APU Forensics Fieldkit

Getting Started:
System Requirements

Getting Started

Windows 10 configuration tends to "drift" away from stability over time with continuous updates

This can cause subtle problems for apps – problems you may not notice until something won't start

It may seem like a problem with the app, *but it is not* – it is a problem with Windows!

Fixing these problems requires a command line interface – there is no other way to get this done

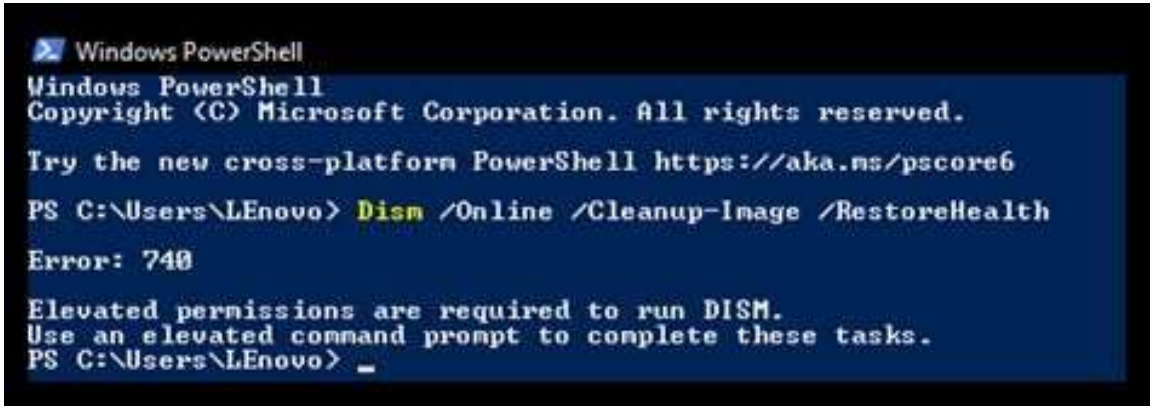
Fixing Windows

We have to run two apps from the Windows command line:

a) **dism** checks Windoze Update to make sure everything is correct (so it needs a network connection)

b) **sfc** uses the files maintained by **dism** to fix configuration issues in the running system

These both require Administrator Privileges



- Start Menu
- Windows System
- Command Prompt
- Right Click -> More
- Run as Administrator

Getting Started: 1) Windows system

Be Patient: these will take a few minutes, but let each command finish to 100%.
There may be some pauses in progress, this is normal.

```
dism /Online /Cleanup-Image /RestoreHealth
```

