

# Dell EMC PowerEdge R740xd2

## BIOS and UEFI Reference Guide

## 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.

<b>Chapter 1: Pre-operating system management applications.....</b>	<b>4</b>
Options to manage the pre-operating system applications.....	4
System Setup.....	4
Viewing System Setup.....	4
System Setup details.....	5
System BIOS.....	5
iDRAC Settings utility.....	26
Device Settings.....	27
Dell Lifecycle Controller.....	27
Embedded system management.....	27
Boot Manager.....	27
Viewing Boot Manager.....	27
Boot Manager main menu.....	27
One-shot UEFI boot menu.....	28
System Utilities.....	28
PXE boot.....	28

# 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](#)
- [System Setup](#)
- [Dell Lifecycle Controller](#)
- [Boot Manager](#)
- [PXE boot](#)


## 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, 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 one of the following:

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


## Viewing System Setup

To view the **System Setup** 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.

## System Setup details

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

Option	Description
<b>System BIOS</b>	Enables you to configure BIOS settings.
<b>iDRAC Settings</b>	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 <i>Integrated Dell Remote Access Controller User's Guide</i> at <a href="#">PowerEdge manuals</a> .
<b>Device Settings</b>	Enables you to configure device settings.
<b>Service Tag Settings</b>	Enables you to configure service tag settings.

## 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 BIOS** 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 the operating system begins to load before you press F2, wait for the system to finish booting, and then restart the 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
<b>System Information</b>	Specifies information about the system such as the system model name, BIOS version, and Service Tag.
<b>Memory Settings</b>	Specifies information and options related to the installed memory.
<b>Processor Settings</b>	Specifies information and options related to the processor such as speed and cache size.
<b>SATA Settings</b>	Specifies options to enable or disable the integrated SATA controller and ports.
<b>NVMe Settings</b>	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 <b>Embedded SATA</b> field on the <b>SATA Settings</b> menu to <b>RAID</b> mode. You might also need to change the <b>Boot Mode</b> setting to <b>UEFI</b> . Otherwise, you should set this field to <b>Non-RAID</b> mode.

Option	Description
<b>Boot Settings</b>	Specifies options to specify the Boot mode (BIOS or UEFI). Enables you to modify UEFI and BIOS boot settings.
<b>Network Settings</b>	Specifies options to manage the UEFI network settings and boot protocols. Legacy network settings are managed from the <b>Device Settings</b> menu.
<b>Integrated Devices</b>	Specifies options to manage integrated device controllers and ports, specifies related features and options.
<b>Serial Communication</b>	Specifies options to manage the serial ports, its related features and options.
<b>System Profile Settings</b>	Specifies options to change the processor power management settings, memory frequency.
<b>System Security</b>	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.
<b>Redundant OS Control</b>	Sets the redundant OS info for redundant OS control.
<b>Miscellaneous Settings</b>	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 BIOS version.


### Viewing System Information

To view the **System Information** 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 Information**.

### System Information details

#### About this task

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

Option	Description
<b>System Model Name</b>	Specifies the system model name.
<b>System BIOS Version</b>	Specifies the BIOS version installed on the system.

Option	Description
<b>System Management Engine Version</b>	Specifies the current version of the Management Engine firmware.
<b>System Service Tag</b>	Specifies the system Service Tag.
<b>System Manufacturer</b>	Specifies the name of the system manufacturer.
<b>System Manufacturer Contact Information</b>	Specifies the contact information of the system manufacturer.
<b>System CPLD Version</b>	Specifies the current version of the system complex programmable logic device (CPLD) firmware.
<b>UEFI Compliance Version</b>	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.

### Viewing Memory Settings

To view the **Memory 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 the operating system begins to load before you press F2, wait for the system to finish booting, and then restart the 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
<b>System Memory Size</b>	Specifies the memory size in the system.
<b>System Memory Type</b>	Specifies the type of memory installed in the system.
<b>System Memory Speed</b>	Specifies the system memory speed.

Option	Description
<b>System Memory Voltage</b>	Specifies the system memory voltage.
<b>Video Memory</b>	Specifies the amount of video memory.
<b>System Memory Testing</b>	Specifies whether the system memory tests are run during system boot. Options are <b>Enabled</b> and <b>Disabled</b> . This option is set to <b>Disabled</b> by default.
<b>Dram Refresh Delay</b>	By enabling the <b>CPU memory controller</b> to delay running the <b>REFRESH</b> commands, you can improve the performance for some workloads. By minimizing the delay time, it is ensured that the memory controller runs the <b>REFRESH</b> command at regular intervals. For Intel-based servers, this setting only affects systems configured with DIMMs which use 8 Gb density DRAMS.
<b>Memory Operating Mode</b>	Specifies the memory operating mode. The options available are <b>Optimizer Mode</b> , <b>Single Rank Spare Mode</b> , <b>Multi Rank Spare Mode</b> , and <b>Mirror Mode</b> . This option is set to <b>Optimizer Mode</b> by default.  <b>NOTE:</b> The <b>Memory Operating Mode</b> option can have different default and available options based on the memory configuration of your system.
<b>Current State of Memory Operating Mode</b>	Specifies the current state of the memory operating mode.
<b>ADDDC Setting</b>	Enables or disables <b>ADDDC Setting</b> feature. When Adaptive Double DRAM Device Correction (ADDDC) is enabled, failing DRAM's are dynamically mapped out. When set to <b>Enabled</b> it can have some impact to system performance under certain workloads. This feature is applicable for x4 DIMMs only. This option is set to <b>Enabled</b> by default.
<b>Native tRFC Timing for 16Gb Density DIMMs</b>	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 <b>Enabled</b> by default.
<b>Opportunistic Self-Refresh</b>	Enables or disables opportunistic self-refresh feature. This option is set to <b>Disabled</b> by default.
<b>DIMM Self Healing (Post Package Repair) on Uncorrectable Memory Error</b>	Enables or disables Post Package Repair (PPR) on Uncorrectable Memory Error. This option is set to <b>Enabled</b> by default.
<b>Correctable Error Logging</b>	Enables or disables logging of correctable memory threshold error. This option is set to <b>Disabled</b> by default.

