

Dell EMC PowerEdge T340

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.

Chapter 1: Pre-operating system management applications.....	4
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.....	22
Device Settings.....	22
Dell Lifecycle Controller.....	22
Embedded system management.....	22
Boot Manager.....	23
Viewing Boot Manager.....	23
Boot Manager main menu.....	23
One-shot UEFI boot menu.....	23
System Utilities.....	23
PXE boot.....	23

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
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 <i>Integrated Dell Remote Access Controller User's Guide</i> at www.dell.com/poweredgemanuals .
Device Settings	Enables you to configure device 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 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
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.
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.

Option	Description
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 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
System Model Name	Specifies the system model name.
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.

Option	Description
System Manufacturer	Specifies the name of the system manufacturer.
System Manufacturer Contact Information	Specifies the contact information of the system manufacturer.
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.


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

Option	Description
Memory Operating Mode	Specifies the memory operating 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.
Current State of Memory Operating Mode	Specifies the current state of the memory operating mode.

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
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.
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.
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.
x2APIC Mode	Enables or disables the x2APIC mode. This option is set to Disabled by default.

Option	Description														
Number of Cores per Processor	Controls the number of enabled cores in each processor. This option is set to All by default.														
Processor Core Speed	Specifies the maximum core frequency of the processor.														
Processor 1	The following settings are displayed for each processor installed in the system: <table> <tr> <th>Option</th><th>Description</th></tr> <tr> <td>Family-Model-Stepping</td><td>Specifies the family, model, and stepping of the processor as defined by Intel.</td></tr> <tr> <td>Brand</td><td>Specifies the brand name.</td></tr> <tr> <td>Level 2 Cache</td><td>Specifies the total L2 cache.</td></tr> <tr> <td>Level 3 Cache</td><td>Specifies the total L3 cache.</td></tr> <tr> <td>Number of Cores</td><td>Specifies the number of cores per processor.</td></tr> <tr> <td>Microcode</td><td>Specifies the microcode.</td></tr> </table>	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.	Microcode	Specifies the microcode.
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.														
Microcode	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
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 applicable only for AHCI Mode. 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.

Option	Description
For AHCI Mode or RAID Mode , BIOS support is always enabled.	
Option	Description
Model	Specifies the drive model of the selected device.
Drive Type	Specifies the type of drive attached to the SATA port.
Capacity	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.
- **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
Boot Mode	<p>Enables you to set the boot mode of the system.</p> <p> CAUTION: 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 UEFI, you can set this option to UEFI. Setting this field to BIOS allows compatibility with non-UEFI operating systems. This option is set to UEFI by default.</p> <p> NOTE: Setting this field to UEFI disables the BIOS Boot Settings menu.</p>

Option	Description
Boot Sequence Retry	Enables or disables the Boot Sequence Retry feature. If this option is set to Enabled and the system fails to boot, the system re-attempts the boot sequence after 30 seconds. 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 generic USB boot. This option is set to Disabled by default.
Hard-disk Drive Placeholder	Enables or disables Hard-disk Drive Placeholder.
UEFI Boot Settings	<p>Enables or disables UEFI Boot options.</p> <p>The Boot options include IPv4 PXE and IPv6 PXE. This option is set to IPv4 by default.</p> <p> NOTE: This option is enabled only if the boot mode is UEFI.</p>
UEFI Boot Sequence	Enables you to change the boot device order.
Boot Options Enable/Disable	Enables you to select the enabled or disabled 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:** 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
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.
HTTP Device n (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.
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 enabled, a UEFI boot option is created for the iSCSI device automatically. This is set to Enabled by default.
iSCSI Device1 Settings	Enables you to control the configuration of the iSCSI device.

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
User Accessible USB Ports	<p>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;</p> <p>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.</p> <p> NOTE: Selecting Only Back Ports On and All Ports Off disables the USB management port and also restricts access to the iDRAC features.</p>
Internal USB Port	<p>Enables or disables the internal USB port. This option is set to On or Off. This option is set to On by default.</p>
iDRAC Direct USB Port	<p>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.</p>
Embedded NIC1 and NIC2	<p> NOTE: The Embedded NIC1 and NIC2 options are only available on systems that do not have Integrated Network Card 1.</p> <p>Enables or disables the Embedded NIC1 and NIC2 options. If set to Disabled, 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.</p>
I/OAT DMA Engine	<p>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.</p>
Embedded Video Controller	<p>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.</p> <p> 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.</p>
Current State of Embedded Video Controller	<p>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 Enabled.</p>
OS Watchdog Timer	<p>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.</p>
Memory Mapped I/O above 4 GB	<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 Enabled by default.</p>
Slot Disablement	<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>

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

Table 2. Slot Disablement

Option	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.
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.

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
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.
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 Device1=COM2 or Serial Device 2=COM1 by default.