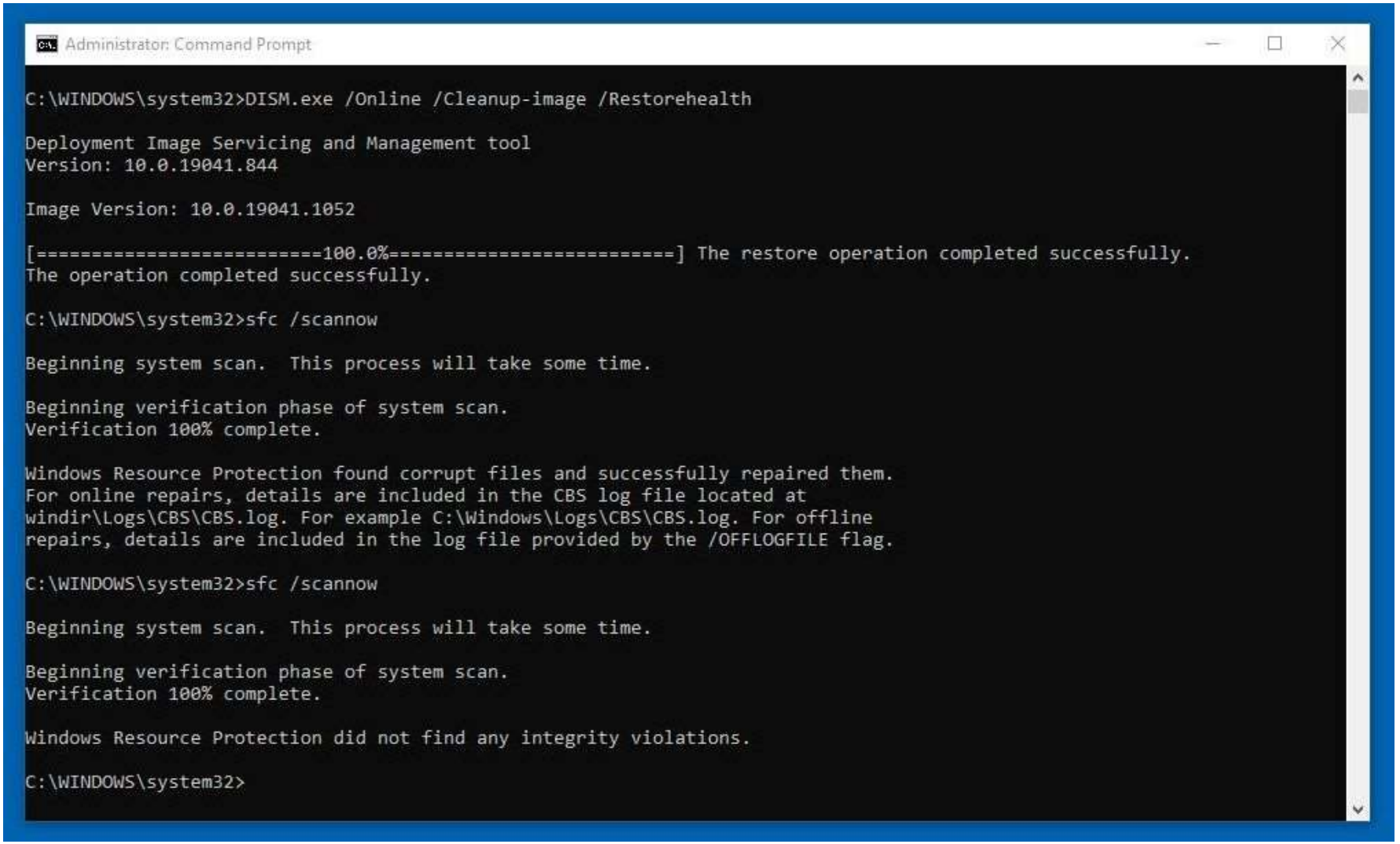
wait for **dism** *to finish before running* **sfc**

```
sfc /scannow
```

if sfc reports that it fixed errors, run it again
(it can take up to 3 runs to make it happy)

when sfc reports no errors, shut down and restart

Run as Administrator




Q&A

BIOS

- The Basic Input Output System (BIOS) is code on a chip on the system motherboard.
- When the system is powered on the BIOS is the first software that runs. It identifies the hardware, configures it, tests it, and connects it to the operating system for further instruction.
  - This is called the boot process.

[Video] what is bios
https://support.lenovo.com/videos/VID100790

BIOS Settings

- Entering the BIOS setup utility allows you to change the boot process order as well as a variety of CPU settings.
- Unified Extensible Firmware Interface (UEFI) is similar to BIOS, but has some advantages.
  - It can boot from USB disks, has a graphical user interface with network capability, and is backward and forward compatible.
- Over time, UEFI is expected to replace direct access to the BIOS.

Getting Started: 2) Virtualization Enabled?

- Hardware support for virtualization (**Intel VT-x or AMD-v**) is ***always required*** to run **64bit VMs**, and any VM that uses more than one CPU core.
  - Virtualbox versions 5 and 6.0 (July 2020) can run 32-bit VMs with software virtualization on ***almost*** all hosts (no VT-x or AMD-V setting in the BIOS is required)
  - MyTyVM is one of the last 32-bit single-core VM Guest operating systems

Start Menu - Windows Admin Tools - System Info

- **at the bottom**
  - Hyper-V - Virtualization Enabled in Firmware: **Yes**
    - **Ready to go**

Getting Started: 2) Virtualization Enabled?

Start Menu - Windows Admin Tools - System Info

- **at the bottom**
  - Hyper-V - Virtualization Enabled in Firmware: **No**
- You need to enable hardware support for virtualization in the host system BIOS.
- Note your exact system model, then check how to get into the BIOS settings at boot time.
- Once you get there you need to track down the setting, which is buried in a menu
  - There are examples at the end of this document


Q&A

Getting Started: 3) Install Virtualbox

VirtualBox 6.1.20 (released 20 April 2021)

- VMM: Fixed guest OS hanging under certain circumstances when Hyper-V is present

The current version is recommended for download

- Comes in two parts because of copyright
  - Platform Pack (main application) **(Required)**
  - Extension Pack (licensed) **(Optional)**