## 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, and logical processor idling.


### Viewing Processor Settings

To view the **Processor 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 **Processor Settings**.

## Processor Settings details

### About this task

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

Option	Description
<b>Logical Processor</b>	Enables or disables the logical processors and displays the number of logical processors. If this option is set to <b>Enabled</b> , the BIOS displays all the logical processors. If this option is set to <b>Disabled</b> , the BIOS displays only one logical processor per core. This option is set to <b>Enabled</b> by default.
<b>CPU Interconnect Speed</b>	<p>Enables you to govern the frequency of the communication links among the CPUs in the system.</p> <p> <b>NOTE:</b> The standard and basic bin processors support lower link frequencies.</p> <p>The options available are <b>Maximum data rate, 10.4 GT/s</b>, and <b>9.6 GT/s</b>. This option is set to <b>Maximum data rate</b> by default.</p> <p>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.</p> <p>For the best performance, you should select <b>Maximum data rate</b>. Any reduction in the communication link frequency affects the performance of non-local memory accesses and cache coherency traffic. In addition, it can slow access to non-local I/O devices from a particular CPU.</p> <p>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.</p>
<b>Virtualization Technology</b>	Enables or disables the virtualization technology for the processor. This option is set to <b>Enabled</b> by default.
<b>Adjacent Cache Line Prefetch</b>	Optimizes the system for applications that need high utilization of sequential memory access. This option is set to <b>Enabled</b> by default. You can disable this option for applications that need high utilization of random memory access.
<b>Hardware Prefetcher</b>	Enables or disables the hardware prefetcher. This option is set to <b>Enabled</b> by default.
<b>DCU Streamer Prefetcher</b>	Enables or disables the Data Cache Unit (DCU) streamer prefetcher. This option is set to <b>Enabled</b> by default.
<b>DCU IP Prefetcher</b>	Enables or disables the Data Cache Unit (DCU) IP prefetcher. This option is set to <b>Enabled</b> by default.
<b>Sub NUMA Cluster</b>	Enables or disables the Sub NUMA Cluster. This option is set to <b>Disabled</b> by default.
<b>UPI Prefetch</b>	Enables you to get the memory read started early on the DDR bus. The Ultra Path Interconnect (UPI) Rx path will spawn the speculative memory read to the Integrated Memory Controller (iMC) directly. This option is set to <b>Enabled</b> by default.
<b>LLC Prefetch</b>	Enables or disables the LLC Prefetch on all threads. This option is set to <b>Disabled</b> by default.
<b>Dead Line LLC Alloc</b>	When enabled, it opportunistically fills dead lines in LLC. When disabled, it never fills dead lines in LLC. This option is set to <b>Enabled</b> by default.
<b>Directory AtoS</b>	AtoS optimization reduces remote read latencies for repeat read accesses without intervening writes. This option is set to <b>Disabled</b> by default.
<b>Logical Processor Idling</b>	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 <b>Disabled</b> by default.
<b>Configurable TDP</b>	Enables you to configure the TDP level. The available options are <b>Nominal</b> , <b>Level 1</b> , and <b>Level 2</b> .

