ITFreeTraining

UEFI

For the free video please see
http://itfreetraining.com/ap/1b50

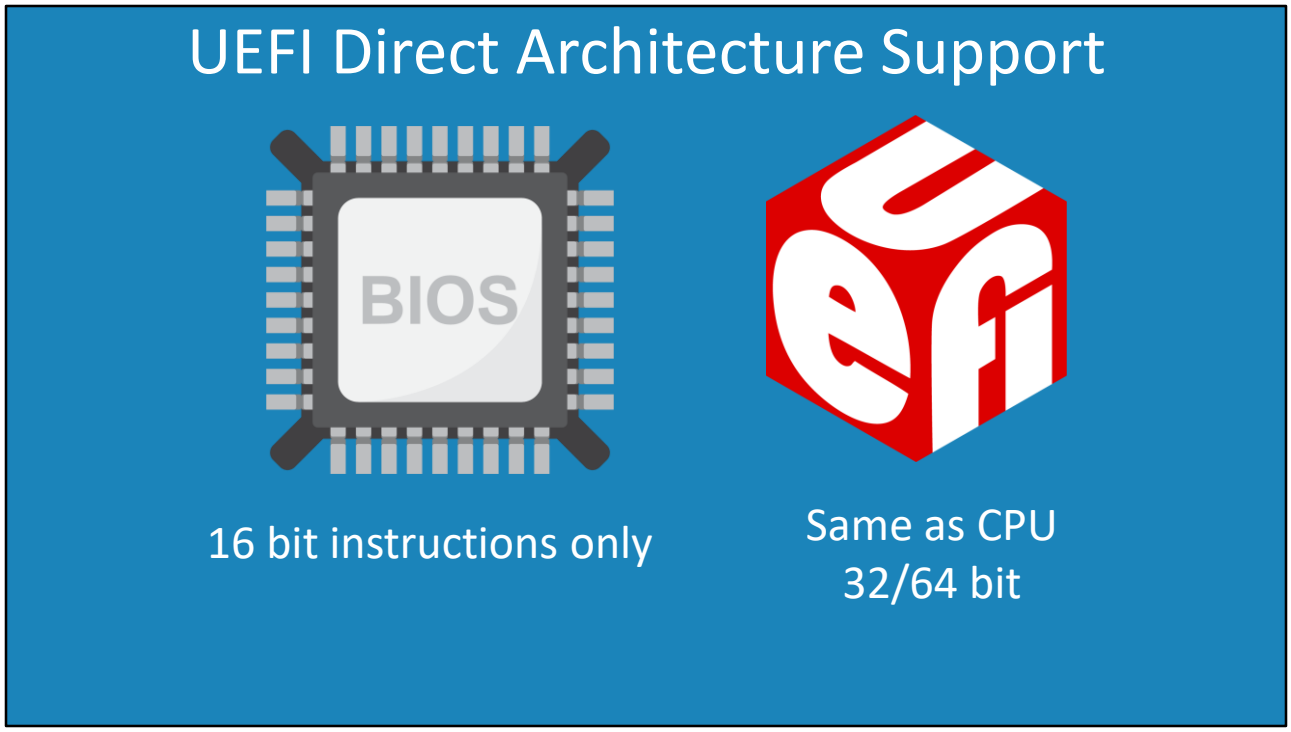
In this video from ITFreeTraining I will look at Unified Extensible Firmware Interface or UEFI. Traditionally BIOS performed the role of the initial boot process for a computer; UEFI is replacing BIOS and addresses a number of limitations of the BIOS.

Access the rest of the course http://ITFreeTraining.com/ap
Download the PDF handout http://ITFreeTraining.com/handouts/ap/1b50.pdf

What is UEFI?

- Developed in 2005
- Replaces legacy BIOS
- Addresses limitations of BIOS
- Adds additional features
- Often referred to as firmware or BIOS

0:0:17 UEFI was first developed in 2005. It was designed to replace BIOS. BIOS or the basic input output system has been around since the 70's. There have been a lot of improvements in computing during this time and BIOS has been able to address some of these but not others. UEFI addresses the limitations of BIOS and also adds additional features that were not available in BIOS. The UEFI is a single chip located on the motherboard. You can see in this example, the left motherboard has one UEFI chip and the right motherboard has two. In the case of the right motherboard there are two chips in case one was to fail. The chip can vary in size and shape but generally nowadays is quite small. The UEFI chip contains the software that is used when the computer first starts up. You may also hear it referred to as firmware or even BIOS. Often hardware devices will have software embedded in them which is used to operate the device. For example, a video camera. Think of it as software for hardware. This software for hardware is often referred to as firmware. As the UEFI is software to make the hardware of the computer operate this is why it is often called firmware. You may also hear UEFI referred to as BIOS. Whilst technically this is incorrect, BIOS has been around for so long that people, especially IT technicians, are just more accustomed to using this name. It may also be called UEFI BIOS. Next, I will take a look at some of the differences between UEFI and BIOS.



