the system supports Non-Uniform Memory Access (NUMA) (asymmetric) memory configurations. |

| | | |
|---|---|---|
| | | 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. Die and Socket Interleaving should only be enabled for Operating Systems that are not NUMA aware.<br><br>**Note:** This option is only available on systems with AMD processors. |
| **Node Interleaving** | • Enabled<br>• **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.<br><br>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. |
| **ADDDC Setting** | • **Enabled**<br>• Disabled | When Adaptive Double DRAM Device Correction (ADDDC) is enabled, failing DRAMs are dynamically mapped out. This action can have some impact on system performance under certain workloads. This feature only applies to x4 DIMMs, and when Fault Resilient Mode (FRM) is disabled.<br><br>**Note:** This option is only available on systems with Intel processors. |
| **Memory Map Out** | N/A | This field controls DIMMs slots on the system. |
| **Memory Training** | • **Fast**<br>• Retrain at Next Boot<br>• Enable | Fast - Use previously saved memory training parameters to train the memory subsystem when memory configuration is not changed. System boot time is reduced when memory configurations is not changed. If memory configuration is changed, system automatically enables "Retrain at Next Boot" to force one-time full memory training steps, and then go back to "Fast" afterward.<br>Retrain at Next Boot - Force one-time full memory training steps at next system power on. System boot time is slowed on next boot.<br>Enable - Force full memory training steps on every system power on. System boot time is slowed on every boot.<br><br>**Note:** This option is only available on systems with Intel processors. |

| Menu Item | Options | Description |
|---|---|---|
| **Correctable Memory ECC SMI** | • Enabled<br>• Disabled | Allows the system to log ECC corrected DRAM errors into the SEL log. Logging these rare errors can help identify marginal components; however, the system will pause for a few milliseconds after an error while the log entry is created. Latency conscious customers may wish to disable the feature. Spare Mode, and Mirror mode require this feature to be enabled. |
| **Opportunistic Self-Refresh** | • Enabled<br>• **Disabled** | When set to Enabled, the Integrated Memory Controllers (IMCs) may go into self-refresh when it is idled for a period.<br><br>**Note:** This option is only available on systems with AMD processors. |
| **Correctable Error Logging** | • **Enabled**<br>• Disabled | Enable/Disable logging of correctable memory threshold error. |

## 1.3 System BIOS—Persistent Memory

The Persistent Memory page is the main page for saving the Persistent Memory settings. When Intel Optane Persistent Memory is populated, the **Intel Persistent Memory** page is displayed. If an NVDIMM-N is detected in the system, the **NVDIMM-N Persistent Memory** page is displayed.




| Menu Item | Options | Description |
|---|---|---|
| **Persistent Memory Scrubbing** | • **Auto**<br>• One Shot<br>• Enable<br>• Disable | Set the Persistent Memory Scrubbing mode to any one of the following:<br>• Auto: System automatically scrubs persistent memory during BIOS POST when a multi-bit error is detected.<br>• One Shot: System scrubs the persistent memory during BIOS POST on the entire persistent memory range. During the next boot operation, system reverts to the Auto-persistent memory mode.<br>• Enable: System scrubs the entire persistent memory range during BIOS POST after every boot operation.<br>• Disable: System never scrubs the persistent memory range.<br>**Note**: Based on the system memory population, scrubbing a persistent memory on the entire persistent memory range can take more than 60 minutes during BIOS POST. |

### 1.3.1 System BIOS—Intel Persistent Memory

The Intel Persistent Memory page is the main page for Intel Optane Persistent Memory which displays information about the total persistent memory capacities in the system and the other pages such as Persistent Memory DIMM configuration and Region Configuration.

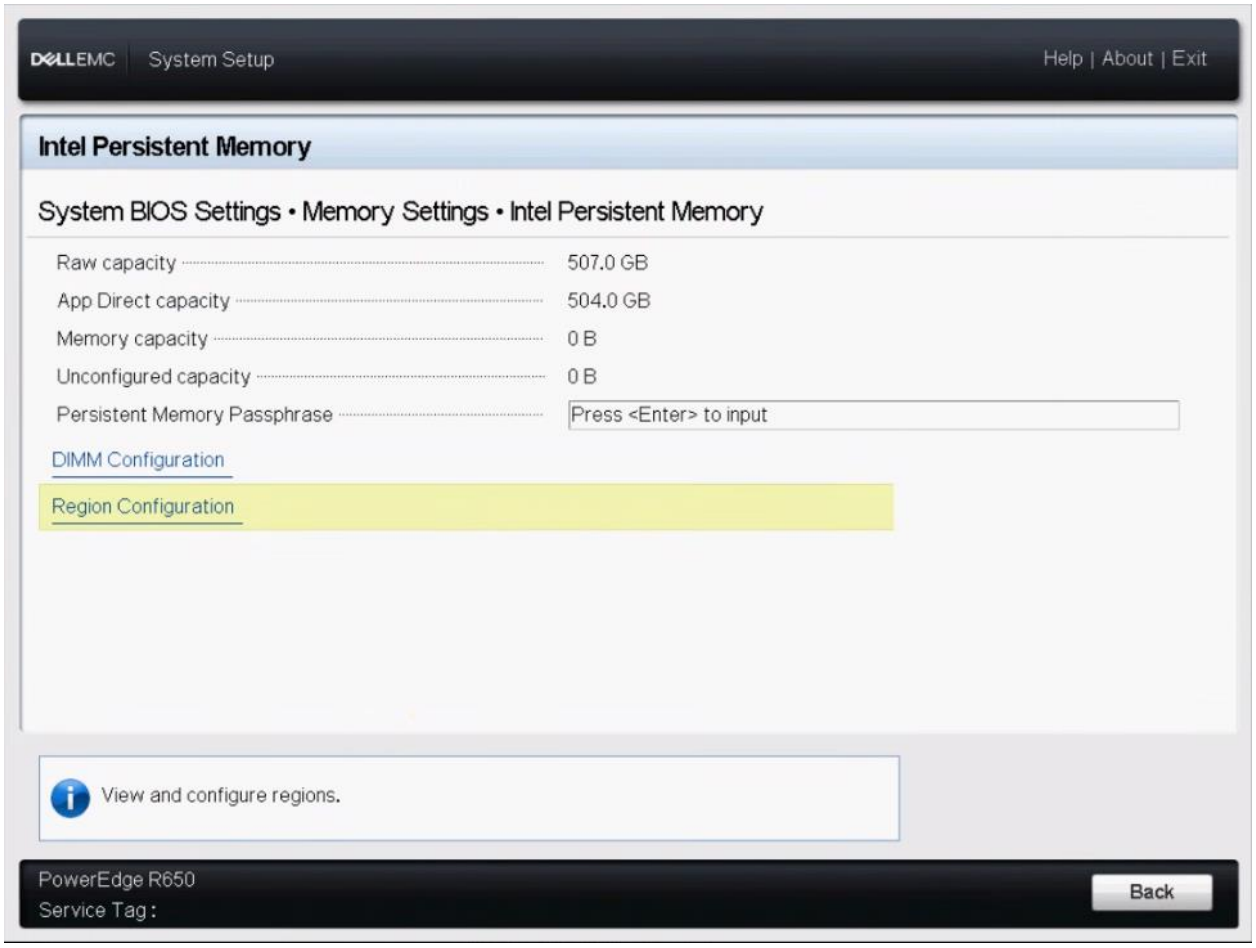



Figure 6 Intel Persistent Memory

| Info items | Description |
|---|---|
| **Raw Capacity** | The total Intel Optane Persistent Memory capacity in the system. |
| **App Direct Capacity** | The total memory capacity of Intel Optane Persistent Memories that are configured as App Direct Mode. |
| **Memory Capacity** | The total memory capacity of Intel Optane Persistent Memories that are configured as Memory Mode. |
| **Unconfigured Capacity** | The total memory capacity of Intel Optane Persistent Memories that are not configured. |
| **Persistent Memory Passphrase** | The Persistent Memory Passphrase unlocks secured Persistent Memory DIMMs. All Persistent Memory DIMMs are affected if the passphrase is modified.<br>WARNING: Entering and confirming a blank passphrase disables passphrase security in all Persistent Memory DIMMs. |
| | |

## 1.3.2 System BIOS—Persistent Memory DIMM Configuration

The Persistent Memory DIMM Configuration page displays a list of Intel Optane DIMMs that are in the system.

