Bits & Bytes

Arkansas' Premier Computer Club

February 2021

Bella Vista Computer Club - John Ruehle Center

Highlands Crossing Center, 1801 Forest Hills Blvd Suite 208 (lower level), Bella Vista, AR 72715

Website: http://BVComputerClub.org **Email: editor@bvcomputerclub.org**

COVID-19 VIRUS ADJUSTMENTS

During normal times all meetings are on the lower level of the Highlands Crossing Center in Bella Vista. During the COVID-19 pandemic we will continue to suspend in-person meetings and classes and conduct on-line meetings using Zoom over the Internet.

To attend a Zoom meeting or class, you need Internet access and a device with the Zoom application installed.

MEETINGS

(Online) Board Meeting: February 8, 6pm, using Zoom

(Online) General Meeting: February 8, 7pm, "**Introduction to Linux**", presented by Joel Ewing. This is a high-level view of a free alternative Operating System to MS Windows that has a significant number of users world wide and is available for PCs and other hardware platforms.

Zoom meeting access information will be emailed to membership the weekend before. Visitors or Guests may obtain Zoom meeting connection info from our website the weekend before the meeting.

Genealogy SIG: **No meeting** (3rd Saturday).

HELP CLINICS

No January Help Clinics at John Ruehle center

Members may request Remote Help on our website at https://bvcomputerclub.org at menu path Member Benefits ►Remote Help .

MEMBERSHIP

Single membership is $25; $10 for each additional family member in the same household. Join by mailing an application (from the web site) with check, or complete an application and pay at any meeting.

It is now also possible to Join or Renew membership on line on our website at https://bvcomputercub.org at menu path Get Involved ►Join/Renew . Payment may be by Credit Card, or, if you have a PayPal account, by whatever means you have defined on PayPal.

CLASSES

(Online) "Introduction to the Edge Browser" – Joel Ewing, Thursday, February 25, 10am – noon.

Advance sign up required for each listed class: Contact Grace: email to edu@bvcomputerclub.org, text 469-733-8395, call 479-270-1643, or sign up at the General Meeting. Classes are **free to Computer Club members.** Class access information will be emailed to those signed up for the class the day before class.

Check the monthly calendar and announcements for any last minute schedule changes at http://bvcomputerclub.org .

WHAT HAPPENS WHEN YOUR ZOOM HOST HAS A POWER OUTAGE – AND OTHER HAPPY TALES

By Greg Skalka, President, Under the Computer Hood User Group
August 2020 issue, Drive Light
www.uchug.org
president (at) uchug.org
Reprinted with permission from APCUG

In these COVID times, large gatherings are prohibited, so groups like ours can no longer meet in person. Fortunately, technology has come to our rescue, as many groups now hold virtual meetings through Zoom or another video conferencing service. As was made clear to me at our last meeting, however, technology runs on electricity, and you can’t participate when your power goes out. Several factors played in our favor, so for most attendees, the show went on without me with many probably unaware. As long as the outage is not too widespread and the meeting is set up correctly, we found Zoom is very robust and fault-tolerant, even when the meeting host drops off.

Our last physical meeting was in the first week of March, just before our meeting venue was closed to outside groups. Since then, we have met in the cloud on Zoom quite successfully. A large part of that was due to APCUG (Association of Personal Computer User Groups), of which our group is a member. APCUG has provided us access to one of their paid Zoom accounts, so our meetings can run their normal two-hour duration (avoiding the time limits of a free account). Additionally, our board meets once a month using Zoom. For three of our four Zoom general meetings, APCUG also provided us with presentations through their Speakers Bureau presenters. We are now so used to the virtual meeting format that it has become routine. That is often when fate decides it is time to throw a curveball.

Our July meeting initially followed our now-familiar script. I had scheduled our meeting using the APCUG Zoom account and sent the meeting information to our editor, Art, so that it could be sent out through the member email list. Thirty minutes before the meeting start time, I logged into Zoom and started the meeting session.

While we so far have not had any of the virtual meeting problems other non-APCUG groups have reported (like Zoom-bombing), we try to follow all recommended security precautions. We now use a passcode for our meetings to reduce the chance of random interlopers. We have also enabled the Zoom waiting room, which keeps those joining in a virtual holding area until admitted to the meeting by the meeting host. We don’t publish our meeting’s Zoom information, but instead, send it only to our members, vetted guests, and those that have requested it through email (and have provided a name so that they can be recognized in the waiting room).

