Topic 3B: Configure BIOS/UEFI:

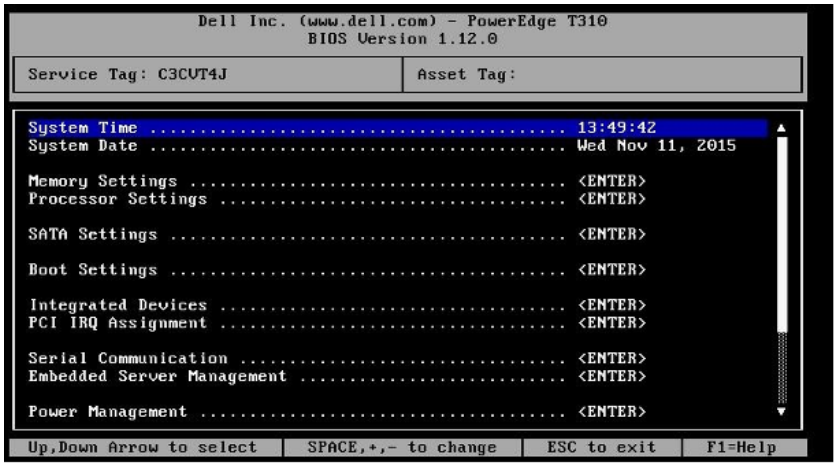
Firmware refers to the software that are directly integrated into the hardware. For example, BIOS, UEFI, etc. The motherboard firmware is the software that checks and verifies everything that is required to run an OS system like all the hardware are functional or not. Firmware is distinct from other software because it is very closely tied to the specific hardware device type and model.

For many years, the system firmware for a PC was called **Basic Input Output System (BIOS).** It only supports 32-bit operation and limited functionality. Newer motherboards use **Unifies Extensible Firmware Interface (UEFI).** It supports 64-bit CPU operation at boot. It includes full GUI and mouse operation at boot, network functionality at boot, and better boot security. A computer with **UEFI** can also support legacy **BIOS** mode.

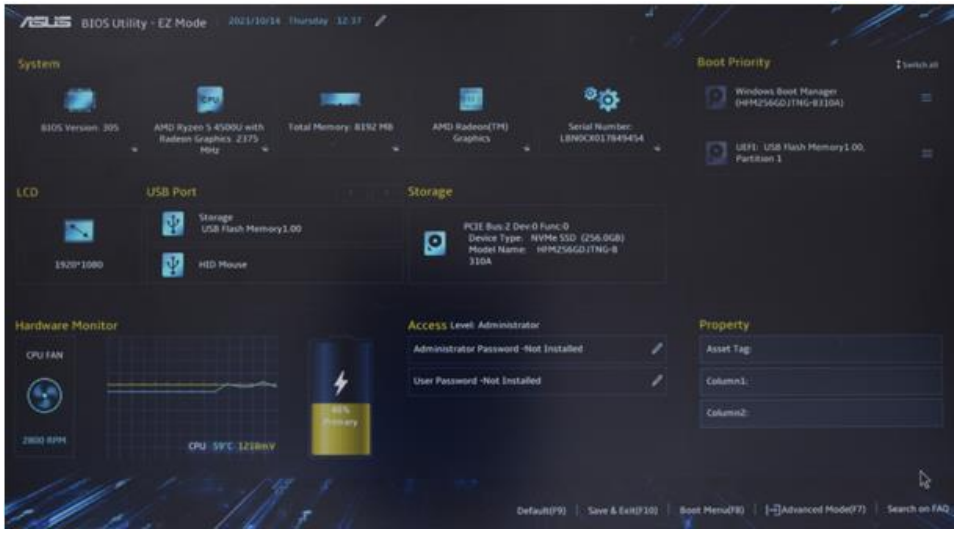
We basically use firmware settings to change or access **System Settings.** BIOS or UEFI mode are accessed via a keyword press during boot process. Usually **Esc, Del, F1, F2, F10, or F12.**

Nowadays, computers boot so quickly so that we are not able to see the instruction popping to enter to the UEFI or BIOS. So, in this case, if you are not being able to see those, then you can press **Shift** and click the **Restart button** from the windows login screen to access the **UEFI** options.

In BIOS, you can only use keyboard not mouse. UEFI offers you graphical interface and mouse support.



A BIOS setup program.



Boot and Device Options:

When you enter into the BIOS or UEFI mode, one of the important features you can see in there is the **Boot Options Sequence** or **Boot Order Priority**. This defines the order in which the system firmware searches devices for boot manager.