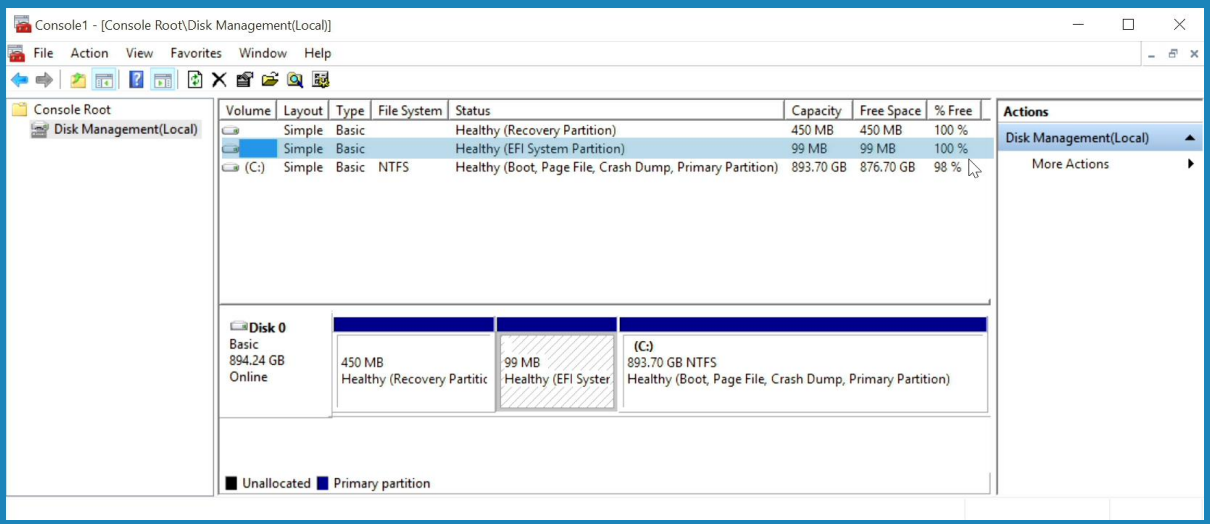
0:1:53 The first big difference is that BIOS supports only 16bit instructions, regardless of what the CPU supports. UEFI supports the same instructions as the CPU. CPUs on the market today are generally 32bit or 64bit. Since, the first Intel CPUs ran in 16bit mode, it made sense for the BIOS to operate on 16bit instructions. However, as CPU's improved, for backward compatibility reasons, BIOS kept running in 16bit. For a long time, since the BIOS was used for initial start up and setup this was not a problem. With modern 32bit and 64bit CPUs, the CPU will start in pseudo 16bit mode. This mode allows the BIOS to operate with 16bit instructions. This has a lot of limitations, for example the BIOS will not be able to access all the memory in the computer. The idea behind having a pseudo 16bit mode is to allow BIOS to start the computer up and then switch to either 32 or 64bit mode. Thus, 16bit is designed essentially just to allow the operating system to boot and is very limited in what it can do. UEFI on the other hand, can run code that is the same as the CPU. This allows UEFI to access all the RAM on the computer. UEFI can also run its own software and device drivers without an operating system being installed.