To help me in this waiting room filtering, our editor tries to come into the meeting early. I make him a co-host, giving him the power to see and admit from the waiting room (and, as it turns out, take over should something happen to me, the host). In those 30 minutes before the meeting, I also share my screen periodically, showing a few presentation slides with basic meeting information for the evening, so attendees know they are in the right place and know what to expect.

At about 7 PM I started our July meeting with an introduction of the evening’s agenda. Following tradition, I then made our Webmaster, Bob, a co-host, so that he could share his screen and show us the links to new, exciting and helpful software he had added this month to the Library Links section of our web site (www.uchug.org).

Following Bob’s report, I introduced our APCUG Speakers Bureau presenter for the evening, Francis Chao, and made him a Zoom co-host. Francis then shared his screen for the first of his two presentations, a comparison of cloud storage services. I’m not that enamored with cloud storage, so I was waiting for his second presentation (which I had suggested to the board), USB-C.

Francis was probably about halfway through his interesting USB-C presentation (around 8:15 PM) when I suddenly heard the sickening sound of a power outage. Some might say that a power outage makes no sound, that it is more an absence of sound, but I disagree. The clicks of relays switching off, the change in pitch of computer fans slowing down and the frequency of power supply hum changing all make up the sound I recognize as power failure. Even before my eyes could tell my brain about the sudden loss of photons, it knew from the sound what had happened.

Since the desktop PC, I was Zooming on did not have a UPS or uninterruptable power supply, I sat there in the dark for a moment, wondering how widespread the outage was. Though it was past sunset, I could see by the dim outside glow enough to get up and out of the upstairs computer room. I saw through the front windows that my street was dark and neighbor kids were starting to come outside with flashlights.

My first concern was for the safety of the first lady. I found my wife downstairs in her office, on her computer. She has a practically brand-new desktop PC with dual monitors and a UPS with a brand-new battery. I had replaced everything for her at the beginning of the year in response to that now insignificant crisis, the Windows 7 end-of-life. She sat in the glow of the monitors. I told her to save and close everything, and then shut her computer down.

The next course of action was to get flashlights. We have a handy rechargeable flashlight plugged into an outlet in our downstairs hall. The flashlight part sits in a charging base, so it is always ready. The light comes when it loses its input power (either from being lifted out of its base or by an outage). When the power went off, the flashlight came on like a beacon. I took the flashlight out of the holder and proceeded to the garage, where our emergency flashlights were stored with our camping gear.

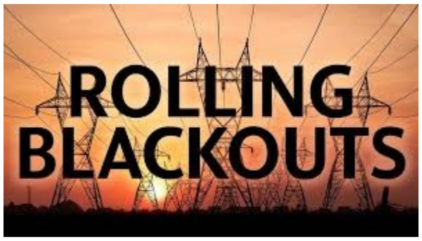
Going into the garage, I instinctively flipped on the light switch, and then realized that was a pointless action. I would find myself doing the same thing several more times before the power came back. I got to the camping gear and found the flashlights, but they were all dead. “Time to buy more 6V lantern batteries,” I told myself. I took my rechargeable auto trouble light from the garage and went back to the house.

It was finally time to send a text to Art to tell him my street’s power was out. Was the Zoom meeting still going? He replied that it continued without me. Having others as co-hosts allowed Zoom to handle my dropping out and continue with the meeting. Likely, most attendees didn’t even notice.

I next went around the house looking for things that should be turned off, so surges, when power is restored, won’t cause additional damage. I turned off the PC I had been using for the Zoom meeting. My laptop was on as it has a built-in UPS, its battery. Not sure how long the power would be off, I shut it down. I also have an old XP desktop in my home office that now was quiet. It normally is always on, except during a power outage. The automated call we received from SDG&E indicated the power was estimated to be restored by 2:30 AM. I went around the house turning off light switches, in case it did come back on after we had gone to bed.

Around 9:30 PM the power came back on. I sent Art another text; he said the meeting had ended about 30 minutes earlier. The meeting had worked out fine despite my being powerless.