Option	Description																
	<ul style="list-style-type: none"> <li>• <b>Nominal</b> - This is the default TDP.</li> <li>• <b>Level 1</b> - Additional factory defined TDP alternative.</li> <li>• <b>Level 2</b> - Additional factory defined TDP alternative.</li> </ul> <p> <b>NOTE:</b> This option is only available on certain stock keeping units (SKUs) of the processors.</p>																
<b>x2APIC Mode</b>	Enables or disables the x2APIC mode. This option is set to <b>Enabled</b> by default.																
<b>Number of Cores per Processor</b>	Controls the number of enabled cores in each processor. This option is set to <b>All</b> by default.																
<b>Processor Core Speed</b>	Specifies the maximum core frequency of the processor.																
<b>Processor Bus Speed</b>	Displays the bus speed of the processor.																
<b>Processor n</b>	The following settings are displayed for each processor that is installed in the system:																
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><b>Family-Model-Stepping</b></td> <td>Specifies the family, model, and stepping of the processor as defined by Intel.</td> </tr> <tr> <td><b>Brand</b></td> <td>Specifies the brand name.</td> </tr> <tr> <td><b>Level 2 Cache</b></td> <td>Specifies the total L2 cache.</td> </tr> <tr> <td><b>Level 3 Cache</b></td> <td>Specifies the total L3 cache.</td> </tr> <tr> <td><b>Number of Cores</b></td> <td>Specifies the number of cores per processor.</td> </tr> <tr> <td><b>Maximum Memory Capacity</b></td> <td>Specifies the maximum memory capacity per processor.</td> </tr> <tr> <td><b>Microcode</b></td> <td>Specifies the microcode.</td> </tr> </tbody> </table>	Option	Description	<b>Family-Model-Stepping</b>	Specifies the family, model, and stepping of the processor as defined by Intel.	<b>Brand</b>	Specifies the brand name.	<b>Level 2 Cache</b>	Specifies the total L2 cache.	<b>Level 3 Cache</b>	Specifies the total L3 cache.	<b>Number of Cores</b>	Specifies the number of cores per processor.	<b>Maximum Memory Capacity</b>	Specifies the maximum memory capacity per processor.	<b>Microcode</b>	Specifies the microcode.
Option	Description																
<b>Family-Model-Stepping</b>	Specifies the family, model, and stepping of the processor as defined by Intel.																
<b>Brand</b>	Specifies the brand name.																
<b>Level 2 Cache</b>	Specifies the total L2 cache.																
<b>Level 3 Cache</b>	Specifies the total L3 cache.																
<b>Number of Cores</b>	Specifies the number of cores per processor.																
<b>Maximum Memory Capacity</b>	Specifies the maximum memory capacity per processor.																
<b>Microcode</b>	Specifies the microcode.																

## SATA Settings

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


### Viewing SATA Settings

To view the **SATA 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 **SATA Settings**.

## SATA Settings details

### About this task


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

Option	Description
<b>Embedded SATA</b>	Enables the embedded SATA option to be set to <b>Off</b> , <b>AHCI</b> , or <b>RAID</b> modes. This option is set to <b>AHCI Mode</b> by default.
<b>Security Freeze Lock</b>	Sends <b>Security Freeze Lock</b> command to the embedded SATA drives during POST. This option is applicable only for AHCI Mode. This option is set to <b>Enabled</b> by default.
<b>Write Cache</b>	Enables or disables the command for the embedded SATA drives during POST. This option is set to <b>Disabled</b> by default.
<b>Port n</b>	Sets the drive type of the selected device.  For <b>AHCI Mode</b> or <b>RAID Mode</b> , BIOS support is always enabled.
<b>Option</b>	<b>Description</b>
<b>Model</b>	Specifies the drive model of the selected device.
<b>Drive Type</b>	Specifies the type of drive attached to the SATA port.
<b>Capacity</b>	Specifies the total capacity of the drive. This field is undefined for removable media devices such as optical drives.

## 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.

- **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, 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.

- **BIOS**: The **BIOS Boot Mode** is the legacy boot mode. It is maintained for backward compatibility.


## Viewing Boot Settings

To view the **Boot 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 **Boot Settings**.

## Boot Settings details

### About this task

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

Option	Description
<b>Boot Mode</b>	<p>Enables you to set the boot mode of the system.</p> <p> <b>CAUTION:</b> Switching the boot mode may prevent the system from booting if the operating system is not installed in the same boot mode.</p> <p>If the operating system supports <b>UEFI</b>, you can set this option to <b>UEFI</b>. Setting this field to <b>BIOS</b> allows compatibility with non-UEFI operating systems. This option is set to <b>UEFI</b> by default.</p> <p> <b>NOTE:</b> Setting this field to <b>UEFI</b> disables the <b>BIOS Boot Settings</b> menu.</p>
<b>Boot Sequence Retry</b>	<p>Enables or disables the <b>Boot Sequence Retry</b> feature. If this option is set to <b>Enabled</b> and the system fails to boot, the system re-attempts the boot sequence after 30 seconds. This option is set to <b>Enabled</b> by default.</p>
<b>Hard-Disk Failover</b>	<p>Specifies the drive that is booted in the event of a drive failure. The devices are selected in the <b>Hard-Disk Drive Sequence</b> on the <b>Boot Option Setting</b> menu. When this option is set to <b>Disabled</b>, only the first drive in the list is attempted to boot. When this option is set to <b>Enabled</b>, all drives are attempted to boot in the order selected in the <b>Hard-Disk Drive Sequence</b>. This option is not enabled for <b>UEFI Boot Mode</b>. This option is set to <b>Disabled</b> by default.</p>
<b>Generic USB boot</b>	<p>Enables or disables generic USB boot. This option is set to <b>Disabled</b> by default.</p>
<b>Hard-disk Drive Placeholder</b>	<p>Enables or disables Hard-disk Drive Placeholder.</p>
<b>Boot Option Settings</b>	<p>Configures the boot sequence and the boot devices.</p>
<b>BIOS Boot Settings</b>	<p>Enables or disables BIOS boot options.</p> <p> <b>NOTE:</b> This option is enabled only if the boot mode is BIOS.</p>
<b>UEFI Boot Settings</b>	<p>Enables or disables UEFI Boot options.</p> <p>The Boot options include <b>IPv4 PXE</b> and <b>IPv6 PXE</b>. This option is set to <b>IPv4</b> by default.</p> <p> <b>NOTE:</b> This option is enabled only if the boot mode is UEFI.</p>
<b>UEFI Boot Sequence</b>	<p>Enables you to change the boot device order.</p>


## Choosing system boot mode

System Setup enables you to specify one of the following boot modes for installing your operating system:


- BIOS boot mode is the standard BIOS-level boot interface.
- UEFI boot mode (the default), is an enhanced 64-bit boot interface.