Larger Storage Support

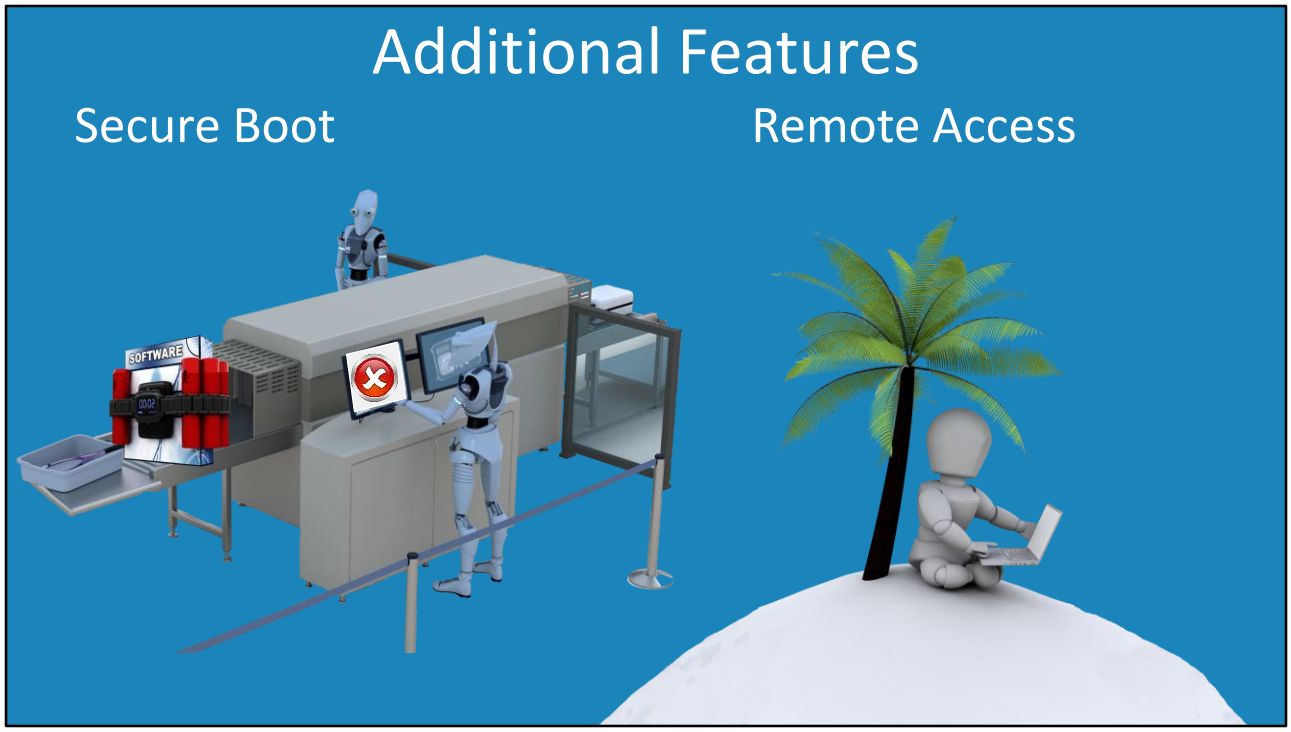
Supports storage drives over 2 TB
Supports GPT partition table

0:3:20 The next big difference is that UEFI supports larger storage devices. UEFI supports storage devices over two terabytes in size. It does this by using the GUID Partition Table or GPT partition table. BIOS uses a master boot record or MBR. MBR has the greatest compatibility since it has been around since the first personal computers were developed. However, MBR has a limit of only being able to address two terabytes of space. You will find however, that some operating systems and BIOS combinations will be able to use GPT drives as data drives and in some cases maybe able to boot from them. The difference with UEFI is that it will always support booting from a drive with GPT. BIOS will not always support booting from a GPT drive, it depends on which operating system is running. Linux will generally support it whereas Windows will generally not. Most UEFI will also have backward compatibility options. These options will allow UEFI to use a storage device with an MBR partition.

UEFI Storage Access



0:4:26 The next change is that UEFI can access local storage. If I open disk manager, you will notice that there is a partition called EFI. This EFI partition can be used by UEFI to load additional software. For example, some computers may have recovery tools installed in the EFI partition that UEFI can access. This essentially means that UEFI software is able to expand to be larger than what can be stored on the UEFI chip on the motherboard. It is important (as an administrator) not to delete this partition.



0:5:03 UEFI also offers a lot of other features. I won't go through all the features, but there are two more I will look at in detail. The first is secure boot. Secure boot essentially provides a method to check the operating system and its device drivers. If it has been modified by malware or an attack this will be detected. It does this by making sure the operating system and device drivers are digitally signed. In the case of Windows this is not a problem as Microsoft has signed their operating system and drivers. However, some alterative operating systems support secure boot while others do not. If you run Linux and compile a custom kernel this can also cause problems. If you experience problems, you can always switch secure boot off. The next feature that I will look at is remote access. Remote access allows the computer to be controlled from remote locations. Not all UEFI will support this and you will find the ones that do are the ones that are marketed toward the business market. To end this video, I will have a look at the setup of a UEFI computer so you can get an understanding where you may find the features that I talked about in this video and how they might work.

