Dell EMC PowerEdge R940xa

BIOS and UEFI Reference Guide

Part Number: E54S Series
Regulatory Type: E54S001
March 2022
Rev. A03

DELL Technologies

Notes, cautions, and warnings

NOTE: A NOTE indicates important information that helps you make better use of your product.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

Contents

1

Pre-operating system management applications

You can manage basic settings and features of a system without booting to the operating system by using the system firmware.

Topics:

Options to manage the pre-operating system applications

Your system has the following options to manage the pre-operating system applications:

- System Setup
- Dell Lifecycle Controller
- Boot Manager
- Preboot Execution Environment (PXE)

System Setup

By using the **System Setup** screen, you can configure the BIOS settings, iDRAC settings,BMC settings, and Device settings of your system.

NOTE: Help text for the selected field is displayed in the graphical browser by default. To view the help text in the text browser, press F1.

You can access system setup by using two methods:

- Standard graphical browser—The browser is enabled by default.
- Text browser—The browser is enabled by using Console Redirection.

View System Setup

To view the **System Setup** screen, perform the following steps:

Steps

1. Turn on, or restart your system.
2. Press F2 immediately after you see the following message:

```
F2 = System Setup
```

NOTE: If your operating system begins to load before you press F2, wait for the system to finish booting, and then restart your system and try again.

System Setup details

The **System Setup Main Menu** screen details are explained as follows:

Option	Description
System BIOS	Enables you to configure BIOS settings.
iDRAC Settings	Enables you to configure the iDRAC settings. The iDRAC settings utility is an interface to set up and configure the iDRAC parameters by using UEFI (Unified Extensible Firmware Interface). You can enable or disable various iDRAC parameters by using the iDRAC settings utility. For more information about this utility, see *Integrated Dell Remote Access Controller User's Guide* at www.dell.com/idracmanuals.
iDRAC Settings	Enables you to configure BMC settings. The iDRAC settings utility is an interface to set up and configure the BMC parameters by using UEFI. You can enable or disable various BMC parameters by using the iDRAC settings utility. For more information about this utility, see *Integrated Dell Remote Access Controller 8 User's Guide* at www.dell.com/idracmanuals.
Device Settings	Enables you to configure device settings such as network cards or storage controllers.

System BIOS

You can use the **System BIOS** screen to edit specific functions such as boot order, system password, setup password, set the SATA and PCIe NVMe RAID mode, and enable or disable USB ports.

Viewing System BIOS

To view the **System Setup** screen, perform the following steps:

Steps

1. Turn on, or restart your system.
2. Press F2 immediately after you see the following message:

```
F2 = System Setup
```

NOTE: If your operating system begins to load before you press F2, wait for the system to finish booting, and then restart your system and try again.

3. On the **System Setup Main Menu** screen, click **System BIOS**.

System BIOS Settings details

About this task

The **System BIOS Settings** screen details are explained as follows:

Option	Description
System Information	Specifies information about the system such as the system model name, BIOS version, and Service Tag.
Memory Settings	Specifies information and options related to the installed memory.
Processor Settings	Specifies information and options related to the processor such as speed and cache size.
SATA Settings	Specifies options to enable or disable the integrated SATA controller and ports.

Option	Description
NVMe Settings	Specifies options to change the NVMe settings. If the system contains the NVMe drives that you want to configure in a RAID array, you must set both this field and the **Embedded SATA** field on the **SATA Settings** menu to **RAID** mode. You might also need to change the **Boot Mode** setting to **UEFI**. Otherwise, you should set this field to **Non-RAID** mode.
Boot Settings	Specifies options to specify the Boot mode (BIOS or UEFI). Enables you to modify UEFI and BIOS boot settings.
Network Settings	Specifies options to manage the UEFI network settings and boot protocols. Legacy network settings are managed from the **Device Settings** menu.
Integrated Devices	Specifies options to manage integrated device controllers and ports, specifies related features and options.
Serial Communication	Specifies options to manage the serial ports, its related features and options.
System Profile Settings	Specifies options to change the processor power management settings, memory frequency.
System Security	Specifies options to configure the system security settings, such as system password, setup password, Trusted Platform Module (TPM) security, and UEFI secure boot. It also manages the power button on the system.
Redundant OS Control	Sets the redundant OS info for redundant OS control.
Miscellaneous Settings	Specifies options to change the system date and time.

System Information

You can use the **System Information** screen to view system properties such as Service Tag, system model name, and the BIOS version.

View System Information

To view the **System Information** screen, perform the following steps:

Steps

1. Turn on, or restart your system.
2. Press F2 immediately after you see the following message:

```
F2 = System Setup
```

NOTE: If your operating system begins to load before you press F2, wait for the system to finish booting, and then restart your system and try again.

3. On the **System Setup Main Menu** screen, click **System BIOS**.
4. On the **System BIOS** screen, click **System Information**.

System Information details

About this task

The **System Information** screen details are explained as follows:

Option	Description
System Model Name	Specifies the system model name.

Option	Description
System BIOS Version	Specifies the BIOS version installed on the system.
System Management Engine Version	Specifies the current version of the Management Engine firmware.
System Service Tag	Specifies the system Service Tag.
System Manufacturer	Indicates the name of the Original Equipment Manufacturer (OEM).
System Manufacturer Contact Information	Indicates the contact information of the Original Equipment Manufacturer (OEM).
System CPLD Version	Specifies the current version of the system, complex programmable logic device (CPLD) firmware.
UEFI Compliance Version	Specifies the UEFI compliance level of the system firmware.

Memory Settings

You can use the **Memory Settings** screen to view all the memory settings and enable or disable specific memory functions, such as system memory testing and node interleaving.

View Memory Settings

To view the **Memory Settings** screen, perform the following steps:

Steps

1. Turn on, or restart your system.
2. Press F2 immediately after you see the following message:

```
F2 = System Setup
```

NOTE: If your operating system begins to load before you press F2, wait for the system to finish booting, and then restart your system and try again.

3. On the **System Setup Main Menu** screen, click **System BIOS**.
4. On the **System BIOS** screen, click **Memory Settings**.

Memory Settings details

About this task

The **Memory Settings** screen details are explained as follows:

Option	Description
System Memory Size	Specifies the memory size in the system.
System Memory Type	Specifies the type of memory that is installed in the system.
System Memory Speed	Specifies the system memory speed.