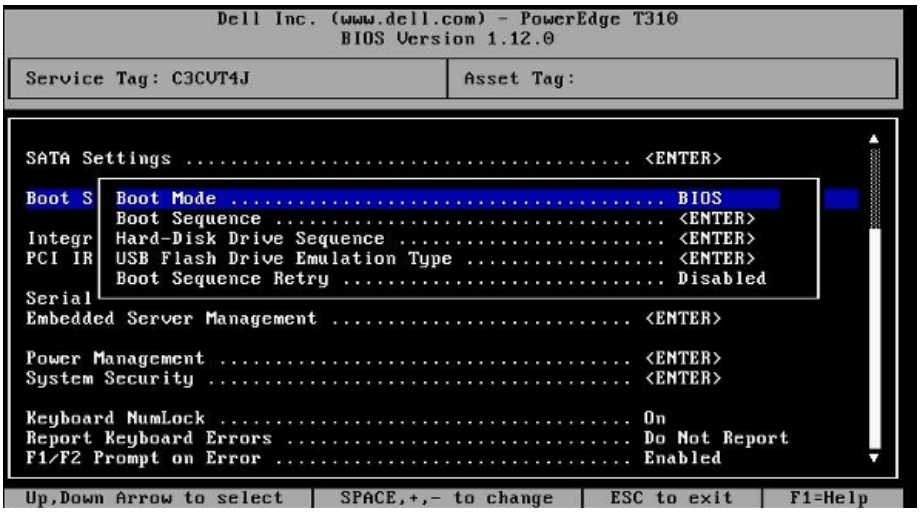
Options available are:

- **Fixed Disks (HDDs or SSDs):** Fixed disk means the disk that cannot be detachable from the system right. Normally, we can Hard Disk directly in the first place. But if we have SSDs attached with SATA in our computer, then it is displayed in under the heading **SATA/AHCI** devices. And if we have SSDs installed as PCIe Add-In Card (AIC) or on the M.2 Interface, it will be shown under the heading **NVMe**.

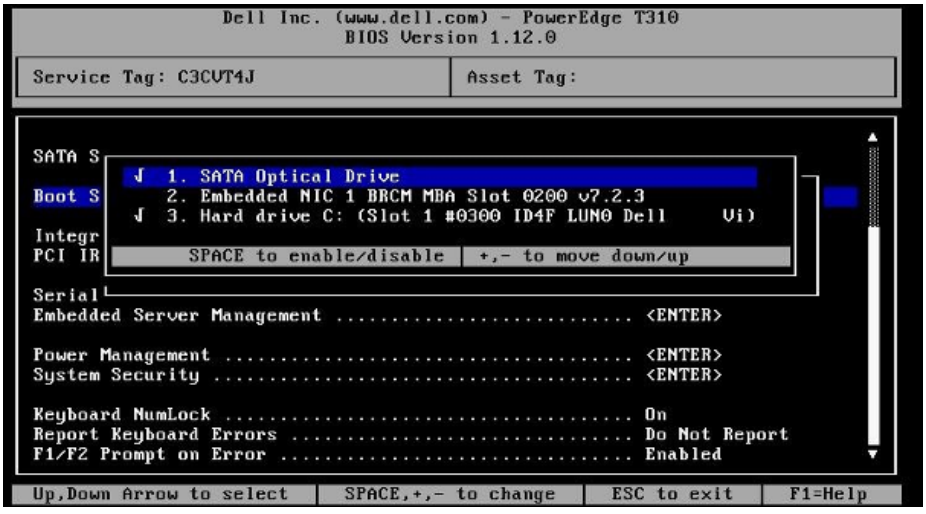
- **Optical Drive (CD/DVD/Blu-ray):** If you need to performing a repair install from optical media, you need to select this device in the highest priority.

- **USB:** Most modern systems can boot from USB drive that has been formatted as a boot device. This option is often used for OS installs and repair utility boot disks that are too large to fit in an optical media.

- **Network/PXE:** Uses the network adapter to obtain the boot settings from a specially configured server.