BE SURE to
Right-Click and Run As Administrator
when you install

Virtualbox works best from the default location – C:\Program Files
(You can put the VMs anywhere)

Getting Started: 4) Create a VM

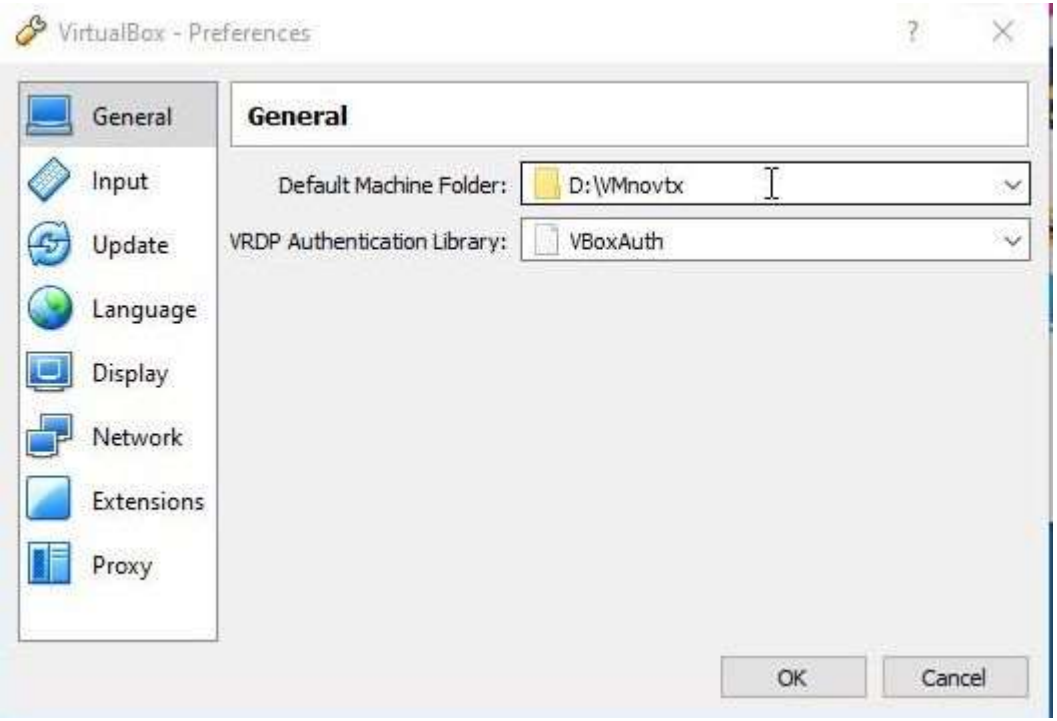
Download the Base.iso from http://my-tiny.net

and follow the pdf or the video

Virtualbox 6 has a slightly different icon layout than the version 5 interface in the videos, but it is not a problem.

Where to put the VMs

File > Preferences

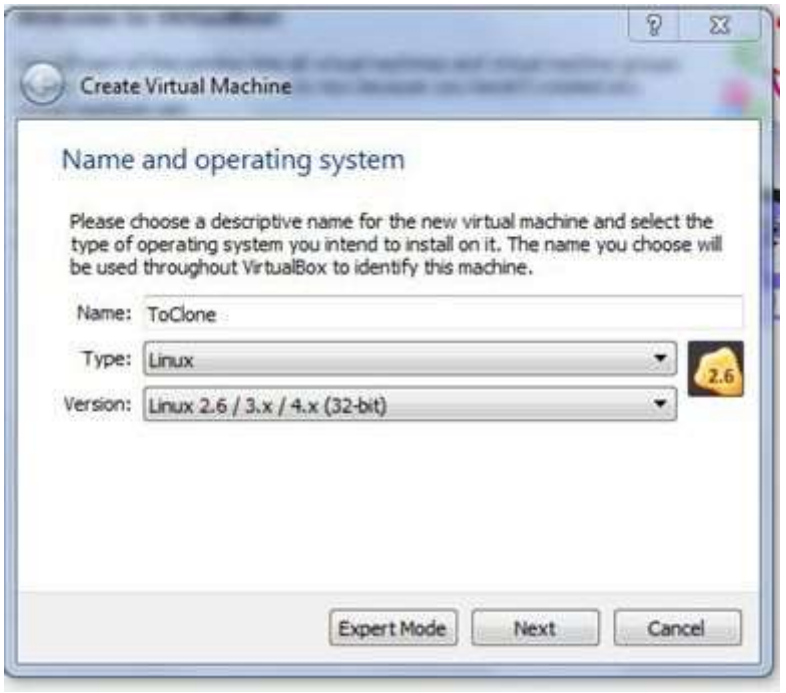


- You can store your VMs anywhere by setting the **Default Machine Folder**
- But Remember: Windoze may change drive letters for removable drives