If you have configured your system to boot to UEFI mode, it replaces the system BIOS.

1. From the **System Setup Main Menu**, click **Boot Settings**, and select **Boot Mode**.
2. Select the UEFI boot mode you want the system to boot into.

 **CAUTION:** Switching the boot mode may prevent the system from booting if the operating system is not installed in the same boot mode.

3. After the system boots in the specified boot mode, proceed to install your operating system from that mode.

 **NOTE:** Operating systems must be UEFI-compatible to be installed from the UEFI boot mode. DOS and 32-bit operating systems do not support UEFI and can only be installed from the BIOS boot mode.

 **NOTE:** For the latest information about supported operating systems, go to [OS support](#)

## Changing boot order

### About this task


You may have to change the boot order if you want to boot from a USB key or an optical drive. The following instructions may vary if you have selected **BIOS** for **Boot Mode**.

### Steps

1. On the **System Setup Main Menu** screen, click **System BIOS > Boot Settings > UEFI/BIOS Boot Settings > UEFI/BIOS Boot Sequence**.
2. Use the arrow keys to select a boot device, and use the plus (+) and minus (-) sign keys to move the device down or up in the order.
3. Click **Exit**, and then click **Yes** to save the settings on exit.

## 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:** 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. 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 **Network Settings**.

## Network Settings screen details

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

### About this task

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

**Option**                      **Description**

**UEFI HTTP Settings**

**Options**                      **Description**

**HTTP Device (n = 1 to 4)**      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.

**Table 1. HTTP Device n Settings screen details**

Option	Description
<b>Interface</b>	Specifies the NIC interface used for this device.
<b>Protocol</b>	Enables you to select protocol <b>IPv4</b> or <b>IPv6</b> . This is set to <b>IPv4</b> by default.
<b>VLAN</b>	Enables or Disable <b>VLAN</b> . This is set to <b>Disabled</b> by default.
<b>VLAN ID</b>	This is set to <b>1</b> .
<b>VLAN Priority</b>	This is set to <b>0</b> .
URI (will obtain from DHCP server if not specified)	

**UEFI iSCSI Settings**

Enables you to control the configuration of the iSCSI device.

**Table 2. UEFI iSCSI Settings screen details**

Option	Description
<b>iSCSI Initiator Name</b>	Specifies the name of the iSCSI initiator in IQN format.
<b>iSCSI Device1</b>	Enables or disables the iSCSI device. When enabled, a UEFI boot option is created for the iSCSI device automatically. This is set to <b>Disabled</b> by default.
<b>iSCSI Device1 Settings</b>	Enables you to control the configuration of the iSCSI device.
<b>Connection 1</b>	Enables you to control the configuration of the iSCSI connection.
<b>Connection 2</b>	Enables you to control the configuration of the iSCSI connection.
<b>Connection 1 Settings</b>	Enables you to control the configuration of the iSCSI connection.
<b>Connection 2 Settings</b>	Enables you to control the configuration of the iSCSI connection.
<b>Connection order</b>	Enables you to control the order of the iSCSI connection.

# 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 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 **Integrated Devices**.

## Integrated Devices details

### About this task

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

Option	Description
<b>User Accessible USB Ports</b>	Configures the user accessible USB ports. Selecting <b>Only Back Ports On</b> disables the front USB ports; selecting <b>All Ports Off</b> disables all front and back USB ports;  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.
<b>Internal USB Port</b>	Enables or disables the internal USB port. This option is set to <b>On</b> or <b>Off</b> . This option is set to <b>On</b> by default.
<b>iDRAC Direct USB Port</b>	The iDRAC Direct USB port is managed by iDRAC exclusively with no host visibility. This option is set to <b>ON</b> or <b>OFF</b> . When set to <b>OFF</b> , iDRAC does not detect any USB devices installed in this managed port. This option is set to <b>On</b> by default.
<b>Integrated RAID Controller</b>	Enables or disables the integrated RAID controller. This option is set to <b>Enabled</b> by default.
<b>Embedded NIC1 and NIC2</b>	<b>NOTE:</b> The Embedded NIC1 and NIC2 options are only available on systems that do not have <b>Integrated Network Card 1</b> .  Enables or disables the Embedded NIC1 and NIC2 options. If set to <b>Disabled</b> , the NIC may still be available for shared network access by the embedded management controller. The embedded NIC1 and NIC2 options are only available on systems that do not have Network Daughter Cards (NDCs). The Embedded NIC1 and NIC2 option is mutually exclusive with the Integrated Network Card 1 option. Configure the Embedded NIC1 and NIC2 option by using the NIC management utilities of the system.
<b>I/OAT DMA Engine</b>	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. This option is set to <b>Disabled</b> by default.
<b>I/O SnoopHoldOff Response</b>	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.