Next came the most annoying part of a power outage – resetting the many clocks that have no power backup. I also had to wait for the modem and router to come back up, for my Wi-Fi mesh router to restart and for all my Wi-Fi devices to reconnect. Since I’d need my desktop PC working in the morning to take my online health assessment so I could go into work in these COVID times, I had to verify it would boot up. I tried turning on my XP computer, but it would not show any signs of life. The last time I had shut it off I had problems getting it to start again. At the time, I thought the power supply has a problem but managed to get it running. Now I left its diagnosis for another time.



It turns out this outage was just a warm-up (pun intended) for another one we had about a week later. An excessive heatwave in the west meant the possibility of rolling blackouts instituted by the utility company. We had our power shut down for about 30 minutes, but this time it was around dinner time and still light outside. I’d at least learned my flashlight lesson and bought some lantern batteries a few days before.

With our hottest days in San Diego probably still ahead this year, we should count on losing power again soon. Whether due to rolling black-outs to reduce stress on the power grid or shut-downs to reduce wildfire risk, any of us could have that powerless feeling in our future. Now is time to prepare – stock up on batteries, get those UPS units working and back up and save your computer work often.

UEFI CONFIGURATION FOR BOOTING LIVE MEDIA

By Dick Maybach, Brookdale Computer User Group
www.bcug.com
n2nd (at) att.net
Reprinted by permission from APCUG

In modern PCs the boot process is controlled by a Unified Extended Firmware Interface (UEFI), that has replaced the old Basic Input-Output System (BIOS), see https://en.wikipedia.org/wiki/Unified_Extensible_Firmware_Interface. Most users, who purchase a machine with Windows installed, can ignore the change, but if you wish to change its configuration you will have to be aware of its differences. In particular, if you wish to enable booting from a live USB device you will want to:

- require a password to access the PC,
- allow booting an alternate operating system from a live memory stick or DVD, and
- allow other operating systems than Windows.

The first challenge is to access the configuration utility, which requires tapping keys during the boot process. (You will have to be quick.) The details vary with the manufacturer, but some common ones are:

- ASUS PCs: <F2>,
- ASUS Motherboards: <F2> or <DEL>,
- Acer: <F2> or <DEL>,
- Dell: <F2> or <F12>,
- Gigabyte/Aorus: <F2> or <DEL>,
- HP: <F10>,
- Lenovo Laptops: <F2> or <Fn> + <F2>,
- Lenovo Desktops: <F1>,
- Lenovo ThinkPads: <ENTER> then <F1>.
- Samsung: <F2>, and
- Toshiba: <F2>.

Check your documentation for others. Windows 10 users can also reach their UEFI configuration through the Advanced Start Menu.

The storage area available to a BIOS was limited, which meant that configuring one was relatively simple, but this restriction was eliminated for a UEFI. As a result, manufacturers have added numerous “features” to differentiate their products from the competition. For example, I have two nearly identical

Dell laptops, the older using a BIOS (with five setup screens) and the newer using a UEFI (with nearly 70). The major problem with the latter is finding what is important to you.

You can improve your PC’s security by enabling passwords; however, these aren’t effective against a knowledgeable attacker, as they can be disabled by opening the case and manipulating a switch or jumper. There are two passwords, “system” allows the boot process to proceed and “administrator” allows changing the UEFI configuration. You should always enable an administrator password to prevent someone from enabling booting from your USB port, which would allow them to boot a live medium and access your disk. For a similar reason, if you’ve enabled USB booting yourself, prevent someone else from doing so by setting a system password.

Figure 1 shows the opening UEFI configuration screen on my Dell laptop, which displays its table of contents.

