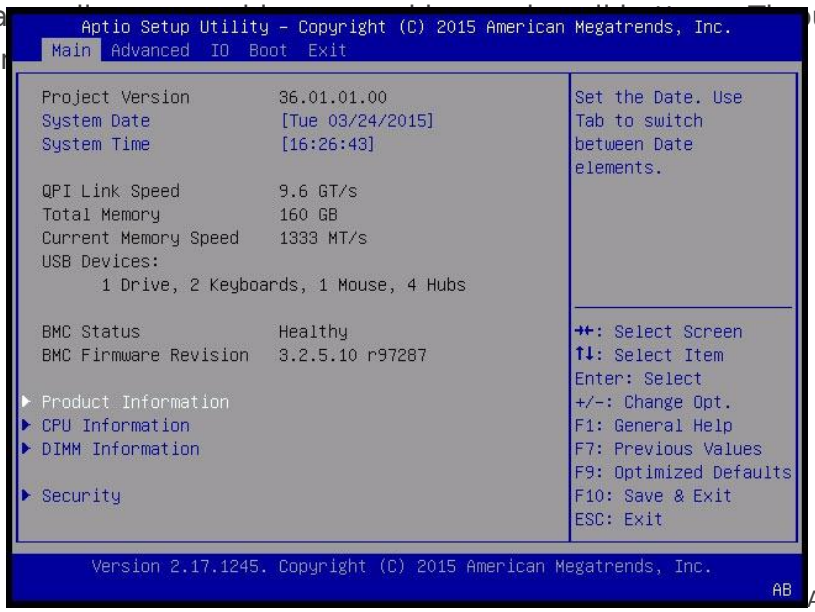
EFI & BIOS

Computer hardware has evolved over the years and the industry stardard have continued to shift. This has led to computer hardware that leverage different mechanisms to achieve the same end. For low-level firmware, there are two technologies widely available for configuring hardware.

BIOS

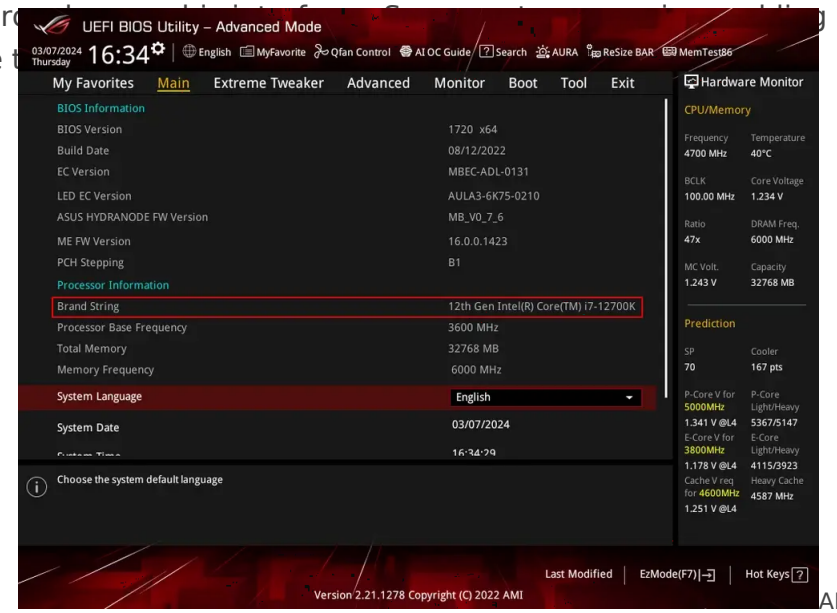
Older PC systems use a BIOS – or Basic Input/Output System – to handle core functions before the computer has loaded an operating system. The BIOS is used to configure fundamental computer settings that affects how hardware interacts with the operating system. This architecture stores your settings on a [illegible] ough a user navigable interface, core co[illegible]



AMI BIOS

EFI

Modern computer systems use UEFI – or the Unified Extensible Firmware Interface – to manage these settings thr[illegible] an advanced or administer mode t[illegible]



AMI UEFI

Configuring Your Hardware

There are numerous manufacturers who use different BIOS and UEFI software for their computer systems. There is no definitive standard for BIOS or EFI systems, resultibg in many different descriptive names for the same features. While we try to cover the most common names, you may need to do some personal research. It's entirely possible that feature is not available on your computer system.

> If a feature is missing, don't panic! You may still be able to follow these guides without running into any issues.

Some OEM systems, such as business-grade workstation PCs, have simplified firmware with minimal configurable options. This computer can work as a server but may require configuration through the operating system to properly manage power and efficiency settings.