Option	Description
<b>Embedded Video Controller</b>	<p>Enables or disables the use of Embedded Video Controller as the primary display. When set to <b>Enabled</b>, the Embedded Video Controller will be the primary display even if add-in graphic cards are installed. When set to <b>Disabled</b>, 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 <b>Enabled</b> by default.</p> <p><b>NOTE:</b> 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.</p>
<b>Current State of Embedded Video Controller</b>	<p>Displays the current state of the embedded video controller. The <b>Current State of Embedded Video Controller</b> 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 <b>Embedded Video Controller</b> setting is set to <b>Disabled</b>.</p>
<b>SR-IOV Global Enable</b>	<p>Enables or disables the BIOS configuration of Single Root I/O Virtualization (SR-IOV) devices. This option is set to <b>Disabled</b> by default.</p>
<b>Internal MicroSD Card Port</b>	<p>Enables or disables the internal MicroSD card port of the Internal Dual SD Module (IDSMD). This option is set to <b>On</b> by default.</p>
<b>Internal MicroSD Card Redundancy</b>	<p>Configures the redundancy mode of the Internal Dual SD Module (IDSMD). When set to <b>Mirror</b> Mode, data is written on both MicroSD cards. After failure of either card and replacement of the failed card, the data of the active card is copied to the offline card during the system boot.</p> <p>When Internal SD Card Redundancy is set to <b>Disabled</b>, only the primary MicroSD card is visible to the OS. This option is set to <b>Disabled</b> by default.</p>
<b>Internal microSD Primary Card</b>	<p>When <b>Redundancy</b> is set to <b>Disabled</b>, either one of the MicroSD card can be selected to present itself as mass storage device by setting it to be primary card. By default primary MicroSD card is selected to be SD Card 1. If MicroSD Card 1 is not present, then the controller will select MicroSD Card 2 to be the primary MicroSD card.</p>
<b>OS Watchdog Timer</b>	<p>If your system stops responding, this watchdog timer aids in the recovery of your operating system. When this option is set to <b>Enabled</b>, the operating system initializes the timer. When this option is set to <b>Disabled</b> (the default), the timer does not have any effect on the system.</p>
<b>Empty Slot Unhide</b>	<p>If <b>Enabled</b>, the root ports of all the empty slots are accessible to the BIOS and OS. This option is set to <b>Disabled</b> by default.</p>
<b>Memory Mapped I/O above 4 GB</b>	<p>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 <b>Enabled</b> by default.</p>
<b>Memory Mapped I/O Base</b>	<p>When set to <b>12 TB</b>, the system will map MMIO base to 12 TB. Enable this option for an OS that requires 44 bit PCIe addressing. When set to <b>512 GB</b>, the system will map MMIO base to 512 GB, and reduce the maximum support for memory to less than 512 GB. Enable this option only for the 4 GPU DGMA issue. This option is set to <b>56 TB</b> by default.</p>
<b>Slot Disablement</b>	<p>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.</p>

**Table 3. Slot Disablement**

Option	Description
<b>Slot 1</b>	<p>Enables or disables or only the boot driver is disabled for the PCIe slot 1. This option is set to <b>Enabled</b> by default.</p>
<b>Slot 2</b>	<p>Enables or disables or only the boot driver is disabled for the PCIe slot 2. This option is set to <b>Enabled</b> by default.</p>

Option	Description
--------	-------------

**Table 3. Slot Disablement (continued)**

Option	Description
<b>Slot 3</b>	Enables or disables or only the boot driver is disabled for the PCIe slot 3. This option is set to <b>Enabled</b> by default.
<b>Slot 4</b>	Enables or disables or only the boot driver is disabled for the PCIe slot 4. This option is set to <b>Enabled</b> by default.
<b>Slot 5</b>	Enables or disables or only the boot driver is disabled for the PCIe slot 5. This option is set to <b>Enabled</b> by default.
<b>Slot 6</b>	Enables or disables or only the boot driver is disabled for the PCIe slot 6. This option is set to <b>Enabled</b> by default.

**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 4. Slot Bifurcation**

Option	Description
<b>Auto Discovery Bifurcation Settings</b>	Platform Default Bifurcation , Auto Bifurcation, and Manual bifurcation
<b>Slot 1 Bifurcation</b>	x4 or x8 Bifurcation
<b>Slot 2 Bifurcation</b>	x4 or x8 Bifurcation
<b>Slot 3 Bifurcation</b>	x4 or x8 Bifurcation
<b>Slot 4 Bifurcation</b>	x16 or x4 or x8 or x4x4x8 or x8x4x4 Bifurcation
<b>Slot 5 Bifurcation</b>	x4 Bifurcation
<b>Slot 6 Bifurcation</b>	x4 Bifurcation

## Serial Communication

You can 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 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 **Serial Communication**.