Option	Description
System Memory Voltage	Specifies the system memory voltage.
Video Memory	Specifies the amount of video memory.
System Memory Testing	Specifies whether the system memory tests are run during system boot. Options are **Enabled** and **Disabled**. This option is set to **Disabled** by default. **NOTE:** When **Enabled** the system takes more to boot. The booting time depends on the size of the system memory.
Dram Refresh Delay	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	Specifies the memory operating mode. The options available are **Optimizer Mode**, **Single Rank Spare Mode**, **Multi Rank Spare Mode**, **Mirror Mode**, and **Dell Fault Resilient Mode**. This option is set to **Optimizer Mode** by default. **NOTE:** The **Memory Operating Mode** option can have different default and available options based on the memory configuration of your system. **NOTE:** The **Fault Resilient Mode** option establishes an area of memory that is fault resilient. This mode can be used by an operating system that supports the feature to load critical applications or enables the operating system kernel to maximize system availability. **NOTE:** Only Optimizer Mode should be selected when Intel DC Optane Persistent Memory is installed.
Current State of Memory Operating Mode	Specifies the current state of the memory operating mode.
Fault Resilient Mode Memory Size [%]	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**.
Node Interleaving	Specifies if Non-Uniform Memory Architecture (NUMA) is supported. If this field is set to **Enabled**, memory interleaving is supported if a symmetric memory configuration is installed. If the field is set to **Disabled**, the system supports NUMA (asymmetric) memory configurations. This option is set to **Disabled** by default.
ADDDC Setting	Enables or disables **ADDDC Setting** feature. When Adaptive Double DRAM Device Correction (ADDDC) is enabled, failing DRAMs are dynamically mapped out. When set to **Enabled** it can have some impact to system performance under certain workloads. This feature is applicable for x4 DIMMs only. This option is set to **Disable** by default.
Native tRFC Timing for 16Gb DIMMs	Enables 16 Gb density DIMMs to operate at their programmed Row Refresh Cycle Time (tRFC). Enabling this feature may improve system performance for some configurations. However, enabling this feature will have no effect on configurations with 16 Gb 3DS/TSV DIMMs. This option is set to **Enabled** by default.
Opportunistic Self-Refresh	Enables or disables opportunistic self-refresh feature. This option is set to **Disabled** by default.
Correctable Error Logging	Enables or disables logging of correctable memory threshold error. This option is set to **Disabled** by default.
DIMM Self Healing (Post Package Repair) on Uncorrectable Memory Error	Enable/Disable Post Package Repair (PPR) on Uncorrectable Memory Error. This option is set to **Enabled** by default.
Persistent Memory	This field controls Persistent Memory on the system. This option is available if the persistent memory module is installed in the system.

Processor Settings

You can use the **Processor Settings** screen to view the processor settings, and perform specific functions such as enabling virtualization technology, hardware prefetcher, logical processor idling.

View Processor Settings

To view the **Processor Settings** screen, perform the following steps:

Steps

1. Turn on, or restart your system.
2. Press F2 immediately after you see the following message:

```
F2 = System Setup
```

NOTE: If your operating system begins to load before you press F2, wait for the system to finish booting, and then restart your system and try again.

3. On the **System Setup Main Menu** screen, click **System BIOS**.
4. On the **System BIOS** screen, click **Processor Settings**.

Processor Settings details

About this task

The **Processor Settings** screen details are explained as follows:

Option	Description
Logical Processor	Enables or disables the logical processors and displays the number of logical processors. If this option is set to **Enabled**, the BIOS displays all the logical processors. If this option is set to **Disabled**, the BIOS displays only one logical processor per core. This option is set to **Enabled** by default.
CPU Interconnect Speed	Enables you to govern the frequency of the communication links among the CPUs in the system. **NOTE:** The standard and basic bin processors support lower link frequencies. The options available are **Maximum data rate**, **10.4 GT/s**, and **9.6 GT/s**. This option is set to **Maximum data rate** by default. Maximum data rate indicates that the BIOS runs the communication links at the maximum frequency that is supported by the processors. You can also select specific frequencies that the processors support, which can vary. For best performance, you should select **Maximum data rate**. Any reduction in the communication link frequency affects the performance of nonlocal memory accesses and cache coherency traffic. In addition, it can slow access to nonlocal I/O devices from a particular CPU. However, if power-saving considerations outweigh performance, you might want to reduce the frequency of the CPU communication links. If you do this, you should localize memory and I/O accesses to the nearest NUMA node to minimize the impact to system performance.
Virtualization Technology	Enables or disables the virtualization technology for the processor. This option is set to **Enabled** by default.
Adjacent Cache Line Prefetch	Optimizes the system for applications that need high utilization of sequential memory access. This option is set to **Enabled** by default. You can disable this option for applications that need high utilization of random memory access.
Hardware Prefetcher	Enables or disables the hardware prefetcher. This option is set to **Enabled** by default.
DCU Streamer Prefetcher	Enables or disables the Data Cache Unit (DCU) streamer prefetcher. This option is set to **Enabled** by default.