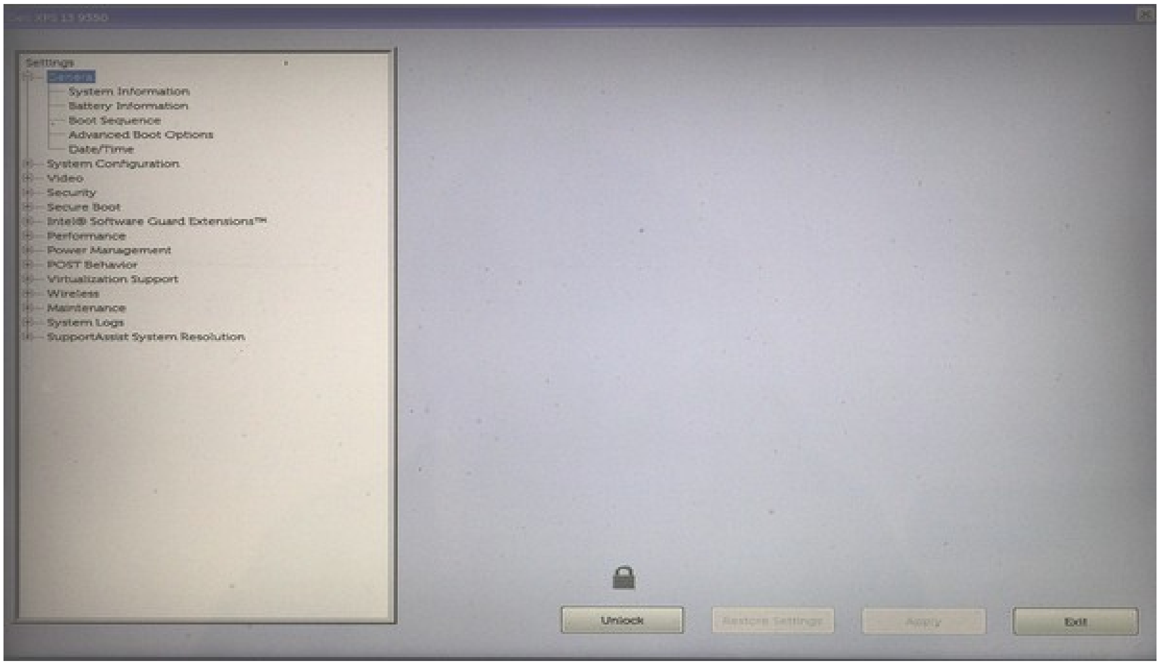


Figure 1. UEFI First Configuration Screen.

Note the Unlock button at the bottom. Select this and enter your administration password, assuming you’ve set one, to make changes.

Most PCs require a keypress at the start of the boot process to enable booting from a USB port (assuming of course you’ve enabled it). Here are some common ones.

- Acer: <Esc> or <F9> or <F12>
- Asus: <Esc> or <F8>
- Dell: <F12>

- Fujitsu: <F12>
- Gigabyte: <F12>
- HP: <Esc> or <F9>
- Intel: <F10>
- Lenovo: <F12>
- Samsung: <Esc>
- Toshiba: <F12>

Check your documentation for others.

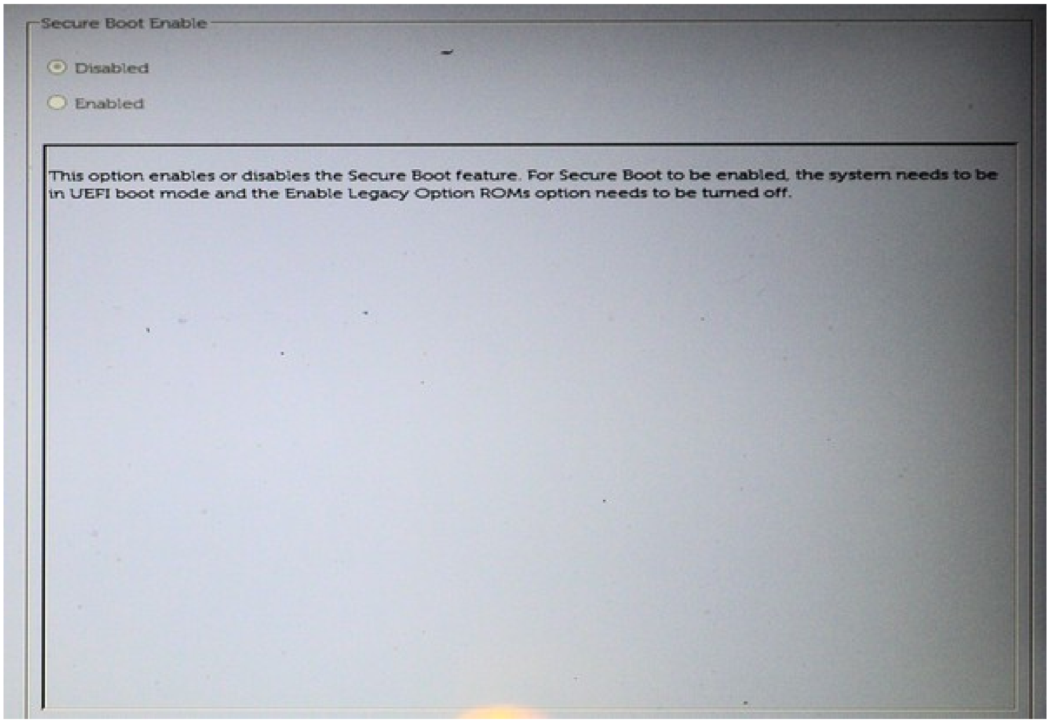
To enable booting from a USB device you will make these changes.