## Serial Communication details

### About this task

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

Option	Description
<b>Serial Communication</b>	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 <b>Auto</b> by default.
<b>Serial Port Address</b>	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 <b>Serial Device1=COM2 or Serial Device 2=COM1</b> by default. <b>NOTE:</b> 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. <b>NOTE:</b> 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 the serial MUX setting to the default setting of Serial Device 1.
<b>External Serial Connector</b>	Enables you to associate the External Serial Connector to <b>Serial Device 1</b> , <b>Serial Device 2</b> , or the <b>Remote Access Device</b> by using this option. This option is set to <b>Serial Device 1</b> by default. <b>NOTE:</b> 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. <b>NOTE:</b> 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.
<b>Failsafe Baud Rate</b>	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 <b>115200</b> by default.
<b>Remote Terminal Type</b>	Sets the remote console terminal type. This option is set to <b>ANSI/VT100/VT220</b> by default.
<b>Redirection After Boot</b>	Enables or disables the BIOS console redirection when the operating system is loaded. This option is set to <b>Enabled</b> 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
<b>System Profile</b>	Sets the system profile. If you set the System Profile option to a mode other than <b>Custom</b> , the BIOS automatically sets the rest of the options. You can only change the rest of the options if the mode is set to <b>Custom</b> . This option is set to <b>Performance Per Watt Optimized (DAPC)</b> by default. DAPC is Dell Active Power Controller. Other options include <b>Performance Per Watt (OS)</b> , <b>Performance</b> , and <b>Workstation Performance</b> . <b>NOTE:</b> All the parameters on the system profile setting screen are available only when the <b>System Profile</b> option is set to <b>Custom</b> .
<b>CPU Power Management</b>	Sets the CPU power management. This option is set to <b>System DBPM (DAPC)</b> by default. DBPM is Demand-Based Power Management. Other options include <b>OS DBPM</b> , and <b>Maximum Performance</b> .
<b>Memory Frequency</b>	Sets the speed of the system memory. You can select <b>Maximum Performance</b> , <b>Maximum Reliability</b> , or a specific speed. This option is set to <b>Maximum Performance</b> by default.
<b>Turbo Boost</b>	Enables or disables the processor to operate in the turbo boost mode. This option is set to <b>Enabled</b> by default.
<b>C1E</b>	Enables or disables the processor to switch to a minimum performance state when it is idle. This option is set to <b>Enabled</b> by default.
<b>C States</b>	Enables or disables the processor to operate in all available power states. This option is set to <b>Enabled</b> by default.
<b>Write Data CRC</b>	Enables or disables the Write Data CRC. This option is set to <b>Disabled</b> by default.
<b>Memory Patrol Scrub</b>	Sets the memory patrol scrub frequency. This option is set to <b>Standard</b> by default.
<b>Memory Refresh Rate</b>	Sets the memory refresh rate to either 1x or 2x. This option is set to <b>1x</b> by default.
<b>Uncore Frequency</b>	Enables you to select the <b>Processor Uncore Frequency</b> option.

Option	Description
	<b>Dynamic mode</b> 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 <b>Energy Efficiency Policy</b> option.
<b>Energy Efficient Policy</b>	Enables you to select the <b>Energy Efficient Policy</b> 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 <b>Balanced Performance</b> by default.
<b>Number of Turbo Boost Enabled Cores for Processor 1</b>	 <b>NOTE:</b> If there are two processors installed in the system, you will see an entry for <b>Number of Turbo Boost Enabled Cores for Processor 2</b> . Controls the number of turbo boost enabled cores for Processor 1. The maximum number of cores is enabled by default.
<b>Monitor/Mwait</b>	Enables the Monitor/Mwait instructions in the processor. This option is set to <b>Enabled</b> for all system profiles, except <b>Custom</b> by default.  <b>NOTE:</b> This option can be disabled only if the <b>C States</b> option in the <b>Custom</b> mode is set to <b>disabled</b> .  <b>NOTE:</b> When <b>C States</b> is set to <b>Enabled</b> in the <b>Custom</b> mode, changing the Monitor/Mwait setting does not impact the system power or performance.
<b>CPU Interconnect Bus Link Power Management</b>	Enables or disables the CPU Interconnect Bus Link Power Management. This option is set to <b>Enabled</b> by default.
<b>PCI ASPM L1 Link Power Management</b>	Enables or disables the PCI ASPM L1 Link Power Management. This option is set to <b>Enabled</b> by default.

## 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. 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 Security**.