Option	Description
DCU IP Prefetcher	Enables or disables the Data Cache Unit (DCU) IP prefetcher. This option is set to **Enabled** by default.
Sub NUMA Cluster	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. Enables or disables the Sub NUMA Cluster. This option is set to **Disabled** by default.
UPI Prefetch	Enables you to get the memory read started early on DDR bus. The Ultra Path Interconnect (UPI) Rx path spawns the speculative memory read to Integrated Memory Controller (iMC) directly. This option is set to **Enabled** by default.
LLC Prefetch	Enables or disables the LLC Prefetch on all threads. This option is set to **Disabled** by default.
Dead Line LLC Alloc	When enabled, it opportunistically fill dead lines in LLC. When disabled, it never fill dead lines in LLC. This option is set to **Enabled** by default.
Directory AtoS	AtoS optimization reduces remote read latencies for repeat read accesses without intervening writes. This option is set to **Disabled** by default.
FastGo	Enables you to select CR OOS Configuration Profiles.
IRQ Throttle	Enables you to throttle local requests that are targeting a remote address.
Logical Processor Idling	Enables you to improve the energy efficiency of a system. It uses the operating system core parking algorithm and parks some of the logical processors in the system which in turn allows the corresponding processor cores to transition into a lower power idle state. This option can only be enabled if the operating system supports it. It is set to **Disabled** by default. **NOTE:** This feature is not supported if CPU Power Management is set to Maximum Performance.
Configurable TDP	Enables you to configure the TDP level. The available options are **Nominal**, **Level 1** and **Level 2**. This option is set to **Nominal** by default. **NOTE:** This option is only available on certain stock keeping units (SKUs) of the processors.
x2APIC Mode	Enables or disables the x2APIC mode. This option is set to **Enabled** by default.
L2 RFO Prefetch	Enables or disables the L2 RFO (Read For Ownership) prefetch. This option is set to **Enabled** by default. The RFO is the process of reading a cache line from the memory into the cache before it can be written to. **NOTE:** This feature is supported only when four processors are installed.
Dell Controlled Turbo	Controls the turbo engagement. Enable this option only when **System Profile** is set to **Performance**. **NOTE:** Depending on the number of installed CPUs, there might be up to four processor listings.
Dell AVX Scaling Technology	Enables you to configure the Dell AVX scaling technology. This option is set to **0** by default.
AVX ICCP Pre-Grant	Allows the system to select between different AVX ICCP transition levels offered by Intel. The default level is 128 Heavy.
Number of Cores per Processor	Controls the number of enabled cores in the processor. Under certain circumstances, you may see limited performance improvements to Intel Turbo Boost Technology and benefits from potentially larger shared caches, when you reduce the number of enabled cores. Most computing environments tend to benefit more from larger number of processing cores, so you must carefully weigh the disabling of cores to gain nominal performance enhancements.
Process Core Speed	Displays the core speed of the processor(s).
Process Bus Speed	Displays the bus speed of the processor(s).
Processor n	The following settings are displayed for each processor installed in the system:

Option	Description

Option	Description
Family-Model-Stepping	Specifies the family, model, and stepping of the processor as defined by Intel.
Brand	Specifies the brand name.
Level 2 Cache	Specifies the total L2 cache.
Level 3 Cache	Specifies the total L3 cache.
Number of Cores	Specifies the number of cores per processor.
Maximum Memory Capacity	Specifies the maximum memory capacity per processor.
Microcode	Specifies the microcode.

SATA Settings

You can use the **SATA Settings** screen to view the SATA settings of SATA devices and enable SATA and PCIe NVMe RAID mode on your system.

NOTE: Dell Storage NX system does not support HDDs connected to SATA ports and does not enable SATA RAID Mode. It supports only PERC RAID Controller.

View SATA Settings

To view the **SATA Settings** screen, perform the following steps:

Steps

1. Turn on, or restart your system.
2. Press F2 immediately after you see the following message:

```
F2 = System Setup
```

NOTE: If your operating system begins to load before you press F2, wait for the system to finish booting, and then restart your system and try again.

3. On the **System Setup Main Menu** screen, click **System BIOS**.
4. On the **System BIOS** screen, click **SATA Settings**.

SATA Settings details

About this task

The **SATA Settings** screen details are explained as follows:

Option	Description
Embedded SATA	Enables the embedded SATA option to be set to **Off** , **AHCI**, or **RAID** modes. This option is set to **AHCI Mode** by default.
Security Freeze Lock	Sends **Security Freeze Lock** command to the embedded SATA drives during POST. This option is set to **Enabled** by default.
Write Cache	Enables or disables the command for the embedded SATA drives during POST. This option is set to **Disabled** by default.
Port n	Sets the drive type of the selected device. For **AHCI Mode** or **RAID Mode**, BIOS support is always enabled.

Option	Description

Option	Description
Model	Specifies the drive model of the selected device. **NOTE:** If no device is installed, it displays **Unkown**.
Drive Type	Specifies the type of drive attached to the SATA port. **NOTE:** If no device is installed, it displays **Unkown Device**.
Capacity	Specifies the total capacity of the drive. This field is undefined for removable media devices such as optical drives. **NOTE:** If no device is installed, it displays **N/A**.

NVMe Settings

The NVMe settings enable you to set the NVMe drives to either **RAID** mode or **Non-RAID** mode.

NOTE: To configure these drives as RAID drives, click **System BIOS Settings** > **SATA Settings** > **Embedded SATA Option** and enable **RAID** mode. If not, you must set this field to **Non-RAID** mode.

View NVMe settings

To view the **NVMe Settings** screen, perform the following steps:

Steps

1. Turn on, or restart your system.
2. Press F2 immediately after you see the following message:

```
F2 = System Setup
```

NOTE: If your operating system begins to load before you press F2, wait for the system to finish booting, and then restart your system and try again.

3. On the **System Setup Main Menu** screen, click **System BIOS**.
4. On the **System BIOS** screen, click **NVMe Settings**.

NVMe Settings details

About this task

The **NVMe Settings** screen details are explained as follows:

Option	Description
NVMe Mode	Enables you to set the NVMe mode. This option is set to **Non RAID** by default.

Boot Settings

You can use the **Boot Settings** screen to set the boot mode to either **BIOS** or **UEFI**. It also enables you to specify the boot order.

- **BIOS**: The **BIOS Boot Mode** is the legacy boot mode. It is maintained for backward compatibility.
- **UEFI**: The Unified Extensible Firmware Interface (UEFI) is a new interface between operating systems and platform firmware. The interface consists of data tables with platform related information, also boot and runtime service calls that are available to the operating system and its loader. The following benefits are available when the **Boot Mode** is set to **UEFI**:

- Support for drive partitions larger than 2 TB.
- Enhanced security (e.g., UEFI Secure Boot).
- Faster boot time.

NOTE: You must use only the UEFI boot mode in order to boot from NVMe drives.

View Boot Settings

To view the **Boot Settings** screen, perform the following steps:

Steps

1. Turn on, or restart your system.
2. Press F2 immediately after you see the following message:

```
F2 = System Setup
```

NOTE: If your operating system begins to load before you press F2, wait for the system to finish booting, and then restart your system and try again.

3. On the **System Setup Main Menu** screen, click **System BIOS**.
4. On the **System BIOS** screen, click **Boot Settings**.