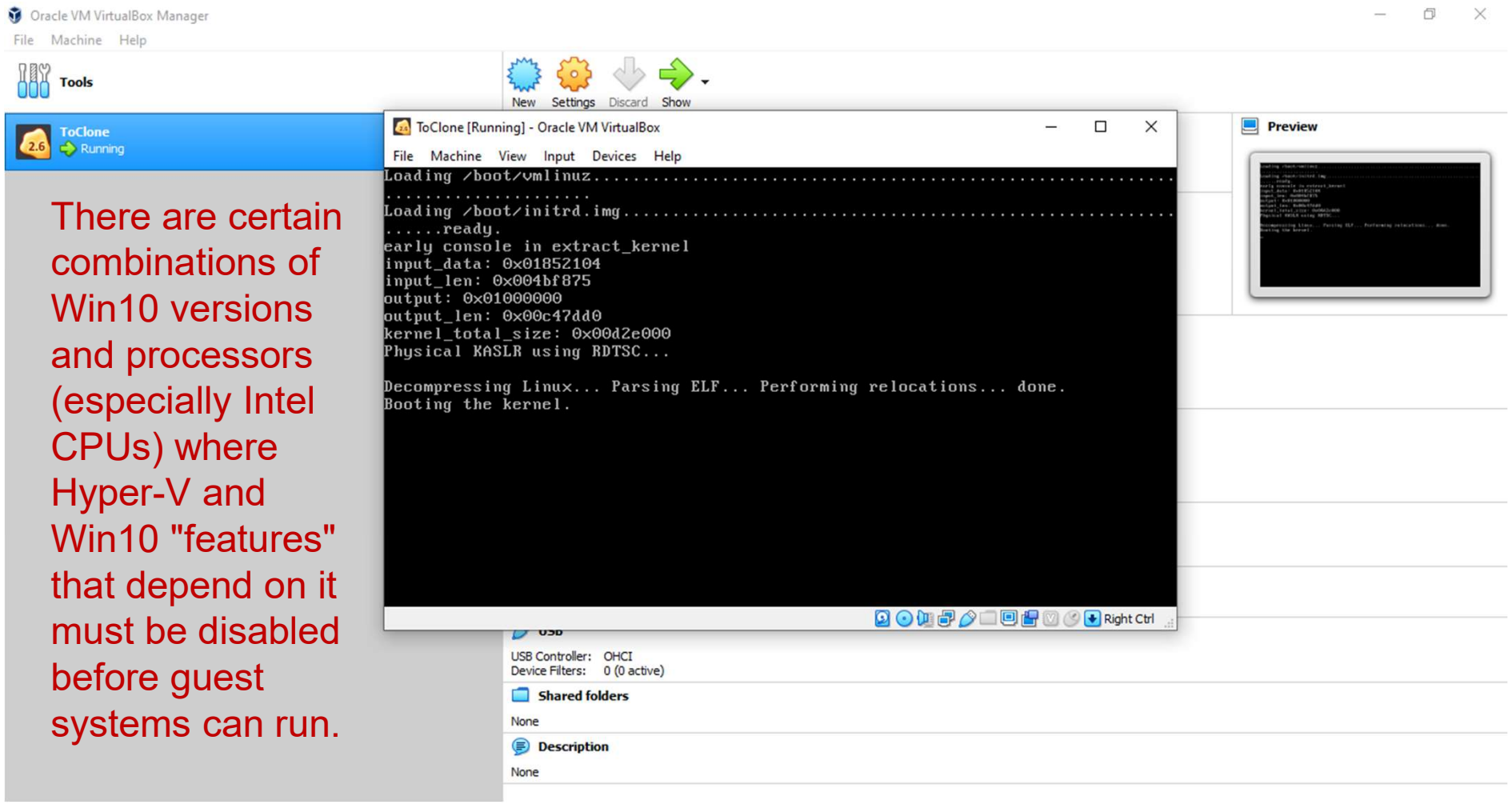
Exit Virtualbox after [OK] to be certain the setting is properly saved