- Disable secure boot.
- Set the boot sequence.
- Enable booting from legacy ROMs.
- Enable USB boot support.
- Disable fast boot.

Record its settings before you change anything on a screen (taking a cell-phone photo is a convenient way to do this). Some settings will result in your PC being unable to boot (ask me how I know), but this isn't a problem if you can undo your last change. If all else fails, most UEFIs have a way to restore the factory settings. On my Dell, it's on the screen of Figure 1 as the (grayed out) button at the right of Unlock. It is enabled by unlocking the UEFI configuration.

Secure boot prevents booting from any operating system that doesn't have a Microsoft certificate, which few OSes other than Windows have. You must disable this if you want to run Linux[1], but it is a security feature, and you may wish to enable it when you go back to Windows. Figure 2 shows the appropriate screen on my Dell, which follows the security section.

[1] No longer true for newer Linux versions. RedHat, Fedora, SUSE, Ubuntu, Debian, and possibly other Linux distros now have support for Microsoft-signed kernels which allow them to function with Secure Boot.   However, some third-party applications (VirtualBox) under Linux which require loading of additional application kernel modules during the boot process, are more difficult to maintain with Secure Boot. They require using a Machine Owner Key (MOK), defining that key to the hardware, and using that key to "sign" those modules whenever they change, or they will fail to load and the application will not function with Secure Boot enabled.   Also note that an Operating System that was installed with Secure Boot enabled may not boot with Secure Boot disabled, and visa versa.   The secure boot certificate signature embedded in a code module is based on a hashed value of bytes in the module, so it will block execution at boot time of both malware-replaced modules from un-trusted sources (unsigned), or modules modified by malware (invalidated signature). Secure Boot blocks one entire class of malware. [editor]