Boot Settings details

About this task

The **Boot Settings** screen details are explained as follows:

Option	Description
Boot Mode	Allows you to configure the Boot Sequence and Enable or Disable the individual boot options. The available options are **BIOS** and **UEFI**. The option is set to **UEFI** by default.
Boot Sequence Retry	Enables or disables the **Boot Sequence Retry** feature. If the last attempt to boot has failed, the system immediately performs a cold reset or retries to boot after 30 seconds time-out period base on the setting of **Reset** or **Enabled**. This option is set to **Enabled** by default.
Hard-Disk Failover	Specifies the drive that is booted in the event of a drive failure. The devices are selected in the **Hard-Disk Drive Sequence** on the **Boot Option Setting** menu. When this option is set to **Disabled**, only the first drive in the list is attempted to boot. When this option is set to **Enabled**, all drives are attempted to boot in the order selected in the **Hard-Disk Drive Sequence**. This option is not enabled for **UEFI Boot Mode**. This option is set to **Disabled** by default.
Generic USB Boot	Enables or disables the USB boot option. This option is set to **Disabled** by default.
Hard-disk Drive Placeholder	Enables or disables the Hard-disk Drive Placeholder option. This option is set to **disabled** by default.

UEFI Boot Settings

The **UEFI Boot Settings** screen enables you to specify the UEFI boot order.

About this task

Option	Description
UEFI Boot Sequence	Enables you to change the **UEFI** boot device order.
Boot Options Enable/Disable	Enables you to enable or disable the **UEFI** boot devices.

Network Settings

You can use the **Network Settings** screen to modify UEFI PXE, iSCSI, and HTTP boot settings. The network settings option is available only in the UEFI mode.

NOTE: The BIOS does not control network settings in the BIOS mode. For the BIOS boot mode, the optional Boot ROM of the network controllers handles the network settings.

Viewing Network Settings

To view the **Network Settings** screen, perform the following steps:

Steps

1. Turn on, or restart your system.
2. Press F2 immediately after you see the following message:

```
F2 = System Setup
```

NOTE: If your operating system begins to load before you press F2, wait for the system to finish booting, and then restart your system and try again.

3. On the **System Setup Main Menu** screen, click **System BIOS**.
4. On the **System BIOS** screen, click **Network Settings**.

Network Settings screen details

The **Network Settings** screen details are explained as follows:

About this task

Option	Description
UEFI PXE Settings	Enables you to control the configuration of the UEFI PXE device.
PXE Device n (n = 1 to 4)	Enables or disables the device. When enabled, a UEFI PXE boot option is created for the device.
PXE Device n Settings(n = 1 to 4)	Enables you to control the configuration of the PXE device.
UEFI HTTP Settings	Enables or disables the device. When enabled, a UEFI HTTP boot option is created for the device.
HTTP Device n Settings (n = 1 to 4)	Enables you to control the configuration of the HTTP device.
UEFI iSCSI Settings	Enables you to control the configuration of the iSCSI device.

Table 1. UEFI iSCSI Settings screen details

Option	Description
iSCSI Initiator Name	Specifies the name of the iSCSI initiator in IQN format.
iSCSI Device1	Enables or disables the iSCSI device. When disabled, a UEFI boot option is created for the iSCSI device automatically. This is set to **Disabled** by default.

Option	Description

Table 1. UEFI iSCSI Settings screen details (continued)

Option	Description
iSCSI Device1 Settings	Enables you to control the configuration of the iSCSI device.

TLS Authentication Configuration	View and/or modify this device's boot TLS authentication mode. None means the HTTP server and the client will not authenticate each other for this boot. One way means the HTTP server will be authenticated by the client, while the client will not be authenticated by the server. This option is set to **None** by default.

Integrated Devices

You can use the **Integrated Devices** screen to view and configure the settings of all integrated devices including the video controller, integrated RAID controller, and the USB ports.

Viewing Integrated Devices

To view the **Integrated Devices** screen, perform the following steps:

Steps

1. Power on or restart the system.
2. Press F2 immediately after you see the following message:

```
F2 = System Setup
```

NOTE: If your operating system begins to load before you press F2, wait for the system to finish booting, and then restart your system and try again.

3. On the **System Setup Main Menu** screen, click **System BIOS**.
4. On the **System BIOS** screen, click **Integrated Devices**.

Integrated Devices details

About this task

The **Integrated Devices** screen details are explained as follows:

Option	Description
User Accessible USB Ports	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; selecting **All Ports Off (Dynamic)** disables all front and back USB ports during POST and front ports can be enabled or disabled dynamically by authorized user without resetting the system. The USB keyboard and mouse still function in certain USB ports during the boot process, depending on the selection. After the boot process is complete, the USB ports will be enabled or disabled as per the setting.
Internal USB Port	Enables or disables the internal USB port. This option is set to **On** by default.
iDRAC Direct USB Port	The iDRAC Direct USB port is managed by iDRAC exclusively with no host visibility. This option is set to **ON** or **OFF**. When set to **OFF**, iDRAC does not detect any USB devices installed in this managed port. This option is set to **On** by default.
Integrated Network Card 1	Enables or disables the integrated network card (NDC). When set to **Disabled**, the NDC is not available to the operating system (OS). This option is set to **Enabled** by default.

Option	Description
	NOTE: If set to **Disabled** (OS), the Integrated NICs might still be available for shared network access by iDRAC.
I/OAT DMA Engine	Enables or disables 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. Enable only if the hardware and software support the feature.
I/O Snoop HoldOff Response	Enables you to select 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.
Embedded Video Controller	Enables or disables the use of Embedded Video Controller as the primary display. When set to **Enabled**, the Embedded Video Controller will be the primary display even if add-in graphic cards are installed. When set to **Disabled**, an add-in graphics card will be used as the primary display. BIOS will output displays to both the primary add-in video and the embedded video during POST and pre-boot environment. The embedded video will then be disabled right before the operating system boots. This option is set to **Enabled** by default. **NOTE:** When there are multiple add-in graphic cards installed in the system, the first card discovered during PCI enumeration is selected as the primary video. You might have to re-arrange the cards in the slots in order to control which card is the primary video.
Current State of Embedded Video Controller	Displays the current state of the embedded video controller. The **Current State of Embedded Video Controller** option is a read-only field. If the Embedded Video Controller is the only display capability in the system (that is, no add-in graphics card is installed), then the Embedded Video Controller is automatically used as the primary display even if the **Embedded Video Controller** setting is set to **Disabled**.
SR-IOV Global Enable	Enables or disables the BIOS configuration of Single Root I/O Virtualization (SR-IOV) devices. This option is set to **Disabled** by default.
OS Watchdog Timer	If your system stops responding, this watchdog timer aids in the recovery of your operating system. When this option is set to **Enabled**, the operating system initializes the timer. When this option is set to **Disabled** (the default), the timer does not have any effect on the system.
Empty Slot Unhide	Enables or disables the root ports of all the empty slots that are accessible to the BIOS and OS. This option is set to **Disabled** by default.
Memory Mapped I/O above 4 GB	Enables or disables the support for the PCIe devices that need large amounts of memory. Enable this option only for 64-bit operating systems. This option is set to **Enabled** by default.
Memory Mapped I/O Base	When set to **12 TB**, the system will map MMIO base to 12 TB. Enable this option for an OS that requires 44 bit PCIe addressing.
PCIe Bus Customization	Provide options for customizing the allocation of PCIe bus ranges to PCIe slot 5 and12 in R940xa.