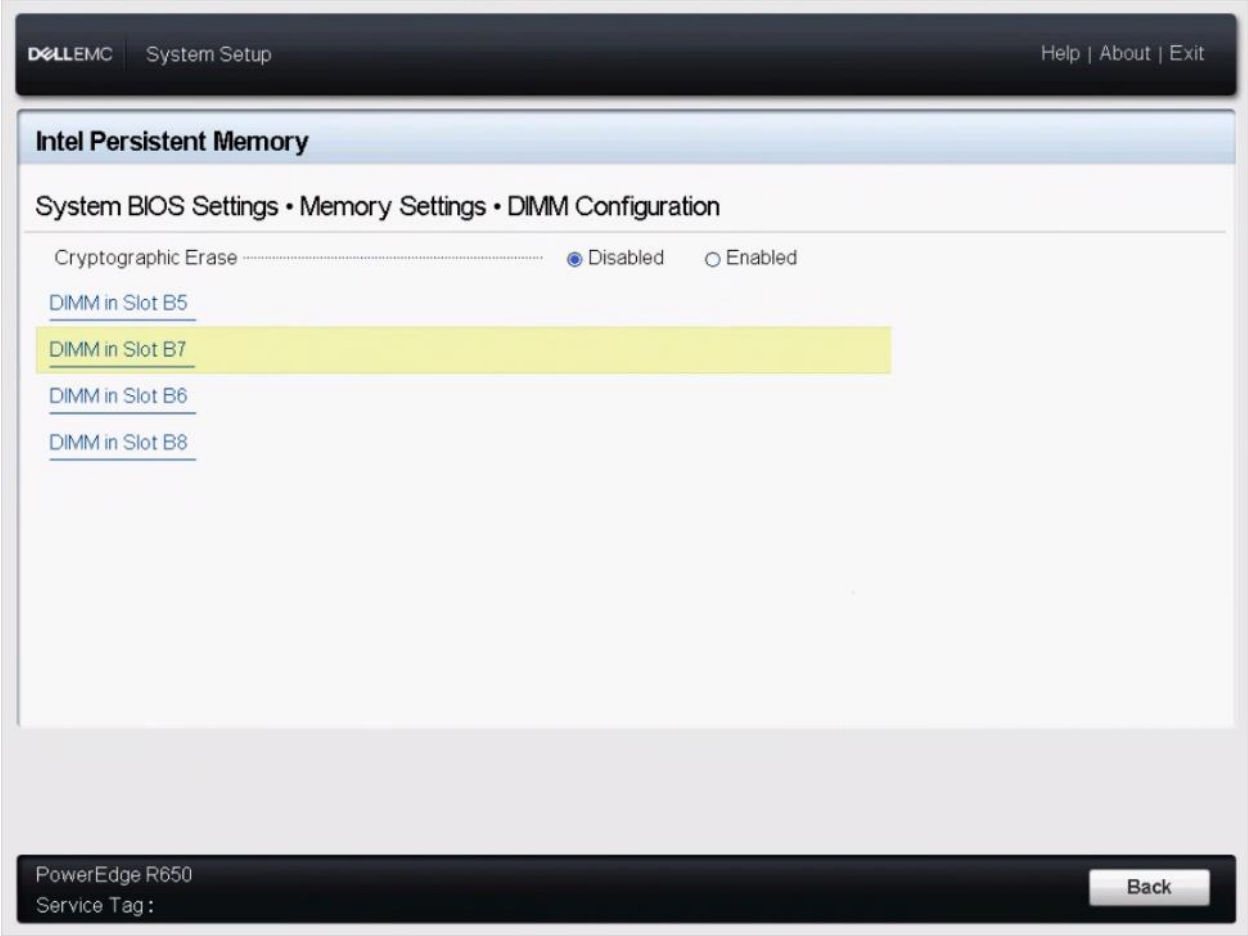



Figure 7 Persistent Memory DIMM Configuration

| Menu Item | Options | Description |
|---|---|---|
| **Cryptographic Erase** | • **Disabled**<br>• Enabled | Enable or Disable Secure Erase Persistent Memory. |

### 1.3.3 System BIOS—DIMM Information

The DIMM Information page displays information about the selected Intel Optane Persistent Memory.

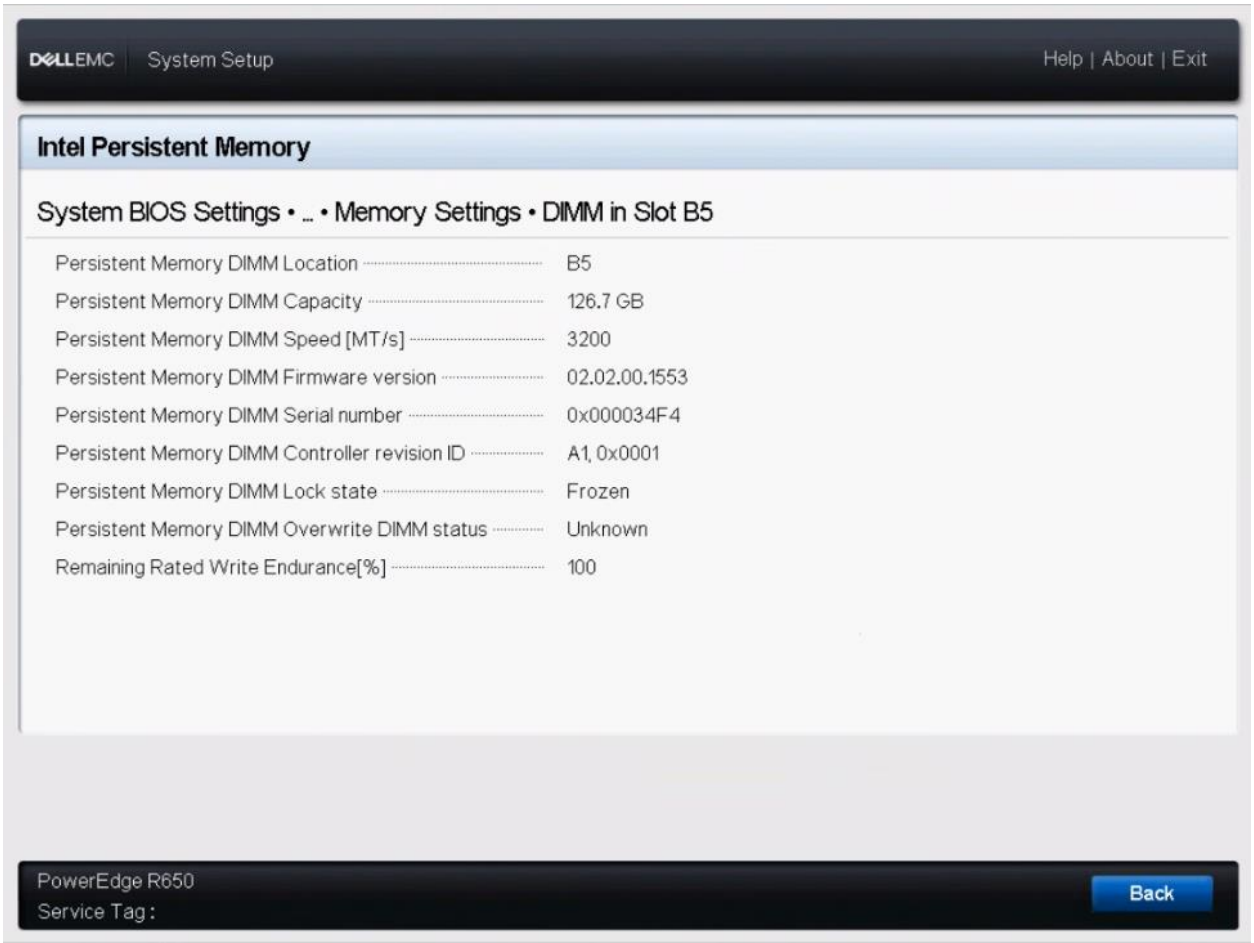



Figure 8 DIMM Information

| Menu Items | Description |
|---|---|
| **Persistent Memory DIMM Location** | The DIMM Slot in which the currently selected Intel Optane Persistent Memory is being populated. |
| **Persistent Memory DIMM Capacity** | The memory capacity of currently selected Intel Optane Persistent Memory. |
| **Persistent Memory DIMM Speed[MHz]** | The operation speed of currently selected Intel Optane Persistent Memory. |
| **Persistent Memory DIMM Firmware Version** | The firmware version of currently selected Intel Optane Persistent Memory. |
| **Persistent Memory DIMM Serial Number** | The serial number of currently selected Intel Optane Persistent Memory. |
| **Persistent Memory DIMM Controller revision ID** | Revision ID of the subsystem memory controller. |
| **Persistent Memory DIMM Lock state** | The security state of this NVDIMM as unknown, disabled, unlocked, locked, frozen, max password, and not supported. |
| **Persistent Memory DIMM Overwrite DIMM status** | The Overwrite DIMM Status of this NVDIMM as unknown, not started, in progress, and completed. |
| **Remain Rate Write Endurance [%]** | This is the lifetime percentage available for currently selected Intel Optane Persistent Memory. |

| Menu Item | Options | Description |
|---|---|---|
| **Secure Erase** | • **Disable**<br>• Enable | Enable or disable the Secure Erase feature for this selected Intel Optane Persistent Memory. When enabled, after successfully secure erasing, this option is set back to Disable. |
| **Overwrite DIMM** | • **Disable**<br>• Enable | Enable or disable the Overwrite DIMM feature for this selected Intel Optane Persistent Memory. When enabled, after the DIMMs are successfully overwritten, this option is set back to Disable. |

### 1.3.4 System BIOS—Region Configuration

The Region Configuration page displays the persistent memory regions used in the system and for creating goal for Intel Optane Persistent Memory.

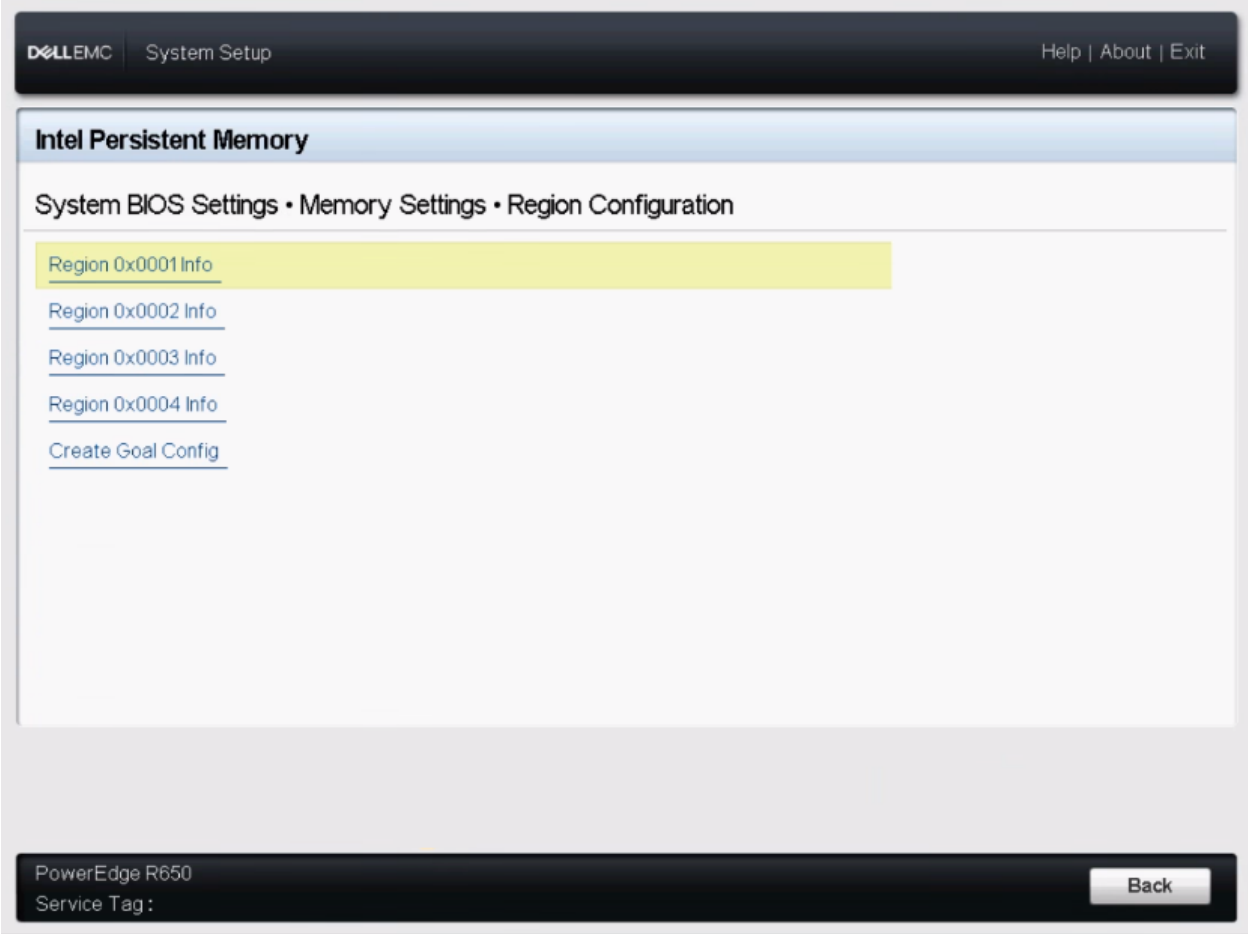



Figure 9 Region Configuration

## 1.3.5 System BIOS—Region Information

The Region Information page displays information about the selected Region.