Secure Boot Enable

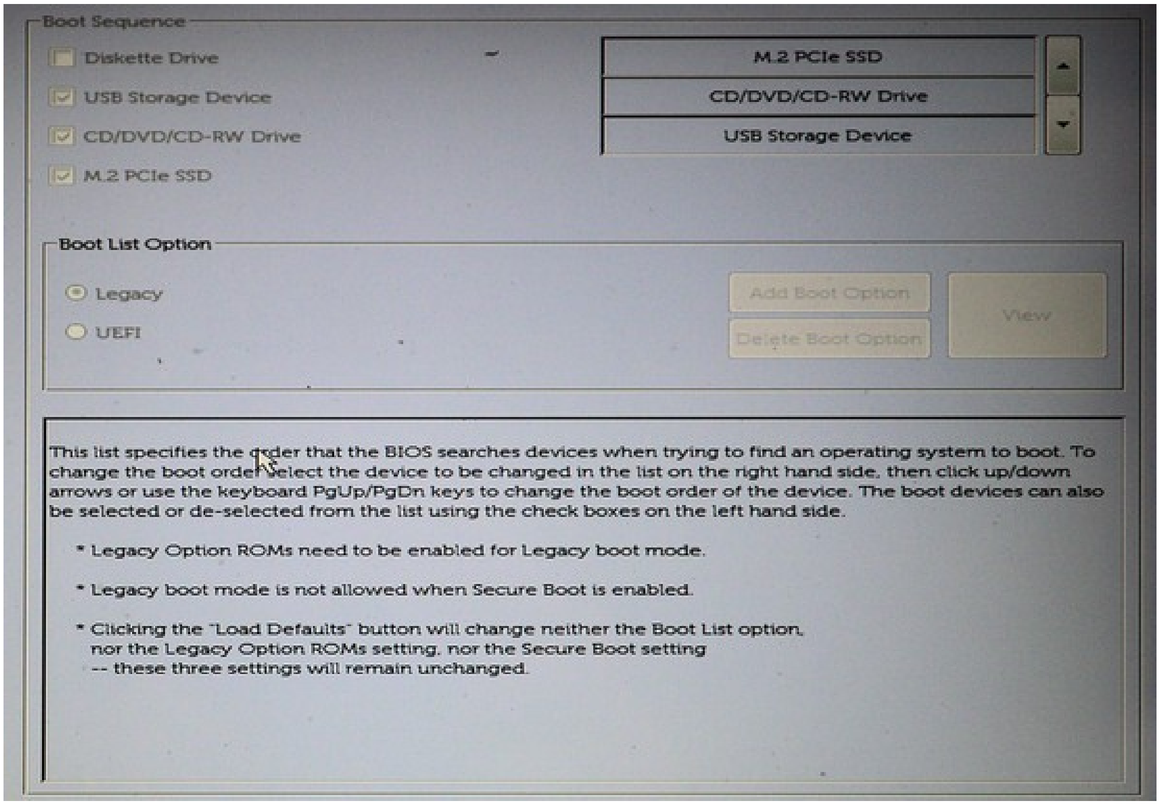
● Disabled

○ Enabled

This option enables or disables the Secure Boot feature. For Secure Boot to be enabled, the system needs to be in UEFI boot mode and the Enable Legacy Option ROMs option needs to be turned off.

Figure 2. Secure Boot Screen.

Set the boot sequence to include USB devices, Figure 3.



Boot Sequence

□ Diskette Drive

☑ USB Storage Device

☑ CD/DVD/CD-RW Drive

☑ M.2 PCIe SSD

M.2 PCIe SSD
CD/DVD/CD-RW Drive
USB Storage Device

Boot List Option

● Legacy

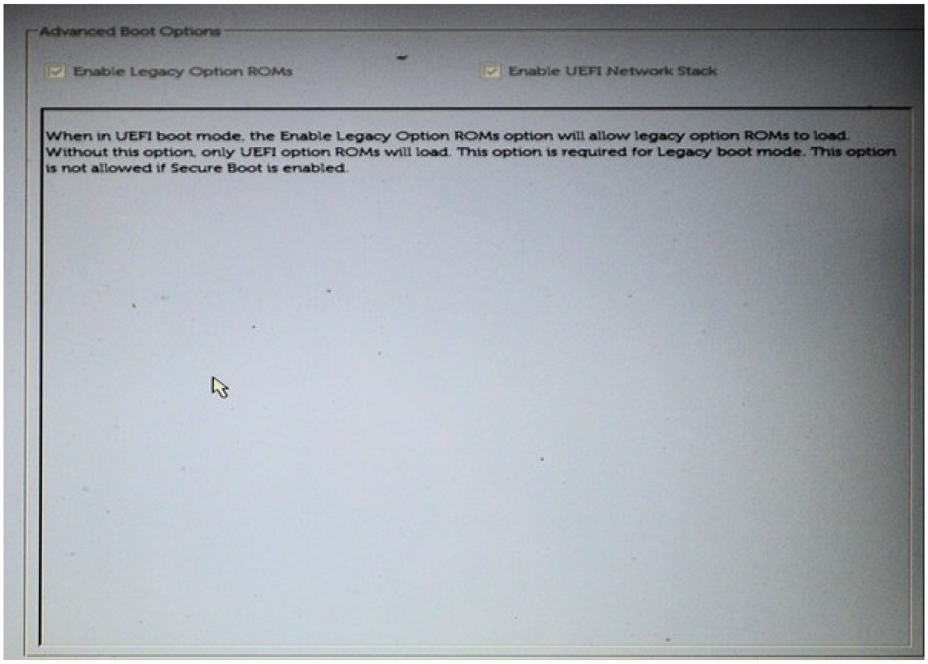
○ UEFI

This list specifies the order that the BIOS searches devices when trying to find an operating system to boot. To change the boot order select the device to be changed in the list on the right hand side, then click up/down arrows or use the keyboard PgUp/PgDn keys to change the boot order of the device. The boot devices can also be selected or de-selected from the list using the check boxes on the left hand side.