Slot Disablement

About this task

The **Slot Disablement** screen details are explained as follows:

Slot Disablement Enables or disables the available PCIe slots on your system. The slot disablement feature controls the configuration of the PCIe cards installed in the specified slot. Slots must be disabled only when the installed peripheral card prevents booting into the operating system or causes delays in system startup. If the slot is disabled, both the Option ROM and UEFI drivers are disabled. Only slots that are present on the system will be available for control.

Table 2. Slot Disablement

Slot number	Description
Slot 1	Enables or disables or only the boot driver is disabled for the PCIe slot 1. This option is set to **Enabled** by default.

Table 2. Slot Disablement (continued)

Slot number	Description
Slot 2	Enables or disables or only the boot driver is disabled for the PCIe slot 2. This option is set to **Enabled** by default.
Slot 3	Enables or disables or only the boot driver is disabled for the PCIe slot 3. This option is set to **Enabled** by default.
Slot 4	Enables or disables or only the boot driver is disabled for the PCIe slot 4. This option is set to **Enabled** by default.
Slot 5	Enables or disables or only the boot driver is disabled for the PCIe slot 5. This option is set to **Enabled** by default.
Slot 6	Enables or disables or only the boot driver is disabled for the PCIe slot 6. This option is set to **Enabled** by default.
Slot 7	Enables or disables or only the boot driver is disabled for the PCIe slot 7. This option is set to **Enabled** by default.
Slot 8	Enables or disables or only the boot driver is disabled for the PCIe slot 8. This option is set to **Enabled** by default.
Slot 9	Enables or disables or only the boot driver is disabled for the PCIe slot 9. This option is set to **Enabled** by default.
Slot 10	Enables or disables or only the boot driver is disabled for the PCIe slot 10. This option is set to **Enabled** by default.
Slot 11	Enables or disables or only the boot driver is disabled for the PCIe slot 11. This option is set to **Enabled** by default.
Slot 12	Enables or disables or only the boot driver is disabled for the PCIe slot 12. This option is set to **Enabled** by default.

Slot Bifurcation

About this task

The **Slot Bifurcation** screen details are explained as follows:

Slot Bifurcation Allows **Platform Default Bifurcation**, **Auto discovery of Bifurcation** and **Manual bifurcation Control**. The default is set to **Platform Default Bifurcation**. The slot bifurcation field is accessible when set to **Manual bifurcation Control** and is grayed out when set to **Platform Default Bifurcation** or **Auto discovery of Bifurcation**.

Table 3. Slot Bifurcation

Option	x16 PCIe riser 1 and 2 configuration	x8 PCIe riser 1 and 2 configuration
Auto Discovery Bifurcation Settings	Platform Default Bifurcation, Auto Bifurcation, Manual bifurcation	Platform Default Bifurcation, Auto Bifurcation, Manual bifurcation
Slot 1 Bifurcation	NA	x4 or x8 Bifurcation
Slot 2 Bifurcation	x4 or x8 or x16, or x4, x4, x8, or x8, x4,x4 Bifurcation	x4 or x8 Bifurcation
Slot 3 Bifurcation	NA	x4 or x8 Bifurcation
Slot 4 Bifurcation	x4 or x8 or x16, or x4, x4, x8, or x8, x4,x4 Bifurcation	x4 or x8 Bifurcation

Table 3. Slot Bifurcation (continued)

Option	x16 PCIe riser 1 and 2 configuration	x8 PCIe riser 1 and 2 configuration
Slot 5 Bifurcation	x4 or x8 Bifurcation	x4 or x8 Bifurcation
Slot 6 Bifurcation	x4 or x8 or x16, or x4, x4, x8, or x8, x4,x4 Bifurcation	x4 or x8 or x16, or x4, x4, x8, or x8, x4,x4 Bifurcation
Slot 7 Bifurcation	x4 or x8 or x16, or x4, x4, x8, or x8, x4,x4 Bifurcation	x4 or x8 or x16, or x4, x4, x8, or x8, x4,x4 Bifurcation
Slot 8 Bifurcation	NA	x4 or x8 Bifurcation
Slot 9 Bifurcation	x4 or x8 or x16, or x4, x4, x8, or x8, x4,x4 Bifurcation	x4 or x8 Bifurcation
Slot 10 Bifurcation	NA	x4 or x8 Bifurcation
Slot 11 Bifurcation	x4 or x8 or x16, or x4, x4, x8, or x8, x4,x4 Bifurcation	x4 or x8 Bifurcation
Slot 12 Bifurcation	x4 or x8 Bifurcation	x4 or x8 Bifurcation

Serial Communication

Use the **Serial Communication** screen to view the properties of the serial communication port.

Viewing Serial Communication

To view the **Serial Communication** screen, perform the following steps:

Steps

1. Power on or restart the system.
2. Press F2 immediately after you see the following message:

```
F2 = System Setup
```

NOTE: If your operating system begins to load before you press F2, wait for the system to finish booting, and then restart your system and try again.

3. On the **System Setup Main Menu** screen, click **System BIOS**.
4. On the **System BIOS** screen, click **Serial Communication**.