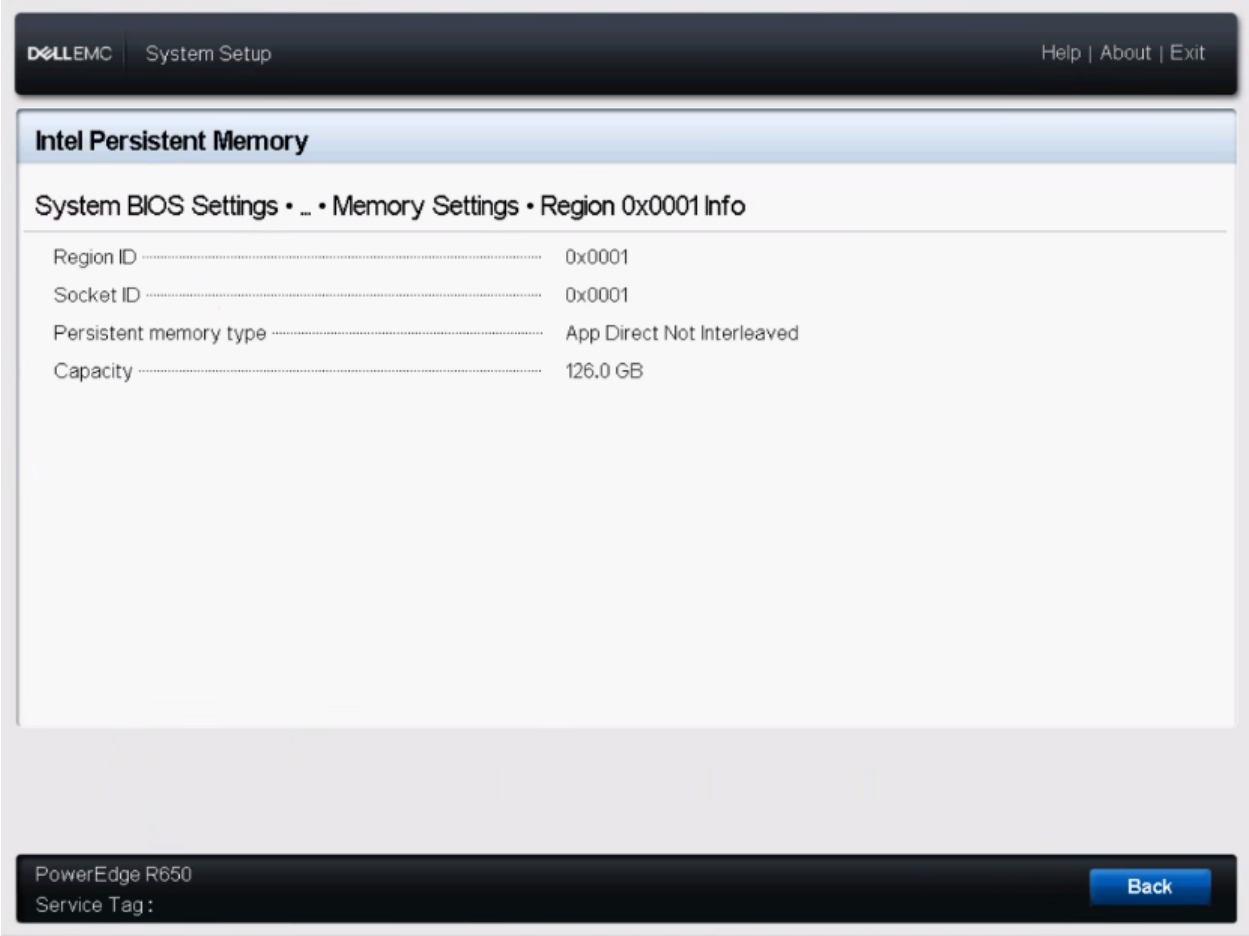



Figure 10 The page of region Info

| Menu item | Description |
|---|---|
| **Region ID** | Identification number of the currently selected region. |
| **Socket ID** | Identification number of the CPU socket that the currently selected region is associated with. |
| **Persistent Memory Type** | The persistent memory type that the currently selected region is configured. It can be AppDirect or AppDirect Non-Interleaved. |
| **Capacity** | Size of the currently selected region. |

## 1.3.6 System BIOS—Create Goal Configuration

The Create Goal Configuration page enables an administrator to Create Goal Configuration for the system.

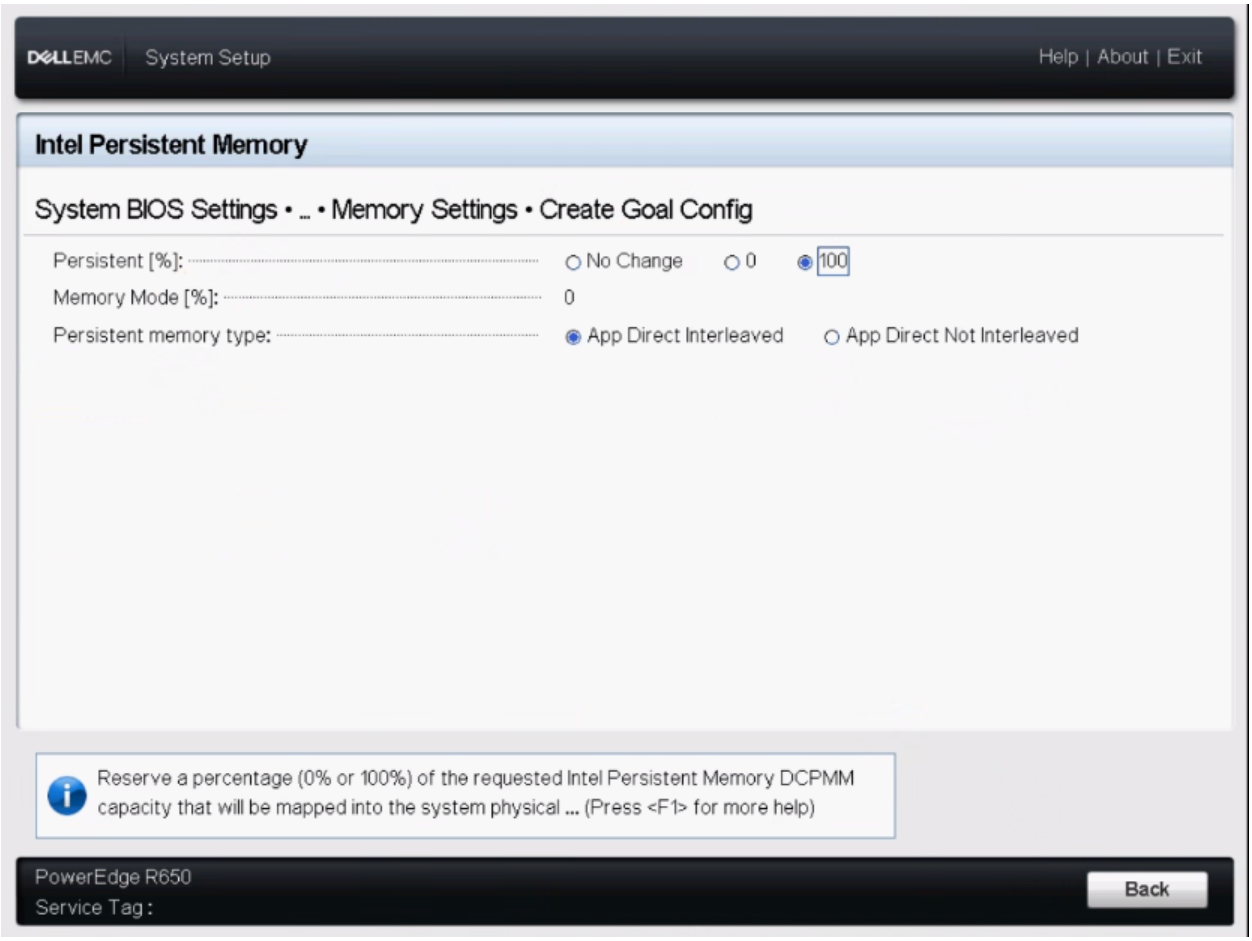



Figure 11 Create Goal Configuration

| Menu Item | Options | Description |
|---|---|---|
| **Operation Target** | • **Platform**<br>• Socket | The region targets to platform level or socket level. |
| **Socket 0-3** | • **Disable**<br>• Enable | Select enable or disable region creation for the selected socket. |
| **Persistent [%]:** | • **No Change**<br>• 0<br>• 100 | Reserve a percentage (0% or 100%) of the requested Intel Persistent Memory DCPMM capacity that will be mapped into the system physical address space as Persistent Memory. Due to platform memory alignment requirements, this value will be aligned automatically. Note: when Persistent sets to 0%, 100% Memory Mode will be set automatically. When Persistent sets to 100% Memory Mode will be set to 0%. |
| **Memory Mode [%]:** | • **No Change**<br>• 0<br>• 100 | Set the percentage of the total capacity to use in Memory Mode (0% or 100%). Due to platform memory alignment requirements, this value will be aligned automatically. |

| | | |
|---|---|---|
| | | **Note:** when Persistent sets to 0%, 100% Memory Mode will be set automatically. When Persistent sets to 100%, Memory Mode will be set to 0%. |

## 1.3.7 System BIOS—NVDIMM-N Persistent Memory

The NVDIMM-N Persistent Memory page displays information about the selected NVDIMM-N Persistent Memory.