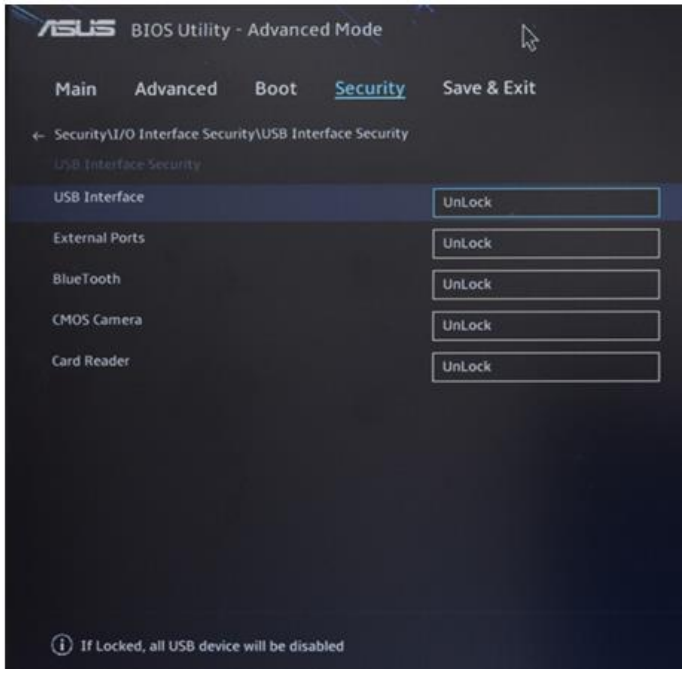


Boot parameters



Boot Order Configuration

USB Permissions:



You can also disable certain ports on your computers from BIOS/UEFI. Let's say you run a small office where employees use computers. To prevent anyone from using a USB stick to steal company files or accidentally introduce a virus, you can use the BIOS/UEFI settings to disable certain USB ports. For example:

- You might lock all USB ports except one that is used for a keyboard or mouse.
- If an employee tries to plug in a USB flash drive, the computer will not recognize it because the port is disabled.

This feature is particularly useful in environments where security is important, like offices, schools, or public computers.

Fans Considerations:

Cooling fans in a computer can usually be adjusted through the system's settings, often found in menus labeled **Cooling**, **Power**, or **Advanced**. These settings let you choose how the fans operate based on your preferences or needs, with options like:

1. **Balanced**: Fans adjust automatically to maintain moderate noise and temperature.
2. **Cool**: Fans run at higher speeds to keep the system extra cool.
3. **Quiet**: Fans run slower to reduce noise, even if the system gets a bit warmer.
4. **Fanless**: Fans turn off entirely, only used in systems designed for silent operation.
5. **Custom**: You set specific speeds and behaviors for the fans.

Key Terms:

- **Minimum Temperature**: The point at which the fans start running to cool the system.
- **Duty Cycle**: Controls how fast the fan runs by adjusting power pulses. A higher percentage means the fan runs faster.

The system's setup program (such as BIOS/UEFI) will also display the **current temperature** measured by sensors near the fans. Additionally, third-party software can provide access to these settings directly from your operating system, making it easier to monitor and adjust fan performance.

Boot Password:

A **boot password** is a security feature that requires the user to enter a password before the operating system starts. It ensures that unauthorized users cannot access the system, even if they have physical access to the computer. Different systems may offer various authentication methods, but two common types of passwords are:

1. **Supervisor/Administrator/Setup Password**:
   This protects access to the **system setup program** (like BIOS/UEFI settings). Only users with this password can change critical system settings.
2. **User/System Password**:
   This locks access to the entire computer. The system will not boot or perform any action until this password is entered. It's a strong security measure for computers that handle sensitive data or perform critical tasks.

Example of Use:
A **User/System Password** is useful for a workstation running monitoring software in a secure environment, like a server room. Since the PC doesn't require interactive logins for regular use, setting a boot password ensures only authorized personnel can start or access the system.
Limitation:
If multiple users need access, they must know the password, which weakens the security. This method is best suited for systems with limited user access rather than shared devices.

These passwords is different from what you enter into your Personal Computer to get access to Operating System. **Boot Password** is required before the operating system even loads. It's set in the system's BIOS/UEFI and protects the entire system from being accessed.

Example:
If your PC has a **boot password** enabled, a thief trying to use your computer would be blocked from even loading the OS. However, if you only rely on an OS login password, the thief could bypass it by booting the PC with a different OS or accessing your hard drive externally.

For personal use, an OS login password is sufficient for most users, but enabling a boot password adds an extra layer of security, especially for sensitive data.

Secure Boot:

Secure Boot is a feature in UEFI (Unified Extensible Firmware Interface) designed to protect your computer from malware that could hijack the boot process. It works by using **cryptographic keys** to verify that only trusted software can load when the computer starts.
Here's how it works:

1. **Cryptographic Keys**: The system firmware (UEFI) is preloaded with keys from trusted OS vendors, like Microsoft (for Windows) or Linux distributions (like Fedora or Ubuntu).
2. **Verification**: When your computer starts, UEFI checks the operating system's boot loader against these keys. If the boot loader has been tampered with (e.g., by malware) or isn't authorized, the system blocks it.
3. **Protection**: This ensures that only an OS digitally signed by the vendor can run, preventing unauthorized or malicious software from booting the computer.