Serial Communication details

About this task

The **Serial Communication** screen details are explained as follows:

Option	Description
Serial Communication	Selects serial communication devices (Serial Device 1 and Serial Device 2) in BIOS. BIOS console redirection can also be enabled, and the port address can be specified. This option is set to **Auto** by default. Enables the **COM** port or **Console Redirection** options. This option is set to **Off** by default.
Serial Port Address	Enables you to set the port address for serial devices. This field sets the serial port address to either COM1 or COM2 (COM1=0x3F8, COM2=0x2F8). This option is set to **Serial Device 1=COM2, Serial Device 2=COM1** by default.

Option	Description
	NOTE: You can use only Serial Device 2 for the 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	Enables you to associate the External Serial Connector to **Serial Device 1**, **Serial Device 2**, or the **Remote Access Device** by using this option. This option is set to **Serial Device 1** by default. **NOTE:** Only Serial Device 2 can be used for Serial Over LAN (SOL). To use console redirection by SOL, configure the same port address for console redirection and the serial device. **NOTE:** Every time the system boots, the BIOS syncs the serial MUX setting saved in iDRAC. The serial MUX setting can independently be changed in iDRAC. Loading the BIOS default settings from within the BIOS setup utility may not always revert this setting to the default setting of Serial Device 1. Enables you to associate the External Serial Connector to Serial Device 1.
Failsafe Baud Rate	Specifies the failsafe baud rate for console redirection. The BIOS attempts to determine the baud rate automatically. This failsafe baud rate is used only if the attempt fails, and the value must not be changed. This option is set to **115200** by default.
Remote Terminal Type	Sets the remote console terminal type. This option is set to **VT100/VT220** by default.
Redirection After Boot	Enables or disables the BIOS console redirection when the operating system is loaded. This option is set to **Enabled** by default.

System Profile Settings

You can use the **System Profile Settings** screen to enable specific system performance settings such as power management.

Viewing System Profile Settings

To view the **System Profile Settings** screen, perform the following steps:

Steps

1. Power on, or restart your system.
2. Press F2 immediately after you see the following message:

```
F2 = System Setup
```

NOTE: If your operating system begins to load before you press F2, wait for the system to finish booting, and then restart your system and try again.

3. On the **System Setup Main Menu** screen, click **System BIOS**.
4. On the **System BIOS** screen, click **System Profile Settings**.

System Profile Settings details

About this task

The **System Profile Settings** screen details are explained as follows:

Option	Description
System Profile	Sets the system profile. If you set the System Profile option to a mode other than **Custom**, the BIOS automatically sets the rest of the options. You can only change the rest of the options if the mode is set to **Custom**. This option is set to **Performance Per Watt Optimized (DAPC)** by default. DAPC is Dell Active Power Controller.Other options include **Performance Per Watt (OS)**, **Performance**, and **Workstation Performance**.

Option	Description
	NOTE: All the parameters on the system profile setting screen are available only when the **System Profile** option is set to **Custom**.
CPU Power Management	Sets the CPU power management. This option is set to **System DBPM (DAPC)** by default. DBPM is Demand-Based Power Management.
Memory Frequency	Sets the speed of the system memory. You can select **Maximum Performance** or a specific speed. This option is set to **Maximum Performance** by default.
Turbo Boost	Enables or disables the processor to operate in the turbo boost mode. This option is set to **Enabled** by default.
C1E	Enables or disables the processor to switch to a minimum performance state when it is idle. This option is set to **Enabled** by default.
C States	Enables or disables the processor to operate in all available power states. This option is set to **Enabled** by default.
Write Data CRC	Enables or disables the Write Data CRC. This option is set to **Disabled** by default.
Memory Patrol Scrub	Sets the memory patrol scrub frequency. This option is set to **Standard** by default.
Memory Refresh Rate	Sets the memory refresh rate to either 1x or 2x. This option is set to **1x** by default.
Uncore Frequency	Enables you to select the **Processor Uncore Frequency** option. **Dynamic mode** enables 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 Efficiency Policy** option.
Energy Efficient Policy	Enables you to select the **Energy Efficient Policy** option. The CPU uses the setting to manipulate the internal behavior of the processor and determines whether to target higher performance or better power savings. This option is set to **Balanced Performance** by default.
Number of Turbo Boost Enabled Cores for Processor 1	**NOTE:** If there are four processors installed in the system, you will see an entry for **Number of Turbo Boost Enabled Cores for Processor 4**. Controls the number of turbo boost enabled cores for Processor 1. The maximum number of cores is All by default.
Monitor/Mwait	Enables the Monitor/Mwait instructions in the processor. This option is set to **Enabled** for all system profiles, except **Custom** by default. **NOTE:** This option can be disabled only if the **C States** option in the **Custom** mode is set to **disabled**. **NOTE:** When **C States** is set to **Enabled** in the **Custom** mode, changing the Monitor/Mwait setting does not impact the system power or performance.
CPU Interconnect Bus Link Power Management	Enables or disables the CPU Interconnect Bus Link Power Management. This option is set to **Enabled** by default.
PCI ASPM L1 Link Power Management	Enables or disables the PCI ASPM L1 Link Power Management. This option is set to **Enabled** by default.
Intel Persistent Memory CR QoS	Controls the tuning function for Quality of Service (QoS) knobs. **Disabled** by default. **Recipe 1** is recommended for 2-2-2 memory configurations in App-Direct. **Recipe 2** is recommended for other memory configurations in App-Direct. **Recipe 3** is recommended for 1 DIMM per channel configurations.
Intel Persistent Memory	Controls the thresholds that trigger switching between near (RDIMM/LRDIMM) and far (DCPMM) memory. **BW Optimized**, selected by default, optimizes for RDIMM/LRDIMM and DCPMM bandwidth.

Performance Setting	**Latency Optimized** offers better RDIMM/LRDIMM latency in the presence of DCPMM. **Balanced Profile** optimizes performance with Memory Mode-configured DCPMM.

System Security

You can use the **System Security** screen to perform specific functions such as setting the system password, setup password and disabling the power button.

Viewing System Security

To view the **System Security** screen, perform the following steps:

Steps

1. Turn on, or restart your system.
2. Press F2 immediately after you see the following message:

```
F2 = System Setup
```

NOTE: If your operating system begins to load before you press F2, wait for the system to finish booting, and then restart your system and try again.

3. On the **System Setup Main Menu** screen, click **System BIOS**.
4. On the **System BIOS** screen, click **System Security**.