TinyNet: linux 2.6/3x/4x/ (32-bit)

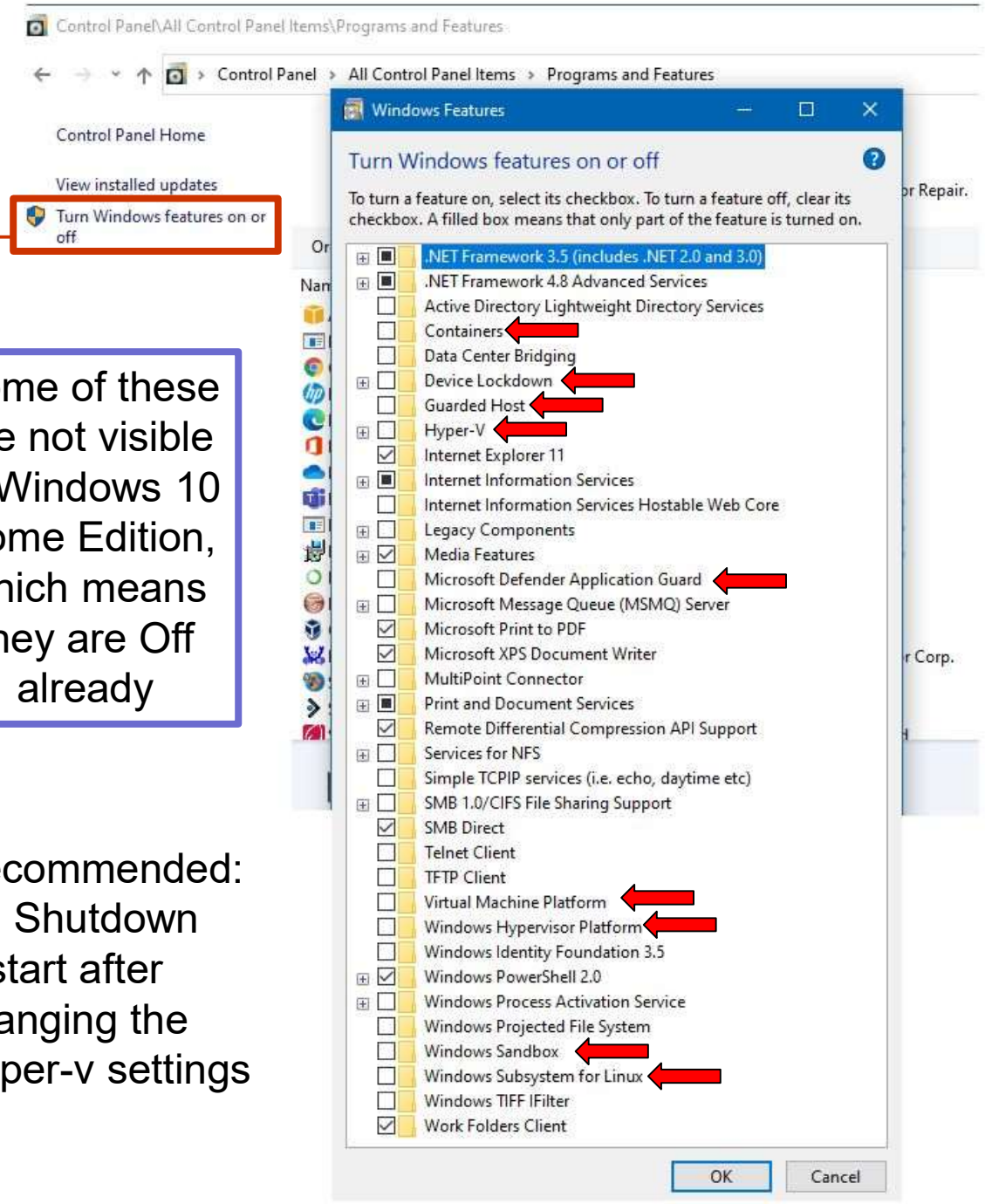
- When creating a VM, make sure you choose the proper version of the guest OS template
- Choosing the correct template allows virtualbox to select the correct settings for other processor features - it's not *just* about 64bit capability any more.



If the VM freezes, Disable Hyper-V



There are certain combinations of Win10 versions and processors (especially Intel CPUs) where Hyper-V and Win10 "features" that depend on it must be disabled before guest systems can run.