Real-Life Example:
Let's say your computer is infected with malware that tries to replace the OS boot loader to gain control over your system. With **Secure Boot** enabled, the malware-modified boot loader would fail the cryptographic key check, and the system would prevent it from running, keeping your computer secure.

Trusted Platform Modules (TPM):

Encryption products make data secure by scrambling it in such a way that it can only subsequently be read if the user has the correct **decryption key**. Hashes can be used to compare two copies of data to verify that they are the same. Unlike encryption, the original data cannot be recovered from the hash code.

A **Trusted Platform Module (TPM)** is a small chip on your computer's motherboard that provides secure storage for sensitive information, like **digital certificates**, **cryptographic keys**, and **hashed passwords**. It acts as a root of trust, ensuring that your system's data and boot process are secure. Every TPM has a unique, unchangeable key (called the **endorsement key**) that identifies and secures the device. During startup, the TPM compares **hashes** (unique digital fingerprints) of critical system components, like the firmware, boot loader, and OS kernel, to check if they've been tampered with. If any changes are detected, the TPM alerts the system. The TPM provides a secure area for storing encryption keys. For example, programs like **Windows BitLocker** use the TPM to securely store the keys needed to unlock encrypted drives. The TPM can be **enabled, disabled, or reset** through the system setup program (BIOS/UEFI). Some settings can also be managed directly from the operating system.

Real-Life Example:
Imagine your laptop is stolen. If you're using **BitLocker drive encryption** with TPM, the encryption keys are stored securely in the TPM chip. Without those keys, even if someone removes your hard drive and connects it to another computer, they won't be able to access your data.
In simple terms, TPM is like a vault in your computer that ensures only trusted software runs and protects your sensitive data from unauthorized access.

But let's say sometime if you removed the TPM enabled Hard Disk from your laptop and connect it to another laptop, then how can you access that Hard Disk?

- ⇨ For this, when you connect the Hard Disk to another laptop, it asks you to enter the **recovery key** which you get when you set up BitLocker in your hard disk in original laptop. It is saved typically in your Microsoft Account. So after entering the correct **key**, you can access it. And if you lost the **recovery key** then the data is effectively lost. No one can access it.

Hardware Security Modules:

A **Hardware Security Module (HSM)** is a secure device, like a **USB thumb drive**, that stores cryptographic keys (the "codes" used for encryption and decryption). It's an alternative to TPM for storing keys when:

1. The computer doesn't have a TPM.
2. You need a recovery option if the TPM is damaged.
3. You need to move an encrypted disk to another computer.

Key Features of HSM:

1. **Secure Storage**:
   The keys are stored on the HSM, ensuring they are safe from unauthorized access.
2. **Authentication**:
   To access the keys on the HSM, the user must authenticate using a:
   - **Password**
   - **PIN (Personal Identification Number)**
   - **Fingerprint** or other biometric methods
3. **Portability**:
   An HSM can be plugged into another computer, allowing you to securely use encrypted data on different systems.

Real-Life Example:
Let's say you've encrypted your hard drive but your computer doesn't support TPM. You can use an **HSM (like a secure USB drive)** to store the encryption keys. If you want to use the encrypted drive on another computer, plug in the HSM and authenticate yourself with the required PIN or password. The HSM will provide the necessary keys to unlock the drive.
This way, your encryption remains portable and secure, even across different computers.

Some Questions and Answers:

1. **Name three keys commonly used to run a PC's BIOS/UEFI system setup program.**
    - Common keys include **F2**, **Delete (Del)**, and **Esc**. Some systems may also use **F1**, **F10**, or **F12** depending on the manufacturer.

---

2. **What widely supported boot method is missing from the following list? HDD, Optical, USB.**
    - The missing boot method is **Network Boot (PXE)**, which allows a system to boot from an image on a network server.

---

3. **When you are configuring firmware-enforced security, what is the difference between a supervisor password and a user password?**
    - A **supervisor password** protects access to the system setup program (BIOS/UEFI settings) and allows changes to configuration settings.
    - A **user password** locks the entire system and prevents the computer from booting without entering the password.

---

4. **True or false? A TPM provides secure removable storage so that encryption keys can be used with different computers.**
    - **False**. A TPM securely stores encryption keys within the computer's hardware, but it is not removable and cannot be used to transfer keys between different computers.