System Security Settings details

About this task

The **System Security Settings** screen details are explained as follows:

Option	Description
CPU AES-NI	Improves the speed of applications by performing encryption and decryption by using the Advanced Encryption Standard Instruction Set (AES-NI). This option is set to **Enabled** by default.
System Password	Sets the system password. This option is set to **Enabled** by default and is read-only if the password jumper is not installed in the system.
Setup Password	Sets the setup password. This option is read-only if the password jumper is not installed in the system.
Password Status	Locks the system password. This option is set to **Unlocked** by default.
TPM Information	**NOTE:** The TPM menu is available only when the TPM module is installed. Enables you to control the reporting mode of the TPM. The **TPM Security** option is set to **Off** by default. You can only modify the TPM Status, and TPM Activation, and the Intel TXT fields if the **TPM Status** field is set to either **On with Pre-boot Measurements** or **On without Pre-boot Measurements**. When TPM 1.2 is installed, the **TPM Security** option is set to **Off**, **On with Pre-boot Measurements**, or **On without Pre-boot Measurements**.

Table 4. TPM 1.2 security information

TPM information	Description
TPM Information	Changes the operational state of the TPM. This option is set to **Type: 1.2-NTC** by default.
TPM Firmware	Indicates the firmware version of the TPM.
TPM Status	Specifies the TPM status.

Option	Description

Table 4. TPM 1.2 security information (continued)

TPM information	Description
TPM Command	Controls the Trusted Platform Module (TPM). When set to **None**, no command is sent to the TPM. When set to **Activate**, the TPM is enabled and activated. When set to **Deactivate**, the TPM is disabled and deactivated. When set to **Clear**, all the contents of the TPM are cleared. This option is set to **None** by default.

When TPM 2.0 is installed, the **TPM Security** option is set to **On** or **Off**. This option is set to **Off** by default.

Table 5. TPM 2.0 security information

TPM information	Description
TPM Information	Changes the operational state of the TPM. This option is set to **Type: 2.0-NTC** by default.
TPM Firmware	Indicates the firmware version of the TPM.
TPM Hierarcy	Enable, disable, or clear the storage and endorsement hierarchies. When set to **Enabled**, the storage and endorsement hierarchies can be used. When set to **Disabled**, the storage and endorsement hierarchies cannot be used. When set to **Clear**, the storage and endorsement hierarchies are cleared of any values, and then reset to **Enabled**.

TPM Advanced Settings

This setting is enabled only when TPM Security is set to ON.

Table 6. TPM Advanced Settings Details

Option	Description
TPM PPI Bypass Provision	When set to **Enabled** allows the Operating System to bypass Physical Presence Interface (PPI), prompts when issuing PPI Advanced Configuration and Power Interface (ACPI) provisioning operations. This option is set to **Disabled** by default.
TPM PPI Bypass Clear	When set to **Enabled** allows the Operating System to bypass Physical Presence Interface (PPI), prompts when issuing PPI Advanced Configuration and Power Interface (ACPI) provisioning operations. This option is set to **Disabled** by default.

Intel(R) TXT

Enables or disables the Intel Trusted Execution Technology (TXT) option. To enable the **Intel TXT** option, virtualization technology and TPM Security must be enabled with Pre-boot measurements. This option is set to **Off** by default.

When TPM 2.0 is installed, **TPM 2 Algorithm** option is available. It enables you to select a hash algorithm from those supported by the TPM (SHA1, SHA256). **TPM 2 Algorithm** option must be set to **SHA256**, to enable TXT.

Power Button

Enables or disables the power button on the front of the system. This option is set to **Enabled** by default.

AC Power Recovery

Sets how the system behaves after AC power is restored to the system. This option is set to **Last** by default.

AC Power Recovery Delay

Sets the time delay for the system to power up after AC power is restored to the system. This option is set to **Immediate** by default.

Option	Description
User Defined Delay (60 s to 600 s)	Sets the **User Defined Delay** option when the **User Defined** option for **AC Power Recovery Delay** is selected.
UEFI Variable Access	Provides varying degrees of securing UEFI variables. When set to **Standard** (the default), UEFI variables are accessible in the operating system per the UEFI specification. When set to **Controlled**, selected UEFI variables are protected in the environment and new UEFI boot entries are forced to be at the end of the current boot order.
In-Band Manageability Interface	When set to **Disabled**, this setting will hide the Management Engine's (ME), HECI devices, and the system's IPMI devices from the operating system. This prevents the operating system from changing the ME power capping settings, and blocks access to all in-band management tools. All management should be managed through out-of-band. This option is set to **Enabled** by default. **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 updating errors.
Secure Boot	Enables Secure Boot, where the BIOS authenticates each pre-boot image by using the certificates in the Secure Boot Policy. Secure Boot is set to **Disabled** by default.
Secure Boot Policy	When Secure Boot policy is set to **Standard**, the BIOS uses the system manufacturer's key and certificates to authenticate pre-boot images. When Secure Boot policy is set to **Custom**, the BIOS uses the user-defined key and certificates. Secure Boot policy is set to **Standard** by default.
Secure Boot Mode	Configures how the BIOS uses the Secure Boot Policy Objects (PK, KEK, db, dbx). If the current mode is set to **Deployed Mode**, the available options are **User Mode** and **Deployed Mode**. If the current mode is set to **User Mode**, the available options are **User Mode**, **Audit Mode**, and **Deployed Mode**.

Options	Description
User Mode	In **User Mode**, PK must be installed, and BIOS performs signature verification on programmatic attempts to update policy objects. The BIOS allows unauthenticated programmatic transitions between modes.
Deployed Mode	**Deployed Mode** is the most secure mode. In **Deployed Mode**, PK must be installed and the BIOS performs signature verification on programmatic attempts to update policy objects. **Deployed Mode** restricts the programmatic mode transitions.

Secure Boot Policy Summary

About this task

The **Secure Boot Policy Summary** screen details are explained as follows:

Secure Boot Policy Summary	Specifies the list of certificates and hashes that secure boot uses to authenticate images.

Secure Boot Custom Policy Settings

About this task

The **Secure Boot Custom Policy Settings** screen details are explained as follows:

Secure Boot Custom Policy Settings	Configures the Secure Boot Custom Policy. To enable this option, set the Secure Boot Policy to **Custom** option.

Redundant OS Control

You can use the **Redundant OS Control** screen to set the redundant OS info for redundant OS control. It enables you to set up a physical recovery disk on your system.