## System Security Settings details

### About this task

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

Option	Description
<b>CPU AES-NI</b>	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 <b>Enabled</b> by default.
<b>System Password</b>	Sets the system password. This option is set to <b>Enabled</b> by default and is read-only if the password jumper is not installed in the system.
<b>Setup Password</b>	Sets the setup password. This option is read-only if the password jumper is not installed in the system.
<b>Password Status</b>	Locks the system password. This option is set to <b>Unlocked</b> by default.
<b>TPM Security</b>	<p> <b>NOTE:</b> The TPM menu is available only when the TPM module is installed.</p> <p>Enables you to control the reporting mode of the TPM. The <b>TPM Security</b> option is set to <b>Off</b> by default. You can only modify the TPM Status, and TPM Activation fields if the <b>TPM Status</b> field is set to either <b>On with Pre-boot Measurements</b> or <b>On without Pre-boot Measurements</b>.</p> <p>When TPM 1.2 is installed, the <b>TPM Security</b> option is set to <b>Off</b>, <b>On with Pre-boot Measurements</b>, or <b>On without Pre-boot Measurements</b>.</p> <p><b>TPM 1.2 security information</b></p> <p><b>TPM Information</b> Changes the operational state of the TPM. This option is set to <b>Type: 2.0-NTC</b> by default.</p> <p><b>TPM Firmware</b> Indicates the firmware version of the TPM.</p> <p><b>TPM Status</b> Specifies the TPM status.</p> <p><b>TPM Command</b> Controls the Trusted Platform Module (TPM). When set to <b>None</b>, no command is sent to the TPM. When set to <b>Activate</b>, the TPM is enabled and activated. When set to <b>Deactivate</b>, the TPM is disabled and deactivated. When set to <b>Clear</b>, all the contents of the TPM are cleared. This option is set to <b>None</b> by default.</p> <p>When TPM 2.0 is installed, the <b>TPM Security</b> option is set to <b>On</b> or <b>Off</b>. This option is set to <b>Off</b> by default.</p> <p><b>TPM 2.0 security information</b></p> <p><b>TPM Information</b> Changes the operational state of the TPM. This option is set to <b>Type: 2.0-NTC</b> by default.</p> <p><b>TPM Firmware</b> Indicates the firmware version of the TPM.</p> <p><b>TPM Hierarchy</b> Enable, disable, or clear the storage and endorsement hierarchies. When set to <b>Enabled</b>, the storage and endorsement hierarchies can be used.</p> <p>When set to <b>Disabled</b>, the storage and endorsement hierarchies cannot be used.</p> <p>When set to <b>Clear</b>, the storage and endorsement hierarchies are cleared of any values, and then reset to <b>Enabled</b>.</p> <p><b>TPM Advanced Settings</b> This setting is enabled only when TPM security is set to <b>ON</b>.</p>

**Table 5. TPM Advanced Settings Details**

Option	Description
<b>TPM PPI Bypass Provision</b>	When set to <b>Enabled</b> 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 <b>Disabled</b> by default.

**Option**                      **Description**

**Table 5. TPM Advanced Settings Details (continued)**

<b>Option</b>	<b>Description</b>
<b>TPM PPI Bypass Clear</b>	When set to <b>Enabled</b> 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 <b>Disabled</b> by default.
<b>TPM2 Algorithm Selection</b>	Allows the user to change the cryptographic algorithms used in the Trusted Platform Module (TPM). The available options are dependent on the TPM firmware. To enable <b>TPM2 Algorithm Selection</b> , Intel(R) TXT technology must be disabled.

**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.

**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**.

Option	Description								
	<table border="1"> <thead> <tr> <th>Options</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><b>User Mode</b></td> <td> <p>In <b>User Mode</b>, PK must be installed, and BIOS performs signature verification on programmatic attempts to update policy objects.</p> <p>The BIOS allows unauthenticated programmatic transitions between modes.</p> </td> </tr> <tr> <td><b>Audit Mode</b></td> <td> <p>In <b>Audit mode</b>, PK is not present. The BIOS does not authenticate programmatic updates to the policy objects, and transitions between modes.</p> <p><b>Audit Mode</b> is useful for programmatically determining a working set of policy objects.</p> <p>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.</p> </td> </tr> <tr> <td><b>Deployed Mode</b></td> <td> <p><b>Deployed Mode</b> is the most secure mode. In <b>Deployed Mode</b>, PK must be installed and the BIOS performs signature verification on programmatic attempts to update policy objects.</p> <p><b>Deployed Mode</b> restricts the programmatic mode transitions.</p> </td> </tr> </tbody> </table>	Options	Description	<b>User Mode</b>	<p>In <b>User Mode</b>, PK must be installed, and BIOS performs signature verification on programmatic attempts to update policy objects.</p> <p>The BIOS allows unauthenticated programmatic transitions between modes.</p>	<b>Audit Mode</b>	<p>In <b>Audit mode</b>, PK is not present. The BIOS does not authenticate programmatic updates to the policy objects, and transitions between modes.</p> <p><b>Audit Mode</b> is useful for programmatically determining a working set of policy objects.</p> <p>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.</p>	<b>Deployed Mode</b>	<p><b>Deployed Mode</b> is the most secure mode. In <b>Deployed Mode</b>, PK must be installed and the BIOS performs signature verification on programmatic attempts to update policy objects.</p> <p><b>Deployed Mode</b> restricts the programmatic mode transitions.</p>
Options	Description								
<b>User Mode</b>	<p>In <b>User Mode</b>, PK must be installed, and BIOS performs signature verification on programmatic attempts to update policy objects.</p> <p>The BIOS allows unauthenticated programmatic transitions between modes.</p>								
<b>Audit Mode</b>	<p>In <b>Audit mode</b>, PK is not present. The BIOS does not authenticate programmatic updates to the policy objects, and transitions between modes.</p> <p><b>Audit Mode</b> is useful for programmatically determining a working set of policy objects.</p> <p>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.</p>								
<b>Deployed Mode</b>	<p><b>Deployed Mode</b> is the most secure mode. In <b>Deployed Mode</b>, PK must be installed and the BIOS performs signature verification on programmatic attempts to update policy objects.</p> <p><b>Deployed Mode</b> restricts the programmatic mode transitions.</p>								
<b>Secure Boot Policy Summary</b>	Specifies the list of certificates and hashes that secure boot uses to authenticate images.								
<b>Secure Boot Custom Policy Settings</b>	Configures the Secure Boot Custom Policy. To enable this option, set the Secure Boot Policy to <b>Custom</b> option.								