- * Legacy Option ROMs need to be enabled for Legacy boot mode.
- * Legacy boot mode is not allowed when Secure Boot is enabled.
- * Clicking the "Load Defaults" button will change neither the Boot List option, nor the Legacy Option ROMs setting, nor the Secure Boot setting -- these three settings will remain unchanged.

Figure 3. Boot Sequence.

Following the advice on Figure 3, enable legacy option ROMs, Figure 4.



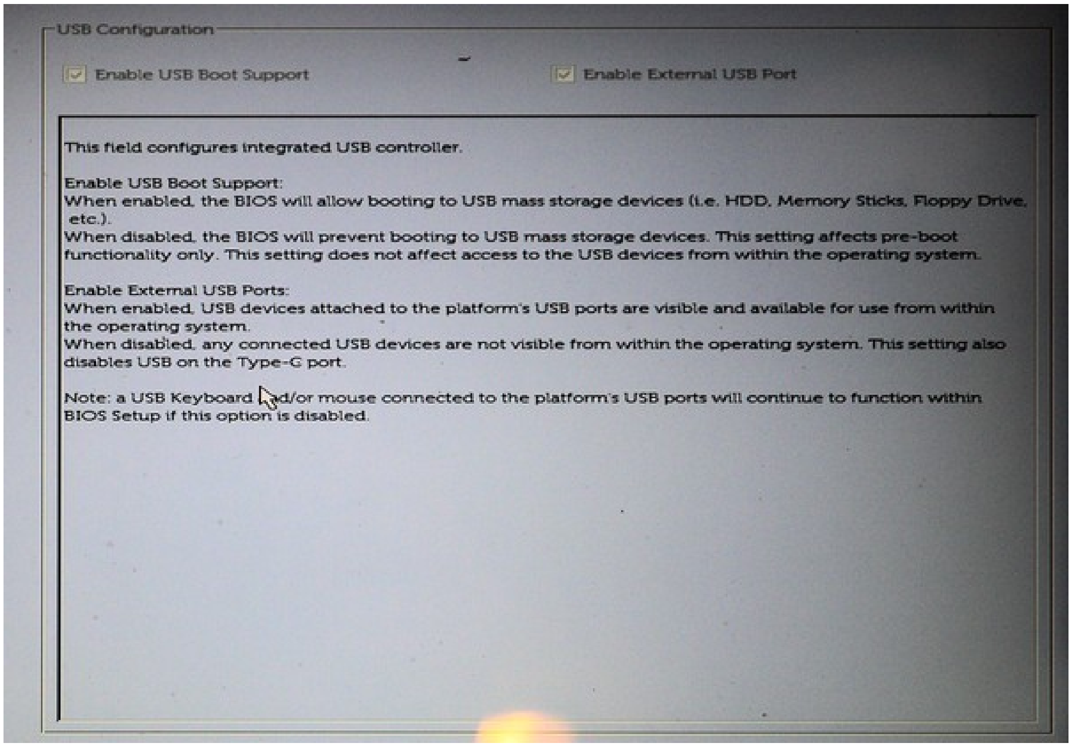
Advanced Boot Options

☑ Enable Legacy Option ROMs ☑ Enable UEFI Network Stack

When in UEFI boot mode, the Enable Legacy Option ROMs option will allow legacy option ROMs to load. Without this option, only UEFI option ROMs will load. This option is required for Legacy boot mode. This option is not allowed if Secure Boot is enabled.

Figure 4. Enable Legacy Option ROMs.

Also enable USB boot support, Figure 5.



USB Configuration

☑ Enable USB Boot Support ☑ Enable External USB Port

This field configures integrated USB controller.