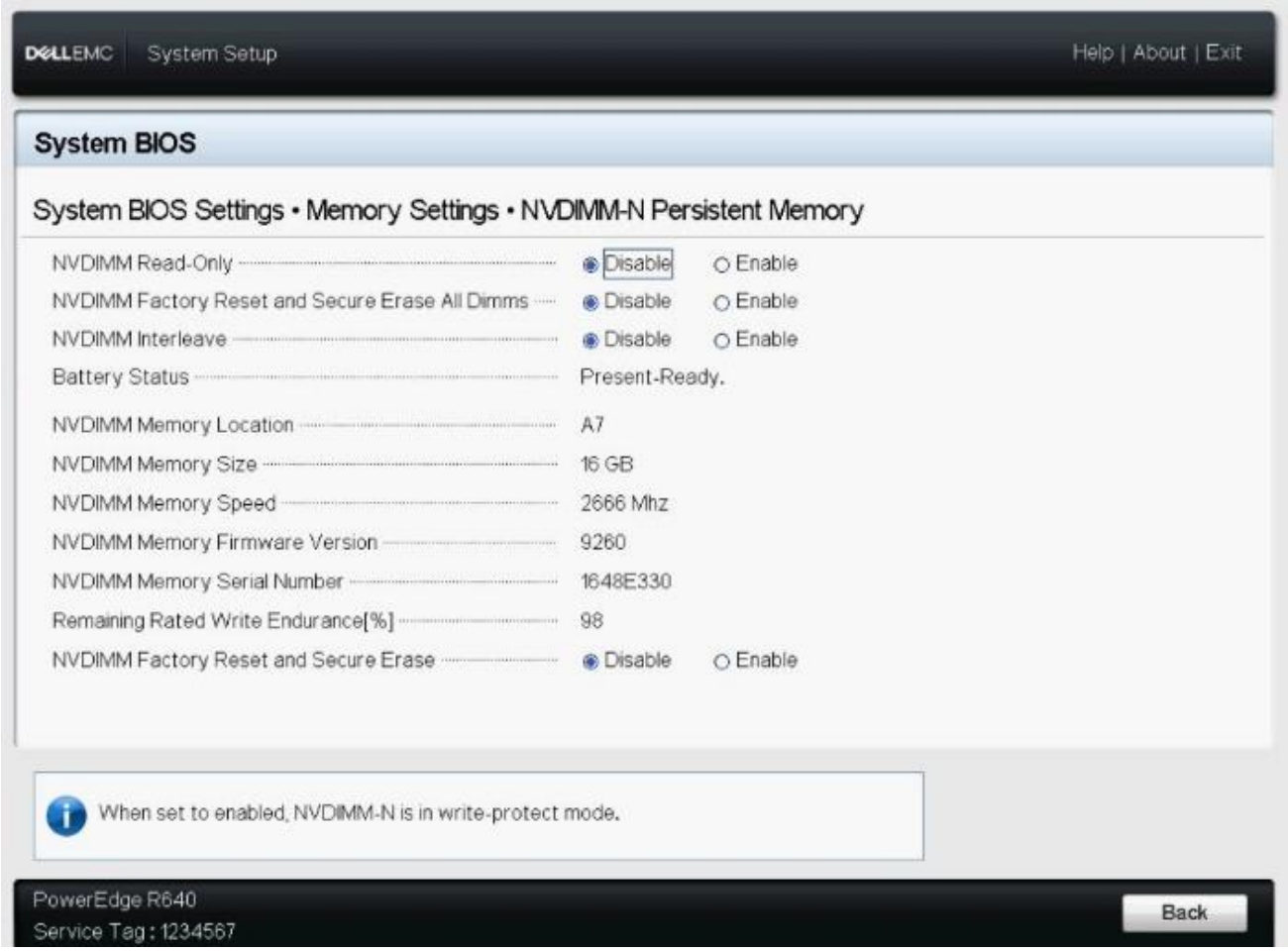



Figure 12 NVDIMM-N Persistent Memory

| Menu Item | Options | Description |
|---|---|---|
| **NVDIMM Read-Only** | • **Disable**<br>• Enable | When set to enable, the NVDIMM-N Persistent Memory is set to protected mode. Any write operation to the persistent memory region is not saved. |
| **NVDIMM Factory Reset and Secure Erase All Dimms** | • **Disable**<br>• Enable | Resets all the NVDIMM-N Persistent Memory in the system to their factory default state and erases all NVDIMM-N Data.<br>**Warning**: All contents are lost after saving and exiting the Setup menu. |
| **NVDIMM Interleave** | • **Disable**<br>• Enable | Enabling this setting interleaves the NVDIMM-N Persistent memories on a per-processor basis. When interleaving is enabled, memory performance increases. However, if one NVDIMM-N fails, the data in all the interleaved NVDIMM-N Persistent memories is lost.<br>When interleaving is disabled, if one NVDIMM-N fails, the data in other NVDIMM-N Persistent Memories remains intact. |
| **NVDIMM Factory Reset and Secure Erase** | • **Disable**<br>• Enable | This option is per-DIMM based and it is available after the information of each NVDIMM-N Persistent Memory.<br>Reset an NVDIMM-N Persistent Memory to its factory default state, and then erase the NVDIMM-N data.<br>**Warning**: All contents in the NVDIMM-N Persistent Memory is lost if changes are saved when exiting the BIOS setup. |

| Info items | Description |
|---|---|
| **Battery Status** | Indicates the battery status—Present-Ready, Present-Offline, or Not Present. |
| **NVDIMM Memory Location** | Indicates the slot location of the NVDIMM-N Persistent Memory. This location is printed next to each DIMM Slot on the main system board. |
| **NVDIMM Memory Size** | The size of the NVDIMM-N Persistent Memory module located at the NVDIMM Memory Location. |
| **NVDIMM Memory Speed** | The speed of the NVDIMM-N Persistent Memory module located at the NVDIMM Memory Location. |
| **NVDIMM Memory Firmware Version** | The Firmware Version of the NVDIMM-N Persistent Memory module located at the NVDIMM Memory Location. |
| **NVDIMM Memory Serial Number** | The serial number of the NVDIMM-N Persistent Memory module located at the NVDIMM Memory Location. |
| **Remain Rated Write Endurance [%]** | The percent of healthy persistent memory of the NVDIMM-N Persistent Memory module located at the NVDIMM Memory Location. |

## 1.4 System BIOS—Processor Settings

The Processor Settings page 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**<br>• Disabled | Allows you to enable or disable the logical processors (Hyper-Threading Technology). |
| **CPU Interconnect Speed** | • **Maximum data rate**<br>• 11.2 GT/s<br>• 10.4 GT/s<br>• 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.<br><br>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.<br><br>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.<br><br>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. |
| **Alternate RTID (Requestor Transaction ID) Setting** | • Enabled<br>• **Disabled** | Manipulates Requestor Transaction IDs, which are QuickPath Interconnect (QPI) resources. Generally, should be left at Disabled, as no workloads have been identified as benefitting from the manipulation of this feature.<br>NOTE: Enabling this option almost always results in negative impacts to overall system performance.<br><br>**Note:** This option is only available on systems with Intel processors. |
| **Virtualization Technology** | • **Enabled**<br>• Disabled | When this option is Enabled, BIOS will enable the processor virtualization features. |
| **IOMMU Support** | • **Enabled**<br>• Disabled | Enable or Disable IOMMU support. Required to create IVRS ACPI Table.<br><br>**Note:** This option is only available on systems with AMD processors. |

| | | |
|---|---|---|
| **Address Translation Services (ATS)** | • **Enabled**<br>• Disabled | Defines the Address Translation Cache (ATC) behavior for devices to cache DMA translations. This field provides an interface to a chipset's Address Translation and Protection Table to translate DMA addresses to host addresses. |
| **Directory Mode** | • **Enabled**<br>• Disabled | Defines the Address Translation Cache (ATC) behavior for devices to cache DMA translations. This field provides an interface to a chipset's Address Translation and Protection Table to translate DMA addresses to host addresses.<br><br>**Note:** This option is only available on systems with Intel processors. |
| **Adjacent Cache Line Prefetch** | • **Enabled**<br>• 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**<br>• 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. |
| **Software Prefetcher** | • **Enabled**<br>• Disabled | When set to Enabled, the processor provides advanced performance tuning by controlling the software prefetcher setting. This setting can affect performance based on the application and workloads running on the system. .<br><br>**Note:** This option is only available on systems with AMD processors. |
| **L1 Stream HW Prefetcher** | • **Enabled**<br>• Disabled | When set to Enabled, the processor provides advanced performance tuning by controlling the L1 stream HW prefetcher setting. This setting can affect performance based on the application and workloads running on the system<br><br>**Note:** This option is only available on systems with AMD processors. |
| **L2 Stream HW Prefetcher** | • **Enabled**<br>• Disabled<br>• | When set to Enabled, the processor provides advanced performance tuning by controlling the L2 stream HW prefetcher setting. This setting can affect performance based on the application and workloads running on the system<br><br>**Note:** This option is only available on systems with AMD processors. |
| **L1 Stride Prefetcher** | • **Enabled**<br>• Disabled | When set to Enabled, the processor provides additional fetch to the data access for an individual instruction for performance tuning by controlling the L1 stride prefetcher setting. This setting can affect performance based on the application and workloads running on the system<br><br>**Note:** This option is only available on systems with AMD processors. |

| | | |
|---|---|---|
| **L1 Region Prefetcher** | • **Enabled**<br>• Disabled | When set to Enabled, the processor provides additional fetch to data along with the data access to the given instruction for performance tuning by controlling the L1 region prefetcher setting. This setting can affect performance based on the application and workloads running on the system.<br><br>**Note:** This option is only available on systems with AMD processors. |
| **L2 Up Down Prefetcher** | • **Enabled**<br>• Disabled | When set to Enabled, the processor uses memory access to determine whether to fetch next or previous for all memory accesses for advanced performance tuning by controlling the L2 up/down prefetcher setting. This setting can affect performance based on the application and workloads running on the system.<br><br>**Note:** This option is only available on systems with AMD processors. |
| **DCU Streamer Prefetcher** | • **Enabled**<br>• 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**<br>• 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<br>• **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. |
| **MADT Core Enumeration** | • Round Robin<br>• **Linear** | This field determines how BIOS enumerates processor cores in the ACPI MADT table.<br>When set to Round Robin, Processor cores are enumerated in a Round Robin order to evenly distribute interrupt controllers for the OS across all Sockets and Dies.<br>When set to Linear, Processor cores are enumerated across all Dies within a Socket before enumerating additional Sockets for a linear distribution of interrupt controllers for the OS.<br><br>**Note:** This option is only available on systems with AMD processors. |
| **NUMA Nodes Per Socket** | • 0<br>• **1**<br>• 2<br>• 4 | This field specifies the number of NUMA nodes per socket. The Zero option is for 2 socket configurations.<br><br>**Note:** This option is only available on systems with AMD processors. |