These are some common keyboard commands to enter the BIOS or UEFI menu by manufacturer:

ASRock	F2 or Del
Asus	F2 or Del
Acer	F2 or Del

Dell	F2 or F12
Gigabyte	F2 or Del
HP	F10
Intel	F2
Lenovo	F1
MSI	Del
Samsung	F2
Toshiba	F2

Disable Unused Hardware & Features

You can increase the overall security of a home server by disabling extraneous hardware as a proactive measure to decrease your cyber attack surface area.

Some common hardware components to disable are:

Serial Port

This legacy protocol is used for old modems and printers.

> *Recommended:* Disabled

Parallel Port

This legacy protocol is used for old printers, scanners and storage devices.

> *Recommended:* Disabled

Audio Ports

Our server ideally will be running "headless" (without a display) and should not be used as a media player.

This can include 3.5mm, optical, HDMI and other audio ports.

> *Recommended:* Disabled

Bluetooth

Bluetooth can be left on for connecting smart devices to Home Assistant, but the protocol can be insecure.

> *Recommended:* Disabled

Thunderbolt

This technology can be enabled for daisy-chaining multiple displays and storage devices, but it has known vulnerabilities and should be disabled if not in use.

> *Recommended:* Disabled

Wireless Internet

We will use a hardwired connection for our server and the wireless card should be disabled if not in use.

> *Recommended:* Disabled

Trusted Platform Module

This technology is used predominantly for Windows 11 and ensures operating system files are not tampered with. Linux can use the module for encrypting hard drives, but it should be disabled otherwise.

>

> *Recommended:* Disabled

Power-Saving Features

We are running an always-on server which means our power efficiency settings are an important consideration. Turning off certain hardware when the computer is idle can increase their life expectancy, while turning off other hardware components can decrease stability.

Cool'n'Quiet or SpeedStep

Cool'n'Quiet (AMD) and SpeedStep (Intel) slow down the processor when idle to decrease overall power usage**.**

> *Recommended:* Enabled

EIST

Enhanced Intel SpeedStep is an advanced mechanism for dynamically scaling the processor's speed and power consumption.

> *Recommended:* Enabled

C-States

This feature allows the CPU to temporarily disable processor sections when they are not being used by the operating system.

> *Recommended:* Enabled or Auto

C1E

This is an advanced power-saving state that temporarily decreases the processor speed when idle while allowing for rapid return to an active state.

> *Recommended:* Enabled

ErP Mode and EuP Mode

This is a comprehensive power feature related to an EU directive that aims to decrease overall device power usage.

While useful for a standard computer, the setting can fundamentally alter system performance by disabling or underclocking hardware.

> *Recommended:* Disabled

Boot Settings

We can ensure that our server correctly boots into the operating system and restarts automatically in the event of a power failure.

Boot Priority

If your server has multiple storage disks, you need to ensure that the disk with the operating system installed has first boot priority.

For security, you can disable booting from additional hard drives.

Keyboard and Mouse Halt

Our server will be remotely accessible and we do not always need input devices – such as a mouse and keyboard – connected to it.

Without this setting disabled, the server will fail to boot without them connected.

>

> *Recommended:* Disabled

Secure Boot

This feature is used to verify operating system files during boot to ensure that malicious software cannot start.

By default, the hardware is configured for Microsoft Windows and can be configured for use with Debian if desired. Otherwise, it should be disabled.

> *Recommended:* Disabled

Fast Boot

This feature disables several important power-on hardware tests and has been known to interfere with some operating system features.

This feature is not supported by Debian out of the box and needs to be configured.

> *Recommended:* Disabled

Restart After Failure

In the event that your server loses power unexpectedly, it can be configured to turn back on when power is restored.

> *Recommended:* Enabled

Wake-on-LAN

Your server can be powered on through your Ethernet connection over the Local Area Network when it receives a "magic packet".

> *Recommended:* Enabled

Power Schedule

Our server should remain on at all times and we do not want our server operating on a power cycling schedule.

> *Recommended:* Disabled

Storage Interface

There are some settings related to the way hard drives and solid state disks communicate with the operating system.

SATA Mode

Advanced Host Controller Interface, or AHCI, enables the use of SSD drives through a SATA connection.

Additionally, it improves performance by strictly enforcing hardware communication standards that can be leveraged by the operating system.

> *Recommended:* AHCI

RAID

Redundant Array of Independent Disks, or RAID, enables your system to duplicate hard drive writes in real-time.

This creates a fully functional backup in the event of a hard drive failure. This architecture needs to be setup before installing an operating system and cannot be installed after.

> *Recommended:* Disabled

Maintenance keyboard_arrow_right

Revision #19
Created 11 February 2025 07:19:54 by metaphorraccoon
Updated 11 May 2025 04:32:39 by metaphorraccoon