## Creating a system and setup password

### Prerequisites

Ensure that the password jumper is enabled. The password jumper enables or disables the system password and setup password features. For more information, see the System board jumper settings section.

 **NOTE:** If the password jumper setting is disabled, the existing system password and setup password are deleted and you need not provide the system password to boot the system.

### Steps

1. To enter System Setup, press F2 immediately after turning on or rebooting your system.
2. On the **System Setup Main Menu** screen, click **System BIOS > System Security**.
3. On the **System Security** screen, verify that **Password Status** is set to **Unlocked**.
4. In the **System Password** field, type your system password, and press Enter or Tab.
 


Use the following guidelines to assign the system password:

  - A password can have up to 32 characters.
  - The password can contain the numbers 0 through 9.

A message prompts you to reenter the system password.
5. Reenter the system password, and click **OK**.
6. In the **Setup Password** field, type your setup password and press Enter or Tab.
 

A message prompts you to reenter the setup password.
7. Reenter the setup password, and click **OK**.
8. Press Esc to return to the System BIOS screen. Press Esc again.
 

A message prompts you to save the changes.

 **NOTE:** Password protection does not take effect until the system reboots.

## Using your system password to secure the system

### About this task

If you have assigned a setup password, the system accepts your setup password as an alternate system password.

### Steps

1. Power on or reboot your system.
2. Type the system password and press Enter.

### Next steps

When **Password Status** is set to **Locked**, type the system password and press Enter when prompted at reboot.

- NOTE:** If an incorrect system password is typed, the system displays a message and prompts you to reenter your password. You have three attempts to type the correct password. After the third unsuccessful attempt, the system displays an error message that the system has stopped functioning and must be turned off. Even after you turn off and restart the system, the error message is displayed until the correct password is entered.

## Deleting or changing system and setup password

### Prerequisites

- NOTE:** You cannot delete or change an existing system or setup password if the **Password Status** is set to **Locked**.

### Steps

1. To enter System Setup, press F2 immediately after turning on or restarting your system.
2. On the **System Setup Main Menu** screen, click **System BIOS > System Security**.
3. On the **System Security** screen, ensure that **Password Status** is set to **Unlocked**.
4. In the **System Password** field, change or delete the existing system password, and then press Enter or Tab.
5. In the **Setup Password** field, alter or delete the existing setup password, and then press Enter or Tab.

**NOTE:** If you change the system password or setup password, a message prompts you to reenter the new password. If you delete the system password or setup password, a message prompts you to confirm the deletion.
6. Press Esc to return to the **System BIOS** screen. Press Esc again, and a message prompts you to save the changes.
7. Select **Setup Password**, change, or delete the existing setup password and press Enter or Tab.

**NOTE:** If you change the system password or setup password, a message prompts you to reenter the new password. If you delete the system password or setup password, a message prompts you to confirm the deletion.

## Operating with setup password enabled

If **Setup Password** is set to **Enabled**, type the correct setup password before modifying the system setup options.

If you do not type the correct password in three attempts, the system displays the following message:

```
Password Invalid. Number of unsuccessful password attempts: <x> Maximum number of password attempts exceeded. System halted.
```

```
Number of unsuccessful password attempts: <3> Maximum number of password attempts exceeded. System Halted!
```

Even after you turn off and restart the system, the error message is displayed until the correct password is typed. The following options are exceptions:

- If **System Password** is not set to **Enabled** and is not locked through the **Password Status** option, you can assign a system password. For more information, see the System Security Settings screen section.
- You cannot disable or change an existing system password.

**NOTE:** You can use the password status option with the setup password option to protect the system password from unauthorized changes.

## Redundant OS Control

In the **Redundant OS Control** screen you can set the redundant OS information. This enables you to set up a physical recovery disk on the system.

## Viewing Redundant OS Control

To view the **Redundant OS Control** 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 **Redundant OS Control**.

## Redundant OS Control screen details

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

### About this task

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

## 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.


### Viewing Miscellaneous Settings

To view the **Miscellaneous 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 **Miscellaneous Settings**.

### Miscellaneous Settings details


#### About this task

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

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

## Device Settings

**Device Settings** enables you to configure the below device parameters:


- Controller Configuration Utility
- Embedded NIC Port1-X Configuration
- NICs in slotX, Port1-X Configuration
- BOSS Card configuration

## Dell Lifecycle Controller

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 lifecycle of the system. 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 [PowerEdge manuals](#).

## Boot Manager

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

### Viewing Boot Manager

#### About this task

To enter Boot Manager:

#### Steps

1. Power on, or restart your system.
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
<b>Continue Normal Boot</b>	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.

<b>Menu item</b>	<b>Description</b>
<b>One-shot Boot Menu</b>	Enables you to access boot menu, where you can select a one-time boot device to boot from.
<b>Launch System Setup</b>	Enables you to access System Setup.
<b>Launch Lifecycle Controller</b>	Exits the Boot Manager and invokes the Dell Lifecycle Controller program.
<b>System Utilities</b>	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 select a boot device 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 allows managing of network devices.