| | | |
|---|---|---|
| **L3 cache as NUMA Domain** | • Enabled<br>• **Disabled**<br>• Auto | This field specifies that each Core Complex (CCX) within the processor will be declared as a NUMA Domain.<br><br>**Note:** This option is only available on systems with AMD processors. |
| **Secure Memory Encryption** | • Enabled<br>• **Disabled** | Enables or disables AMD secure encryption features such as Secure Memory Encryption (SME) and Secure Encrypted Virtualization (SEV).<br>In addition to enabling this option, SME must be supported and activated by the operating system.<br>Similarly, SEV must be supported and activated by the hypervisor.<br>This option also determines if other secure encryption feature such as TSME and SEV-SNP features can be enabled.<br><br>**Note:** This option is only available on systems with AMD processors. |
| **Minimum SEV non-ES ASID** | | This field determines the number of Secure Encrypted Virtualization (SEV) ES and non-ES available Address Space IDs.<br>The number specified is the dividing line between ES and non-ES ASIDs.<br>ES - Encrypted State - the register save state area is also encrypted along with the entire guest memory area.<br>The maximum number of ASIDs available depends on installed CPU and memory configuration which can either be 15, 253 or 509.<br>The default value is 1 and the value entered by user means the number of non-ES ASIDs starts from the value entered and ends at the maximum number of ASIDs available.<br>A value of 1 means there are only non-ES ASIDs available.<br>Example 1: If the maximum number of ASIDs is 15, the default value 1 means there are 15 SEV non-ES ASIDs and 0 SEV ES ASIDs.<br>Example 2: If the maximum number of ASIDs is 15, the value 4 means there are 12 SEV non-ES ASIDs and 3 SEV ES ASIDs.<br>Example 3: If the maximum number of ASIDs is 509, the value 40 means there are 470 SEV non-ES ASIDs and 39 SEV ES ASIDs.<br><br>**Note:** This option is only available on systems with AMD processors. |
| **Secure Nested Paging** | • Enabled<br>• **Disabled** | Enables or disables SEV-SNP, a set of additional security protections.<br><br>**Note:** This option is only available on systems with AMD processors. |
| **Transparent Secure** | • Enabled | Enables or disables TSME.<br>TSME is always-on memory encryption that does not |

| | | |
|---|---|---|
| **Memory Encryption** | • **Disabled** | require operating system or hypervisor support. If the operating system supports SME this field does not need to be enabled. If the hypervisor supports SEV this field does not need to be enabled.<br>Enabling TSME affects system memory performance.<br><br>**Note:** This option is only available on systems with AMD processors. |
| **UPI Prefetch** | • **Enabled**<br>• 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.<br><br>**Note:** This option is only available on systems with Intel processors. |
| **XPT Prefetch** | • **Enabled**<br>• Disabled | XPT prefetch is a mechanism that enables the MS2IDI to take a read request that is being sent to the LLC and speculatively issue a copy of that read to the memory controller.<br><br>**Note:** This option is only available on systems with Intel processors. |
| **LLC Prefetch** | • **Enabled**<br>• Disabled | Enable/Disable LLC Prefetch on all threads.<br><br>**Note:** This option is only available on systems with Intel processors. |
| **Dead Line LLC Alloc** | • **Enabled**<br>• Disabled | Enabled - opportunistically fill dead lines in LLC. Disabled - never fill dead lines in LLC.<br><br>**Note:** This option is only available on systems with Intel processors. |
| **Directory AtoS** | • Enabled<br>• **Disabled** | AtoS optimization reduces remote read latencies for repeat read accesses without intervening writes.<br><br>**Note:** This option is only available on systems with Intel processors. |
| **Logical Processor Idling** | • Enabled<br>• **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.<br><br>**Note:** This option is only available on systems with Intel processors. |

| | | |
|---|---|---|
| **AVX P1** | • **Normal**<br>• Level 1<br>• Level 2 | AVX P1 level selection<br><br>**Note:** This option is only available on systems with Intel processors. |
| **Dynamic SST-Performance Profile** | • Enabled<br>• **Disabled** | Allows the reconfiguration of the processor via Dynamic or Static SST-PP Select.<br><br>**Note:** This option is only available on systems with Intel processors. |
| **SST-Performance Profile** | • **Operating Point 1 \| P1: 2.9 GHz, TDP:205w, Core Count:16**<br>• Operating Point 2 \| P1: 0.0 GHz, TDP:0w, Core Count:0<br>• Operating Point 3 \| P1: 0.0 GHz, TDP:0w, Core Count:0 | Allows the reconfiguration of the processor via Speed Select Technology (SST).<br><br>**Note:** This option is only available on systems with Intel processors. |
| **Intel SST-BF** | • Enabled<br>• **Disabled** | Enable Intel SST-BF. It is only allowed in Performance Per Watt (OS) or Custom (when OSPM is enabled) system profiles.<br><br>**Note:** This option is only available on systems with Intel processors. |
| **Intel SST-CP** | • Enabled<br>• **Disabled** | RAPL Prioritization allows creating core groups of different priority.<br><br>**Note:** This option is only available on systems with Intel processors. |
| **X2Apic Mode** | • Enabled<br>• **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. |
| **AVX ICCP Pre-Grant License** | • Enabled<br>• **Disabled** | Allows the user to enable or disable the selection of different AVX ICCP transition levels offered by Intel. This option is set to Disabled by default.<br><br>**Note:** This option is only available on systems with Intel processors. |
| **AVX ICCP Pre-Grant Level** | • **128 Heavy**<br>• 256 Light<br>• 256 Heavy<br>• 512 Light<br>• 512 Heavy | Allows the system to select between different AVX ICCP transition levels offered by Intel. The default level is 128 Heavy.<br><br>**Note:** This option is only available on systems with Intel processors. |
| **Dell Controlled Turbo** | • Enabled<br>• **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.<br><br>**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 CCDs per Processor** | • **All**<br>• 2<br>• 3<br>• 4<br>• 6 | Enable number of CCDs (Core Chiplet Die) per Processor.<br><br>**Note:** This option is only available on systems with AMD processors. |
| **Number of Cores per CCD** | • **All**<br>• ONE(1+0)<br>• TWO(2+0)<br>• THREE(3+0)<br>• FOUR(4+0)<br>• FIVE(5+0)<br>• SIX(6+0)<br>• SEVEN(7+0) | Enable number of Cores per CCD (Core Chiplet Die).<br><br>**Note:** This option is only available on systems with AMD processors. |
| **Number of Cores per Processor** | • **All**<br>• 1<br>• 2<br>• 4<br>• 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). |
| **Local Machine Check Exception** | • Enabled<br>• **Disabled** | Enable or disable the LMCE feature. This is an extension of the MCA Recovery mechanism providing the capability to deliver Uncorrected Recoverable (UCR) Software Recoverable Action Required (SRAR) errors to one or more specific logical processor threads receiving previously poisoned or corrupted data. When enabled, the UCR SRAR Machine Check Exception is delivered only to the affected thread rather than broadcast to all threads in the system. The feature supports Operating System recovery for cases of multiple, recoverable faults detected in proximity which would otherwise result in a fatal machine check event. The feature is available only on Advanced RAS processors. |
| **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. |
| **Maximum Memory Capacity** | N/A | Displays the maximum amount of system memory supported by this processor. |
| **Microcode** | | Indicates the microcode update signature. |

## 1.5 System BIOS—SATA Settings

The SATA Settings page 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**<br>• RAID Mode<br>• Off | Enables you to set different modes for the embedded SATA controller(s).<br><br>**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**<br>• Disabled | Specifies whether 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.<br><br>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<br>• **Disabled** | Allows you to enable or disable Write Cache on SATA drives during POST. This option is only applicable to AHCI mode, and is not applicable to RAID mode. |
| **Port A (B, C….)** | • **Auto**<br>• 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.<br><br>**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. |

## 1.6 System BIOS—Boot Settings

Boot Settings page 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<br>• **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.<br><br>**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**<br>• 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<br>• **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.<br><br>**Note**: This option is applicable to BIOS boot mode only. |
| **Generic USB Boot** | • Enabled<br>• **Disabled** | When set to Enabled, a Generic USB Boot placeholder will be placed in the UEFI Boot Sequence, which will map to the first bootable USB device in the boot sequence.<br>This allows the entry to remain present even if the USB device is not present.<br>This is only available in UEFI Boot Mode. |
| **Hard-disk Drive Placeholder** | • Enabled<br>• **Disabled** | When set to Enabled, a Generic RAID HDD placeholder will be placed into the UEFI Boot Sequence. The entry will remain present until an operating system or a bootable file is installed on the RAID disk.<br>This setting is only available in UEFI Boot Mode. |
| **Clean all Sysprep order and variables** | • **None**<br>• Yes | When set to None, BIOS will do nothing. When set to Yes, BIOS will delete variables of SysPrep #### and SysPrepOrder this option is a onetime option, will reset to none when deleting variables.<br>This setting is only available in UEFI Boot Mode. |
| **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. |

## 1.7 System BIOS—Network Settings

The Network Settings page 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**<br>• 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<br>• **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<br>• **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<br>• **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. |

## 1.8 System BIOS—Integrated Devices

The Integrated Devices enables you to view and configure the settings of all Integrated Devices in the system.

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

| Menu Item | Options | Description |
|---|---|---|
| **User Accessible USB Ports** | • **All Ports On**<br>• Only Back Ports On<br>• All Ports Off<br>• 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.<br>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.<br><br>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.<br>On the iDRAC GUI, click **System Settings → Hardware Settings → Front Ports**.<br><br>**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. |
| **Enable Front Ports Only** | • Enabled<br>• Disabled | This field enables/disables the front USB ports during the OS runtime when User Accessible USB Ports is set as All Ports Off (Dynamic). |
| **Internal USB Port** | • **Enabled**<br>• Disabled | Allows you to enable or disable the internal USB port. |
| **iDRAC Direct USB Port** | • **On**<br>• 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**<br>• Disabled | Allows you to enable or disable the integrated RAID controller. |
| **Integrated Network Card 1(2)** | • **Enabled**<br>• Disabled | Allows you to enable or disable the integrated network card (NDC). This option is available only to systems that support NDC.<br><br>**Note**: If set to Disabled, the NIC interface may still be available for shared network access by iDRAC. |
| **Embedded NIC1, NIC2, NIC3 and NIC4** | • **Enabled**<br>• Disabled (OS) | Enables or disables the OS interface of the embedded NIC1, NIC2, NIC3 and NIC4 controller.<br>NOTE: If set to Disabled (OS), the embedded NICs may still be available for shared network access by the embedded management controller. This function must |