Demonstration

Hold down shift key when selecting Restart

ITFREETRAINING QUICK TIP

0:6:14 When I start the computer up, to enter the UEFI setup I need to press the delete key. Once in the setup, to access more features, I will press the “Advanced mode” button at the top right of the screen. Once in the advanced options, I will first look at secure boot. To access secure boot, I will select the option Security at the top. Once in the security settings, I will select the option Secure Boot. Secure boot is currently enabled; I can disable it by selecting it and pressing disable. If you are running an operating system that does not support secure boot, you will need to switch it off - otherwise the computer will not be able to start. If you are running an operating system that does support it, you should leave it on for extra security. In order for secure boot to work, keys from the manufacture of the software need to be installed. In the case of this motherboard, the main software manufacturer’s keys are included and can be installed by selecting the option “Install default Secure Boot Keys” and selecting Yes. In some cases, the key for your operating system may not be available (For example, the operating system you are using is not a commonly used operating system or is using a custom kernel). When this occurs, select the option “Key Management” to install additional keys so the operating system will be supported. The next set of options that I will look at are found under the Boot options. Notice the option for Fast Boot is currently set to “Ultra Fast”. UEFI supports a number of options to make the booting process faster. In this case, if Ultra Fast is selected, options like booting from USB devices is disabled. Also, since the computer boots so fast, it may be very difficult or impossible to enter the UEFI setup by pressing a key. However, later on I will show you a way to get around this. Notice that when I disable Fast Boot, an option appears at the bottom “CSM (Compatibility Support Module)”. If you require legacy BIOS features you may need to enter this option. Different UEFI will have different options.

Some BIOS may call it Run in Legacy Mode whilst others may call it CSM as in the case of this UEFI. Once selected, I will next enable it. Once enabled, this will change the other options in the menu. Some additional compatibility features will be enabled; however, some new UEFI features will be removed. The operating system you are running and what hardware you have will determine if you need to enable the Compatibility Support Module. If you do not need to enable it, I would leave it disabled as this allows you access all the new UEFI features. In this case, I will exit out of UEFI without saving any changes. I want to start the computer up in Windows mode to show another way to access the UEFI. Since I am not going to save the changes, Ultra Fast Boot is still enabled. In our videos we will often edit out delays to give you a better experience of watching the video. In this case, the video has not been edited so as to show you just how quickly the computer will start up and can be logged into Windows. This is a new install of Windows so it will boot quite fast anyway, but you can see how quick it can be. Once logged in, I will right click on the Start menu and select the Restart option. When I press Restart I will ensure that I am holding down the shift key, this will force the computer to allow me to choose additional options for the next restart. Once the menu appears, I will select the Troubleshooting option and then select Advanced options. On the Advanced options screen, notice the option for “UEFI Firmware Settings”. Once I select this option and then select the option Restart, the computer will reboot into the UEFI setup. If you are having trouble getting into the UEFI, which is harder if Fast Boot is enabled, this method is another way you can access it.

In The Real World

- Give UEFI a go
- Additional security features
- Enable Secure Boot if possible
- Disable features like Fast Boot if required

0:10:20 In the real world, if you are setting up a new computer give UEFI a go. UEFI is the future after all. I would personally try it and enable the legacy BIOS settings only if needed. UEFI does provide additional features including security features. If possible, enable Secure Boot. If you are running a newer version of Microsoft Windows this should not be a problem. If you are using an alterative operating system this may not be possible. If your boot up is compromised by malware or an attacker, Secure Boot will alert you that something has changed. If you are having problems, disable options like Fast Boot. Having Fast Boot enabled disables features like booting from USB drives. Depending on the feature you want to access, it may be a simple matter of disabling some features or enabling a feature in the setup. That concludes this video. I hope you have found this video useful and I look forward to seeing you in other videos from us. Until the next video, thank you for watching.

References
None

Credits
Trainer: Austin Mason http://ITFreeTraining.com
Voice Talent: HP Lewis http://hplewis.com
Companion Document: Phillip Guld https://philguld.com
Quality Assurance: Brett Batson http://www.pbb-proofreading.uk