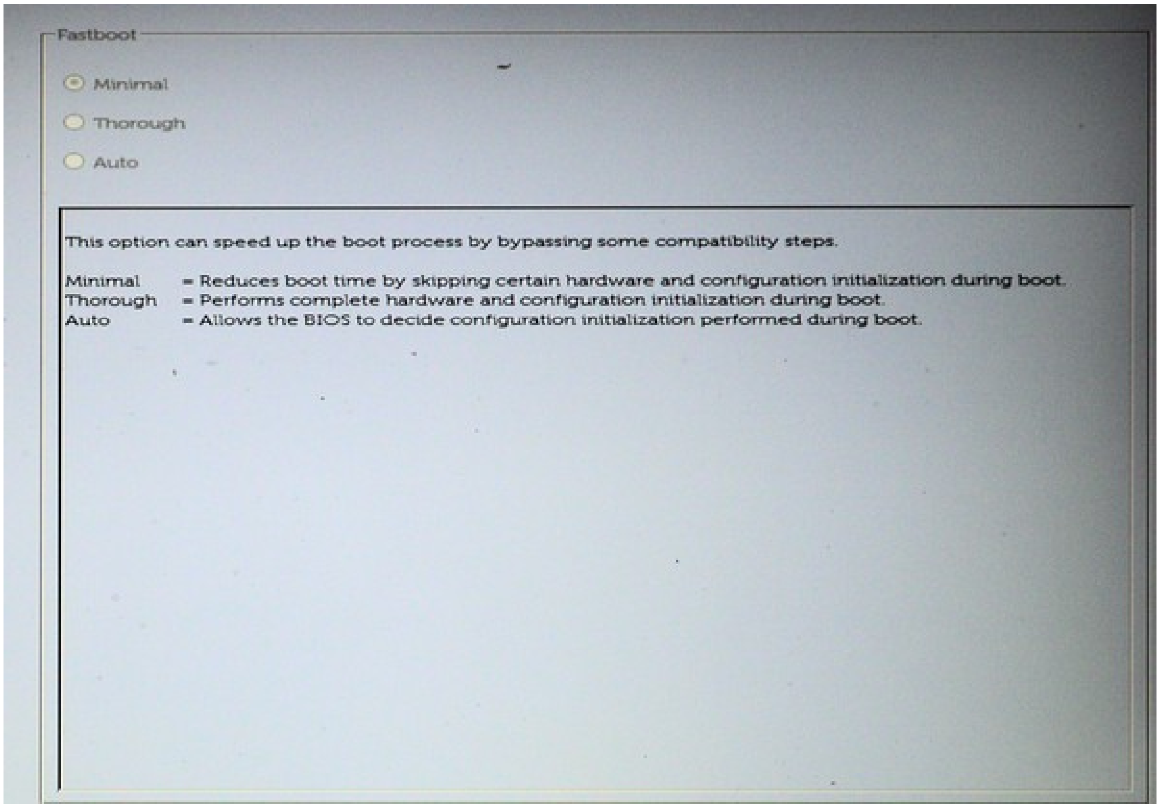
Enable USB Boot Support:
When enabled, the BIOS will allow booting to USB mass storage devices (i.e. HDD, Memory Sticks, Floppy Drive, etc.).
When disabled, the BIOS will prevent booting to USB mass storage devices. This setting affects pre-boot functionality only. This setting does not affect access to the USB devices from within the operating system.

Enable External USB Ports:
When enabled, USB devices attached to the platform's USB ports are visible and available for use from within the operating system.
When disabled, any connected USB devices are not visible from within the operating system. This setting also disables USB on the Type-C port.

Note: a USB Keyboard and/or mouse connected to the platform's USB ports will continue to function within BIOS Setup if this option is disabled.

Figure 5. USB Boot Support.

Finally, disable fast boot support, Figure 6, as this is compatible only with recent versions of Windows.



Fastboot

● Minimal

○ Thorough

○ Auto

This option can speed up the boot process by bypassing some compatibility steps.

```
Minimal     = Reduces boot time by skipping certain hardware and configuration initialization during boot.
Thorough    = Performs complete hardware and configuration initialization during boot.
Auto        = Allows the BIOS to decide configuration initialization performed during boot.
```

Figure 6. Disable Fast Boot.

Although I’ve used Dell as an example, the UEFI configuration on your PC is probably similar. Explore carefully, read the help text, and be sure you can undo your changes. Even if you don’t make changes, exploring your UEFI configuration will tell you much about your PC.