| | | |
|---|---|---|
| | | be configured via the NIC management utilities provided with your system. |
| **I/OAT DMA Engine** | • Enabled<br>• **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.<br><br>**Note:** This option is only available on systems with Intel processors. |
| **Embedded Video Controller** | • **Enabled**<br>• Disabled | This field enables or disables the use of the Embedded Video Controller as the primary display.<br><br>• If Enabled, the Embedded Video Controller will be the primary display even if add-in graphics cards are installed.<br><br>• 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.<br><br>**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. |
| **I/O Snoop HoldOff Response** | • **256 Cycles**<br>• 512 Cycles<br>• 1K Cycles<br>• 2K Cycles | Selects the number of cycles PCI I/O can withhold snoop requests, from the CPU, to allow time to complete its own write to LLC. This setting can help improve performance on workloads where throughput and latency are critical.<br><br>**Note:** This option is only available on systems with Intel processors. |
| **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. |
| **Pcie Preferred IO Bus** | • Enabled<br>• **Disabled** | In certain platform configurations it is possible to improve the performance of an endpoint by enabling Pcie Preferred IO Bus.<br>To select a particular Pcie Bus, references the PCI bus (in Hexadecimal) of the add-in card when requesting Preferred I/O Bus for the device. |

| | | |
|---|---|---|
| | | **Note:** This option is only available on systems with AMD processors. |
| **Pcie Preferred IO Bus Value** | | This field sets the PCI bus address that preferred IO device resides.<br>Bus address ranges from [0x0:0xFF].<br><br>**Note:** This option is only available on systems with AMD processors. |
| **Enhanced Preferred IO** | • Enabled<br>• **Disabled** | When Enhanced Preferred IO is enabled the LCLK speed for the root complex where Preferred IO is enabled will automatically be set to 600 MHz (effective 593 MHz)<br><br>**Note:** This option is only available on systems with AMD processors. |
| **SR-IOV Global Enable** | • Enabled<br>• **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. |
| **RIPS Presence** | • Yes<br>• No | Indicate the presence state of the RIPS (Redundant Internal Persistent Storage). |
| **Internal SD Card Port** | • **On**<br>• Off | Enables or disables the internal SD Card port. |
| **Internal SD Card Redundancy** | • Disabled<br>• Mirror | Configures the redundancy mode of the Internal Dual SD module (IDSDM). When set to Mirror Mode, data is written to both SD cards. After failure of either card or replacement of the failed card, the data of the active card is copied to the offline card during the system boot.<br>When Redundancy is set to disabled, only the primary SD Card is visible to the OS. |
| **Internal SD Presence** | • None<br>• SD Card 1 Only<br>• SD Card 2 Only<br>• Both | Indicate the presence state of the Internal Dual SD module (IDSDM). |
| **Internal SD Primary Card** | • SD Card 1<br>• SD Card 2 | When Redundancy is set to Disabled, either one of the SD cards can be selected to present itself as mass storage device by setting it to be primary card.<br>By default, primary SD card is selected to be SD Card 1. If SD Card 1 is not present, then controller will select SD Card 2 to be primary SD card. |
| **OS Watchdog Timer** | • Enabled<br>• **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 can initialize the timer. When set to Disabled (the default), the timer will have no effect on the system. |
| **Empty Slot Unhide** | • Enabled<br>• **Disabled** | If set to Enabled, root ports of all the empty slots will be accessible to the BIOS and OS. |

| | | |
|---|---|---|
| **Memory Mapped I/O above 4GB** | • **Enabled**<br>• 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.<br><br>**Note:** This option is only available on systems with Intel processors. |
| **Memory Mapped I/O Base** | • **56TB**<br>• 12TB<br>• 512GB | MMIO base default is 56TB. User should not change the default value unless addressing a known issue.<br>When set to 12TB, the system will map MMIO base to 12TB.<br>Enable this feature for an OS that requires 44bit PCIe addressing.<br>When set to 512GB, the system will map MMIO base to 512GB, and reduce the maximum support for memory to less than 512GB. Enable this option only for the 4 GPU DGMA issue.<br><br>**Note:** This option is only available on systems with Intel processors. |
| **Memory Mapped I/O Limit** | • **8TB**<br>• 1TB | Memory Mapped I/O Limit controls where MMIO is mapped.<br>The default, 8TB, is the max address the system supports and recommended in most cases.<br>The 1TB option designed for specific OS which cannot support MMIO over 1TB.<br><br>**Note:** This option is only available on systems with AMD processors. |
| **PCIe Bus Customization** | • **PCIe Bus System Allocation**<br>• PCIe Bus Custom Allocation Option 1<br>• PCIe Bus Custom Allocation Option 2<br>• PCIe Bus Custom Allocation Option 3 | Provide options for customizing the allocation of PCIe bus ranges to PCIe slots.<br>This can be useful when connecting complex device sets to a slot.<br>PCIe Bus System Allocation uses the normal rules of the system to allocate bus ranges.<br>PCIe Bus Custom Allocation Option 1 increases the bus ranges allocated to the wider slots.<br>PCIe Bus Custom Allocation Option 2 increases the bus range allocated to one of the wide slots more than with option 1.<br>PCIe Bus Custom Allocation Option 3 allocates the largest bus range practical to one of the wide slots. Note that use of this option may cause insufficient resources to be available for remaining slots and prevent the system from functioning.<br><br>**Note:** This option is only available on systems with Intel processors. |
| **Slot Disablement** | • **Enabled**<br>• Disabled<br>• 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.<br>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.<br><br>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.<br><br>**Note**: This option is not available if the slot contains a Dell EMC PowerEdge RAID Card (PERC).<br><br>**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<br>• Auto Discovery of Bifurcation<br>• Manual Bifurcation Control | Enables BIOS to dynamically scan for PCIe devices rather than relying strictly on system slot definitions.<br><br>• The Platform Default setting will strictly follow the system slot definitions when configuring each PCIe slot.<br><br>• 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.<br><br>• Manual Control allows the user to override bifurcation settings for each slot.<br><br>CAUTION: Improper configuration of PCIe slots can prevent the system from functioning properly. |

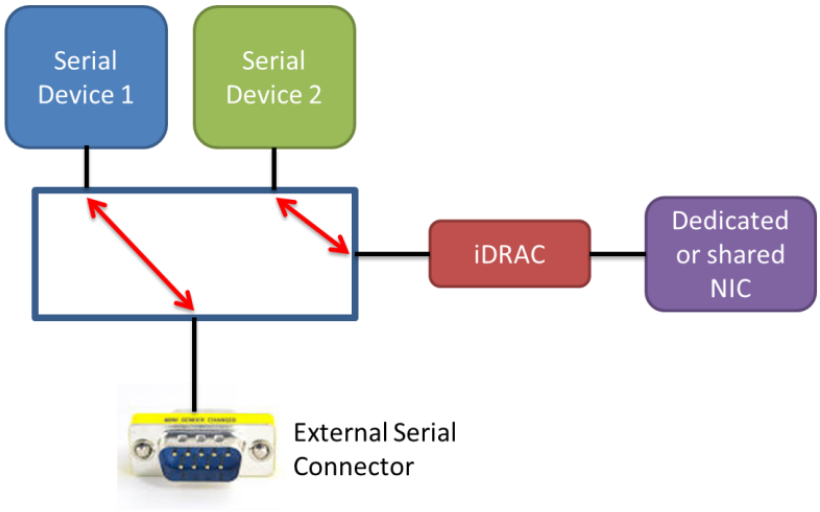
## 1.9 System BIOS—Serial Communication

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.

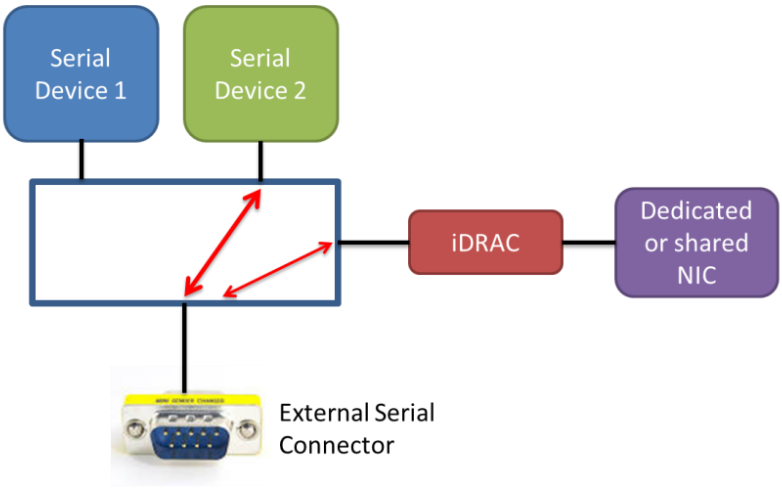
| Menu Item | Options | Description |
|---|---|---|
| **Serial Communication** | • On without Console Redirection<br>• **Auto**<br>• On with Console Redirection via COM1<br>• On with Console Redirection via COM2<br>• Off | Configures the BIOS serial console redirection feature and determines which serial 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<br>• **Serial Device1=COM2,Serial Device2=COM1** | Enables you to set the port address for serial devices.<br>**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**<br>• Serial Device 2<br>• Remote Access Device | Associates the External Serial Connector to Serial Device 1, Serial Device 2 or the Remote Access Device.<br>**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**<br>• 57600<br>• 19200<br>• 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**<br>• 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**<br>• 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:



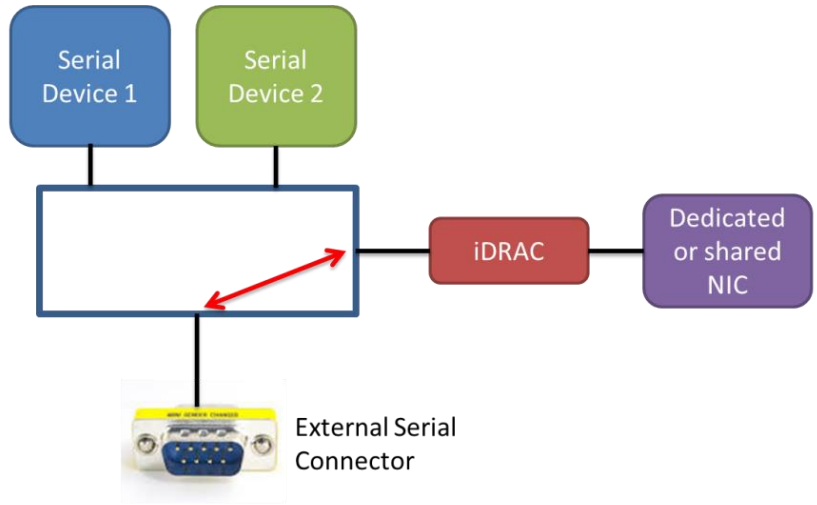

External Serial Connector is set to Serial Device 1. The serial MUX enables concurrent Serial over LAN (SOL ) access and external serial connector access to host.