Option	Description
	<p>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.</p> <p>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 the serial MUX setting to the default setting of Serial Device 1.</p>
External Serial Connector	<p>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.</p> <p>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.</p> <p>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.</p>
Failsafe Baud Rate	<p>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.</p>
Remote Terminal Type	<p>Sets the remote console terminal type. This option is set to ANSI VT100/VT220 by default.</p>
Redirection After Boot	<p>Enables or disables the BIOS console redirection when the operating system is loaded. This option is set to Enabled by default.</p>

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	<p>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 (OS) by default.</p> <p> NOTE: All the parameters on the system profile setting screen are available only when the System Profile option is set to Custom.</p>
CPU Power Management	Sets the CPU power management. This option is set to OS DBPM by default.
Memory Frequency	Sets the speed of the system memory. You can select Maximum Performance , Maximum Reliability , 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.
Memory Refresh Rate	Sets the memory refresh rate to either 1x or 2x. This option is set to 1x by default.
Uncore Frequency	<p>Enables you to select the Processor Uncore Frequency option.</p> <p>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.</p>
Number of Turbo Boost Enabled Cores for Processor 1	<p> NOTE: If there are two processors installed in the system, you will see an entry for Number of Turbo Boost Enabled Cores for Processor 2.</p> <p>Controls the number of turbo boost enabled cores for Processor 1. The maximum number of cores is enabled by default.</p>
Monitor/Mwait	<p>Enables the Monitor/Mwait instructions in the processor. This option is set to Enabled for all system profiles, except Custom by default.</p> <p> NOTE: This option can be disabled only if the C States option in the Custom mode is set to disabled.</p> <p> 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.</p>
PCI ASPM L1 Link Power Management	Enables or disables the PCI ASPM L1 Link Power Management. This option is set to Enabled 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
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 Security	 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 fields if the TPM Status field is set to either On with Pre-boot Measurements or On without Pre-boot Measurements .
TPM Information	Changes the operational state of the TPM. This option is set to No Change by default.
TPM Status	Specifies the TPM status.
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.  CAUTION: Clearing the TPM results in the loss of all keys in the TPM. The loss of TPM keys may affect booting to the operating system. This field is read-only when TPM Security is set to Off . The action requires an additional reboot before it can take effect.
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.
Intel(R) SGX	Enables or disables the Intel Software Guard Extension (SGX) option. This option is set to Software by default.  NOTE: The SGX menu is available, only when the SGX supported processor is installed.
SGX Launch Control Policy	Allows controlling the Launch Control Policy (LCP) of Software Guard Extensions (SGX) technology. This option is set to Unlocked by default.
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 240 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	<p>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.</p> <p> 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.</p>								
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	<p>Configures how the BIOS uses the Secure Boot Policy Objects (PK, KEK, db, dbx).</p> <p>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.</p> <table> <tr> <th>Options</th><th>Description</th></tr> <tr> <td>User Mode</td><td> <p>In User Mode, 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>Audit Mode</td><td> <p>In Audit mode, PK is not present. The BIOS does not authenticate programmatic updates to the policy objects, and transitions between modes.</p> <p>Audit Mode 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>Deployed Mode</td><td> <p>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.</p> <p>Deployed Mode restricts the programmatic mode transitions.</p> </td></tr> </table>	Options	Description	User Mode	<p>In User Mode, 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>	Audit Mode	<p>In Audit mode, PK is not present. The BIOS does not authenticate programmatic updates to the policy objects, and transitions between modes.</p> <p>Audit Mode 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>	Deployed Mode	<p>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.</p> <p>Deployed Mode restricts the programmatic mode transitions.</p>
Options	Description								
User Mode	<p>In User Mode, 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>								
Audit Mode	<p>In Audit mode, PK is not present. The BIOS does not authenticate programmatic updates to the policy objects, and transitions between modes.</p> <p>Audit Mode 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>								
Deployed Mode	<p>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.</p> <p>Deployed Mode restricts the programmatic mode transitions.</p>								
Secure Boot Policy Summary	Specifies the list of certificates and hashes that secure boot uses to authenticate images.								
Secure Boot Custom Policy Settings	Configures the Secure Boot Custom Policy. To enable this option, set the Secure Boot Policy to Custom 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.
- Only the following special characters are allowed: space, ("), (+), (.), (-), (.), (/), (:), ([), (\), (]), (`).

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:

```
Invalid Password! Number of unsuccessful password attempts: <x> System Halted! Must  
power down.
```

```
Password Invalid. Number of unsuccessful password attempts: <x> 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
Redundant OS Location	<p>Enables you to select a backup disk from the following devices:</p> <ul style="list-style-type: none">• None• IDSDM• SATA Ports in AHCI mode• BOSS PCIe Cards (Internal M.2 Drives)• Internal USB <p>NOTE: RAID configurations and NVMe cards not are included as BIOS does not have the ability to distinguish between individual drives in those configurations.</p>
Redundant OS State	<p>NOTE: This option is disabled if Redundant OS Location is set to None.</p> <p>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.</p> <p>NOTE: BIOS will disable the device in hardware, so it cannot be accessed by the OS.</p>
Redundant OS Boot	<p>NOTE: This option is disabled if Redundant OS Location is set to None or if Redundant OS State is set to Hidden.</p> <p>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.</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
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 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 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/poweredgemanuals.

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 www.dell.com/poweredgemanuals.

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
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 Boot Menu	Enables you to access boot menu, where you can select a one-time boot device to boot from.
Launch System Setup	Enables you to access System Setup.
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 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.