Viewing Redundant OS Control

To view the **Redundant OS Control** screen, perform the following steps:

Steps

1. Turn on, or restart your system.
2. Press F2 immediately after you see the following message:

```
F2 = System Setup
```

NOTE: If your operating system begins to load before you press F2, wait for the system to finish booting, and then restart your system and try again.

3. On the **System Setup Main Menu** screen, click **System BIOS**.
4. On the **System BIOS** screen, click **Redundant OS Control**.

Redundant OS Control screen details

The **Redundant OS Control** screen details are explained as follows:

About this task

Option	Description
Redundant OS Location	Enables you to select a backup disk from the following devices: • **None** • **Internal SD card** • **SATA Ports in AHCI mode** • **BOSS PCIe cards (Internal M.2 Drives)** • **Internal USB** **NOTE:** RAID configurations and NVMe cards not are included as BIOS does not have the ability to distinguish between individual drives in those configurations.
Redundant OS State	**NOTE:** This option is disabled if Redundant OS Location is set to None. When set to **Visible**, the backup disk is visible to the boot list and OS. When set to **Hidden**, the backup disk is disabled and is not visible to the boot list and OS. This option is set to **Visible** by default. **NOTE:** BIOS will disable the device in hardware, so it cannot be accessed by the OS.
Redundant OS Boot	**NOTE:** This option is disabled if Redundant OS Location is set to None or if Redundant OS State is set to Hidden. When set to **Enabled**, BIOS boots to the device specified in **Redundant OS Location**. When set to **Disabled**, BIOS preserves the current boot list settings. This option is set to **Disabled** by default.

Miscellaneous Settings

You can use the **Miscellaneous Settings** screen to perform specific functions such as updating the asset tag and changing the system date and time.

View Miscellaneous Settings

To view the **Miscellaneous Settings** screen, perform the following steps:

Steps

1. Turn on, or restart your system.
2. Press F2 immediately after you see the following message:

```
F2 = System Setup
```

NOTE: If your operating system begins to load before you press F2, wait for the system to finish booting, and then restart your system and try again.

3. On the **System Setup Main Menu** screen, click **System BIOS**.
4. On the **System BIOS** screen, click **Miscellaneous Settings**.

Miscellaneous Settings details

About this task

The **Miscellaneous Settings** screen details are explained as follows:

Option	Description
System Time	Enables you to set the time on the system.
System Date	Enables you to set the date on the system.
Asset Tag	Specifies the asset tag and enables you to modify it for security and tracking purposes.
Keyboard NumLock	Enables you to set whether the system boots with the NumLock enabled or disabled. This option is set to **On** by default. **NOTE:** This option does not apply to 84-key keyboards.
F1/F2 Prompt on Error	Enables or disables the F1/F2 prompt on error. This option is set to **Enabled** by default. The F1/F2 prompt also includes keyboard errors.
Load Legacy Video Option ROM	Enables you to determine whether the system BIOS loads the legacy video (INT 10H) option ROM from the video controller. Selecting **Enabled** if the operating system does not support UEFI video output standards. This field is available only for UEFI boot mode. You cannot set the option to **Enabled** if **UEFI Secure Boot** mode is enabled. This option is set to **Disabled** by default.
Dell Wyse P25/P45 BIOS Access	Enables or disables the Dell Wyse P25/P45 BIOS Access. This option is set to **Enabled** by default.
Power Cycle Request	Enables or disables the Power Cycle Request. This option is set to **None** by default.

iDRAC Settings utility

The iDRAC settings utility is an interface to set up and configure the iDRAC parameters by using UEFI. You can enable or disable various iDRAC parameters by using the iDRAC settings utility.

NOTE: Accessing some of the features on the iDRAC settings utility needs the iDRAC Enterprise License upgrade.

For more information about using iDRAC, see *Dell Integrated Dell Remote Access Controller User's Guide* at www.dell.com/idracmanuals.

Device Settings

Device Settings enables you to configure the device parameters.

Dell Lifecycle Controller

The Dell Lifecycle Controller (LC) provides advanced embedded systems management capabilities, including system deployment, configuration, update, maintenance, and diagnosis. LC is delivered as part of the iDRAC out-of-band solution and Dell system embedded Unified Extensible Firmware Interface (UEFI) applications.

Embedded System Management

The Dell Lifecycle Controller provides advanced embedded system management throughout the system's lifecycle. The Dell Lifecycle Controller can be started during the boot sequence and can function independently of the operating system.

NOTE: Certain platform configurations may not support the full set of features provided by the Dell Lifecycle Controller.

For more information about setting up the Dell Lifecycle Controller, configuring hardware and firmware, and deploying the operating system, see the Dell Lifecycle Controller documentation at www.dell.com/idracmanuals.

Boot Manager

The **Boot Manager** screen enables you to select boot options and diagnostic utilities.

View the boot manager

Perform the following steps to enter the boot manager.

Steps

1. Turn on, or restart your system.
   Enter the result of your step here (optional).
2. Press F11 when you see the following message:

   ```
   F11 = Boot Manager
   ```

   If your operating system begins to load before you press F11, allow the system to complete the booting, and then restart your system and try again.

Boot Manager main menu

Menu item	Description
Continue Normal Boot	The system attempts to boot to devices starting with the first item in the boot order. If the boot attempt fails, the system continues with the next item in the boot order until the boot is successful or no more boot options are found.
One-shot UEFI Boot menu	Enables you to access the UEFI Boot menu and select an one-shot boot option to boot from.
Launch System Setup	Enables you to access System Setup.

Menu item	Description
Launch Lifecycle Controller	Exits the Boot Manager and invokes the Dell Lifecycle Controller program.
System Utilities	Enables you to launch System Utilities menu such as System Diagnostics and UEFI shell.

One-shot UEFI Boot menu

One-shot UEFI Boot menu enables you to access the UEFI Boot menu and select an one-shot boot option to boot from.

System Utilities

System Utilities contains the following utilities that can be launched:

- Launch Diagnostics
- BIOS Update File Explorer
- Reboot System

PXE boot

You can use the Preboot Execution Environment (PXE) option to boot and configure the networked systems remotely.

To access the **PXE boot** option, boot the system and then press F12 during POST instead of using standard Boot Sequence from BIOS Setup. It does not pull any menu or allow managing network devices.