Figure 13 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 14 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 15 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:

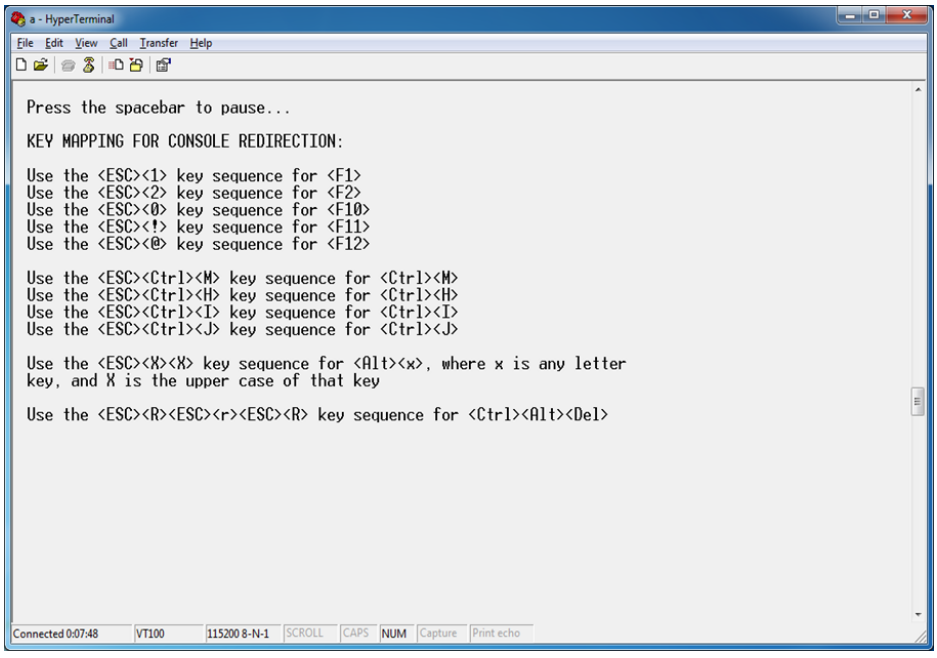



Figure 16 Key mapping for console redirection

## 1.10 System BIOS—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)**<br>• Performance per Watt (OS)<br>• Performance<br>• Workstation Performance<br>• 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.<br><br>**Performance Per Watt Optimized (DAPC)**<br>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.<br><br>Detailed settings for AMD and Intel platforms are descripted in section 1.10.1 and 1.10.2.<br>**Performance Per Watt Optimized (OS)**<br>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. Detailed settings for AMD and Intel platforms are descripted in section 1.10.1 and 1.10.2.<br><br>**Performance**<br>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.<br><br>**Custom**<br>In this mode, you can change the settings of individual options. The following sections will describe each option in detail. |
| **CPU Power Management** | • **System DBPM (DAPC)**<br>• Maximum Performance<br>• OS DBPM | Enables you to set the CPU power management mode.<br><br>• 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.<br><br>• The OS DBPM (Demand Based Power Management) means that it is the OS that controls the processor's power management.<br><br>Maximum Performance mode keeps the processor running at the highest frequency all the time. |
| **Memory Frequency** | • **Maximum Performance**<br>• 3400MHz<br>• 3200MHz<br>• 2933MHz<br>• 2666MHz<br>• 2400MHz<br>• 2133MHz<br>• 1866MHz<br><br>• Maximum Reliability | Governs the BIOS memory frequency. The variables that govern maximum memory frequency include the maximum rated frequency of the DIMMs, the DIMMs per channel population, the processor choice, and this BIOS option. Additional power savings can be achieved by reducing the memory frequency, at the expense of reduced performance.<br>Read-only unless System Profile is set to Custom |
| **Turbo Boost** | • **Enabled**<br>• 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**<br>• Disabled | Allows you to enable or disable the processor to switch to C1E (Enhanced Halt State) when it is idle.<br><br>**Note:** This option is only available on systems with Intel processors. |
| **C States** | • **Enabled**<br>• Disabled | Allows you to enable or disable the processor to operate in all available power states. |
| **Write Data CRC** | • **Enabled**<br>• 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<br>• **Standard**<br>• Disabled | Patrol Scrubbing is a feature that searches the memory for errors and repairs correctable errors to prevent the accumulation of memory errors.<br><br>• 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.<br>• When set to Extended mode, the entire memory array will be scrubbed every hour to further increase system reliability. |
| **Memory Refresh Rate** | • **1x**<br>• 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**<br>• 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.<br><br>**Note:** This option is only available on systems with Intel processors. |
| **Energy Efficient Policy** | • Performance<br>• **Balanced Performance**<br>• Balanced Energy<br>• 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.<br><br>**Note:** This option is only available on systems with Intel processors. |
| **Number of Turbo Boost Enabled Cores for Processor 1(2,3,4)** | 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. |
| **Monitor/Mwait** | • **Enabled**<br>• 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.<br><br>**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.<br><br>**Note:** This option is only available on systems with Intel processors. |

| | | |
|---|---|---|
| **Workload Profile** | • Write Only<br>• HPC Profile<br>• Low Latency Optimized Profile<br>• Virtualization Optimized Performance Profile<br>• Virtualization Optimized Performance Per Watt Profile<br>• DataBase Optimized Performance Profile<br>• Database Optimized Performance Per Watt Profile<br>• SDS Optimized Performance Profile<br>• SDS Optimized Performance Per Watt Profile | Allows optimization of performance based on the workload type.<br>The WorkloadProfile setting is not a 'state'. Setting a workload profile is a one-time action that in turns modifies various BIOS settings to be optimized for the requested workload type. |
| **CPU Interconnect Bus Link Power Management** | • **Enabled**<br>• Disabled | When enabled, CPU interconnect bus link power management can reduce overall system power a bit while slightly reducing system performance.<br><br>**Note:** This option is only available on systems with Intel processors. |
| **PCI ASPM L1 Link Power Management** | • **Enabled**<br>• Disabled | When enabled, PCIe Advanced State Power Management (ASPM) can reduce overall system power a bit while slightly reducing system performance.<br><br>**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. |
| **Processor EIST** | • **Enabled**<br>• Disabled | This field enables or disables Processor EIST. |
| **Intel Persistent Memory CR QoS** | • **Mode 0**<br>• Mode 1<br>• Mode 2 | CR QoS tuning modes.<br>Mode 0 - Disable the PMem QoS Feature<br>Mode 1 - M2M QoS Enable/CHA QoS Disable<br>Mode 2 - M2M QoS Enable/CHA QoS Enable<br><br>**Note:** This option is only available on systems with Intel processors. |
| **Intel Persistent Memory Performance Setting** | • **BW Optimized**<br>• Balanced Profile | NVM baseline performance settings depending on the workload behavior.<br>BW Optimized - Optimized for DDR and DDRT Bandwith.<br>Latency Optimized - Better DDR latency in the presence. |

| | | |
|---|---|---|
| | | **Note:** This option is only available on systems with Intel processors. |
| **Determinism Slider** | • **Power Determinism**<br>• Performance Determinism | It controls whether BIOS will enable determinism to control performance. Performance - BIOS will enable 100% deterministic performance control. Power - BIOS will not enable deterministic performance control.<br><br>**Note:** This option is only available on systems with AMD processors. |
| **Efficiency Optimized Mode** | • Enabled<br>• **Disabled** | Efficiency Optimized Mode maximizes Performance-per-Watt by opportunistically reducing frequency/power.<br>This field enables/disables Efficiency Optimized Mode.<br><br>**Note:** This option is only available on systems with AMD processors. |
| **Algorithm Performance Boost Disable (ApbDis)** | • Enabled<br>• **Disabled** | When enabled a specific hard-fused Data Fabric (SoC) P-state is forced for optimizing workloads sensitive to latency or throughput. (For higher performance) When disabled P-states will be automatically managed by the Application Power Management, allowing the processor to provide maximum performance while remaining within a specified power-delivery and thermal envelope. (For power savings)<br><br>**Note:** This option is only available on systems with AMD processors. |
| **ApbDis Fixed Socket P-State** | • **P0**<br>• P1<br>• P2<br>• P3 | This value defines the forced P-state when ApbDis (Algorithm Performance Boost Disable) is enabled.<br><br>**Note:** This option is only available on systems with AMD processors. |
| **Dynamic Link Width Management (DLWM)** | • Forced<br>• **Unforced** | DLWM reduces the XGMI link width between sockets from x16 to x8 (default), when no traffic is detected on the link. As with Data Fabric and Memory Pstates, this feature is optimized to trade power between core and high IO/memory bandwidth workloads. Forced = Force link width to x16, x8, or x2. Unforced = Link width will be managed by DLWM engine |

| | | |
|---|---|---|
| | | **Note:** This option is only available on systems with AMD processors. |

### 1.10.1 Intel Platform System Profile

| System Profile Settings | Performance Per Watt Optimized (DAPC) | Performance Per Watt Optimized (OS) | Performance | Workstation Performance |
|---|---|---|---|---|
| **CPU Power Management** | System DBPM (DAPC) | OS DBPM | Maximum Performance | Maximum Performance |
| **Memory Frequency** | Maximum Performance | Maximum Performance | Maximum Performance | Maximum Performance |
| **Turbo Boost** | Enabled | Enabled | Enabled | Enabled |
| **C1E** | Enabled | Enabled | Disabled | Disabled |
| **C States** | Enabled | Enabled | Disabled | Enabled |
| **Write Data CRC** | Disabled | Disabled | Disabled | Disabled |
| **Memory Patrol Scrub** | Standard | Standard | Standard | Standard |
| **Memory Refresh Rate** | 1x | 1x | 1x | 1x |
| **Uncore Frequency** | Dynamic | Dynamic | Maximum | Maximum |
| **Energy Efficient Policy** | Balanced Performance | Balanced Performance | Performance | Performance |
| **Number of Turbo Boost Enabled Cores for Processor x** | All | All | All | All |
| **Monitor/Mwait** | Enabled | Enabled | Enabled | Enabled |
| **CPU Interconnect Bus Link Power Management** | Enabled | Enabled | Disabled | Disabled |
| **PCI ASPM L1 Link Power Management** | Enabled | Enabled | Disabled | Disabled |
| **Processor EIST** | Enabled | Enabled | Enabled | Enabled |

### 1.10.2 AMD Platform System Profile

| System Profile Settings | Performance Per Watt Optimized (OS) | Performance |
|---|---|---|
| **CPU Power Management** | OS DBPM | Maximum Performance |
| **Memory Frequency** | Maximum Performance | Maximum Performance |
| **Turbo Boost** | Enabled | Enabled |

| | | |
|---|---|---|
| **C States** | Enabled | Disabled |
| **Write Data CRC** | Disabled | Disabled |
| **Memory Patrol Scrub** | Standard | Standard |
| **Memory Refresh Rate** | 1x | 1x |
| **Number of Turbo Boost Enabled Cores for Processor x** | All | All |
| **PCI ASPM L1 Link Power Management** | Enabled | Disabled |
| **Determinism Slider** | Power Determinism | Power Determinism |
| **Efficiency Optimized Mode** | Disabled | Disabled |
| **Algorithm Performance Boost Disable (ApbDis)** | Disabled | Disabled |
| **Dynamic Link Width Management (DLWM)** | Unforced | Unforced |

## 1.11 System BIOS—System Security

The 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.<br><br>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, except for 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.<br><br>A password must have up to a maximum of 32 characters. |
| **Password Status** | • **Unlocked**<br>• 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. |
| **Bootmanager Password** | • **Always**<br>• Never | Bootmanager password option is available only when Setup Password is enabled.<br>If set to Always (Default value), setup password must be entered for accessing Boot Manager.<br>If set to Never, setup password need not be entered for accessing Boot Manager, One-shot UEFI Boot Menu. |
| **TPM Security (with TPM 1.2 installed)** | • **Off**<br>• On with Pre-boot Measurements<br>• On without Pre-boot Measurements | Enables you to control the reporting of the Trusted Platform Module (TPM).<br><br>• When set to Off, the presence of the TPM is not reported to the OSs.<br><br>• 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.<br><br>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**<br>• On | Enables you to control the reporting of the Trusted Platform Module (TPM).<br><br>When set to Off, the presence of the TPM is not reported to the OS.<br>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**<br>• Activate<br>• Deactivate<br>• Clear | This field allows you to control the Trusted Platform Module (TPM).<br><br>• When set to None, no command is sent to the TPM. |

| | | |
|---|---|---|
| | | • When set to Activate, the TPM will be enabled and activated.<br>• When set to Deactivate, the TPM will be disabled and deactivated.<br>• When set to Clear, all the contents of the TPM will be cleared.<br><br>WARNING: Clearing the TPM will cause loss of all the keys in the TPM. This could affect booting to the OS.<br><br>**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.<br><br>• When set to Enabled, the storage and endorsement hierarchies can be used.<br>• When set to Disabled, the storage and endorsement hierarchies cannot be used.<br>• When set to Clear, the storage and endorsement hierarchies are cleared of any values, and then reset to Enabled. |
| **TPM PPI Bypass Provision** | • Enabled<br>• **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<br>• **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<br>• SHA256<br>• SM3 (if TPM supports it) | Enables or disables Trusted Execution Technology.<br><br>To enable Intel(R) TXT, Virtualization Technology must be enabled, TPM Security must be On, and TPM2 Algorithm must be SHA256. |
| **Intel TXT** | • **Off**<br>• On | Allows you to enable or disable the Intel Trusted Execution Technology (TXT).<br>To enable Intel TXT the following must be set:<br><br>TPM 1.2<br>• Virtualization Technology must be enabled<br>• TPM Security must be “On with Pre-boot Measurements<br>• TPM Status must be “Enabled, Activated”<br><br>TPM 2.0<br>• Virtualization Technology must be enabled<br>• TPM Security must be On<br>• TPM2 Algorithm Selection must be set to SHA256 |

| | | |
|---|---|---|
| | | **Note:** This option is only available on systems with Intel processors. |
| **Memory Encryption** | • Enabled<br>• **Disabled** | Allows enabling or disabling of the Intel Total Memory Encryption<br><br>**Note:** This option is only available on systems with Intel processors. |
| **Intel(R) SGX** | • **Off**<br>• On | Allows enabling or disabling of the Intel Software Guard Extension (SGX) Technology.<br>When set to Off, BIOS disables the SGX technology.<br>When set to On, BIOS enables the SGX technology.<br>When set to Software (if available), allows application to enable the SGX technology.<br>To enable Intel SGX on Intel Xeon E5, certain platform requirements must be met.<br>CPU must be SGX capable. Memory Encryption must be on.<br>Memory population and interleaving rules must be met.<br>For example, SGX does not support UMA. SGX supports ECC DIMMs only.<br>SGX only support same interleaving mode across all CPUs.<br>SGX does not support mirror mode configurations.<br>SGX does not support one channel memory configurations.<br>SGX only supports the same type memory configuration across all CPUs.<br><br>**Note:** This option is only available on systems with Intel processors. |
| **SGX Package Info In-Band Access** | • **Off**<br>• On | Enable/Disable Software Guard Extensions (SGX) Package Info In-Band Access<br><br>**Note:** This option is only available on systems with Intel processors. |
| **PRMRR Size** | • InvalidSize<br>• 1G<br>• **2G**<br>• 4G<br>• 8G<br>• 16G<br>• 32G<br>• 64G<br>• 128G<br>• 256G<br>• 512G | Setting the PRMRR Size<br><br>**Note:** This option is only available on systems with Intel processors. |
| **SGX QoS** | • Disabled<br>• **Enabled** | Enable/Disable SGX Quality of Service |

| | | |
|---|---|---|
| | | **Note:** This option is only available on systems with Intel processors. |
| **Select Owner EPOCH input type** | • SGX Owner EPOCH activated<br>• Change to New Random Owner EPOCHs<br>• **Manual User Defined Owner EPOCHs** | There are two Owner EPOCH modes (Each EPOCH is 64bit): change to new random owner epoch and manually entered by user. After generating new epoch via 'Change to New Random Owner EPOCHs', the selection reverts back to 'Manual User Defined Owner EPOCHs'<br><br>**Note:** This option is only available on systems with Intel processors. |
| **Enable writes to SGXLEPUBKEYHASH [3..0] from OS/SW** | • Disabled<br>• Enabled | Enable writes to SGXLEPUBKEYHASH [3..0] from OS/SW<br><br>**Note:** This option is only available on systems with Intel processors. |
| **Enable/Disable SGX Auto MP Registration Agent** | • **Disabled**<br>• Enabled | The MP registration agent is responsible for register the platform<br><br>**Note:** This option is only available on systems with Intel processors. |
| **SGX Factory Reset** | • **Off**<br>• On | Perform SGX Factory Reset. On the next boot: all registration data will be deleted, and if SGX is enabled, the Initial Platform Establishment will be executed.<br><br>**Note:** This option is only available on systems with Intel processors. |
| **Power Button** | • **Enabled**<br>• Disabled | Allows you to enable or disable the power button on the front panel. |
| **AC Power Recovery** | • **Last**<br>• On<br>• 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.<br><br>• When set to Off, the system will stay off after AC is restored.<br><br>• When set to On, the system will turn on after AC is restored.<br><br>• 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**<br>• Random<br>• 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.<br>• When set to Random, the system will create a random delay for power-up.<br>• 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**<br>• Controlled | This field provides varying degrees of securing UEFI variables.<br><br>When set to Standard, UEFI variables are accessible in the OS based on the UEFI specification.<br><br>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**<br>• 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.<br><br>**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.<br><br>**Note:** This option is only available on systems with Intel processors. |
| **SMM Security Mitigation** | • Enabled<br>• **Disabled** | This option enables or disables additional UEFI SMM Security Mitigation protections.<br>The operating system can use this feature to help protect the secure environment created by virtualization-based security. Enabling this feature provides additional UEFI SMM Security Mitigation protections. However, this feature may cause compatibility issues or loss of functionality with some legacy tools or applications. |
| **Secure Boot** | • Enabled<br>• **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.<br>The following components are validated in the boot process:<br>• UEFI drivers that are loaded from PCIe cards |

| | | |
|---|---|---|
| | | • UEFI drivers and executables from mass storage devices<br>• Operating System boot loaders<br><br>**Note**: Secure Boot is not available unless the Boot Mode (in the Boot Settings menu) is UEFI.<br><br>**Note**: Secure Boot is not available unless the "Load Legacy Video Option ROM" setting (in the Miscellaneous Settings menu) is disabled.<br><br>**Note**: A Setup password is recommended to be enabled for Secure Boot. |
| **Secure Boot Policy** | • **Standard**<br>• 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.<br><br>**Note**: If Custom mode is selected, the Secure Boot Custom Policy Settings menu is displayed.<br><br>**Note**: Changing the default security certificates may cause the system to fail booting from certain boot options. |
| **Secure Boot Mode** | • User mode<br>• **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.<br><br>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.<br><br>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. |
| **Authorize Device Firmware** | • Enabled<br>• **Disabled** | When set to Enabled, this field adds the SHA-256 hash of each third-party device firmware to the Secure Boot Authorized Signature Database. After |

| | | |
|---|---|---|
| | | the hashes are added, the field automatically reverts to Disabled.<br>Note: This field is read-only unless Secure Boot is Enabled, and Secure Boot Policy is Custom. This field is available only in secure system management consoles. |
| **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.<br>A user can enroll and delete the PK, KEK, db, and dbx entries. |

## 1.12 System BIOS—Redundant OS Control

The 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**<br>• Internal SD Card<br>• SATA Port A<br>• SATA Port B<br>• SATA Port C<br>• SATA Port D<br>• SATA Port E<br>• SATA Port F<br>• SATA Port G<br>• SATA Port H<br>• SATA Port I<br>• SATA Port J<br>• SATA Port K<br>• SATA Port L<br>• SATA Port M<br>• SATA Port N<br>• Internal M.2 Drive Slot 1<br>• Internal M.2 Drive Slot 2<br>• Internal M.2 Drive Slot 3<br>• Internal M.2 Drive Slot 4<br>• Internal M.2 Drive Slot 5<br>• Internal M.2 Drive Slot 6<br>• Internal M.2 Drive Slot 7<br>• Internal M.2 Drive Slot 8<br>• Internal M.2 Drive Slot 9<br>• Internal M.2 Drive Slot 10<br>• Internal M.2 Drive Slot 11<br>• Internal M.2 Drive Slot 12<br>• Internal M.2 Drive Slot 13<br>• Internal M.2 Drive Slot 14<br>• Internal USB<br>• 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.<br><br>**Note**: For the devices and slots listed here to be displayed as optional backup devices, their settings must be as specified here:<br>• SD Card Port – On<br>• Internal USB Port – On<br>• Embedded SATA – anything other than Off<br>• PCIe Slot Disablement – Enabled |
| **Redundant OS State** | • **Visible**<br>• 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<br>• **Disabled** | When set to Enabled, the BIOS will boot to the device specified by Redundant OS Location. |

## 1.13 System BIOS—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**<br>• 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**<br>• 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.<br><br>If set to disabled, the BIOS displays the warning or error message on the screen and continues booting to the OS.<br><br>**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<br>• **Disabled** | Indicates whether 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).<br><br>**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**<br>• 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**<br>• Full Power Cycle | Specifies how the system reacts when system transitions to S5 state. When set to None, the transition to S5 is normal.<br>When set to Full Power Cycle, the system will temporarily be forced into a lower power state, like 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.