Some of these are not visible in Windows 10 Home Edition, which means they are Off already

Recommended: full Shutdown restart after changing the Hyper-v settings

- **Start menu**
- **Windows Sytem**
- **Control Panel**
- **Programs and Features**
- **Turn Features on or off**

ALL Hyper-V settings OFF

Caution!

Running VMs on a laptop:

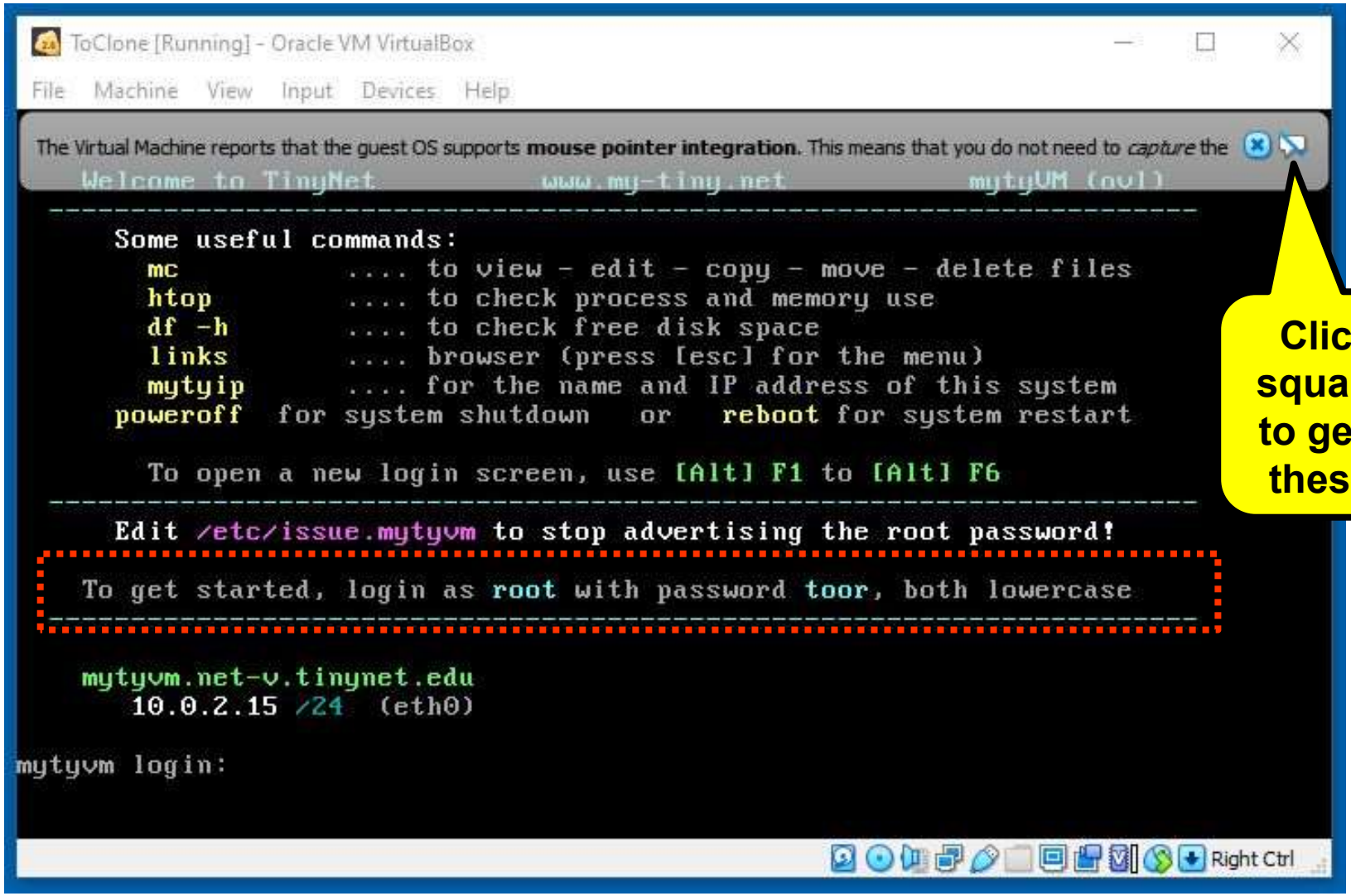
Check your power settings – close lid, low battery, etc.

Never **Hibernate**, only **Sleep**

("Hibernate" suspends too many host processes, and your VM will get corrupted – "Sleep" works well enough)

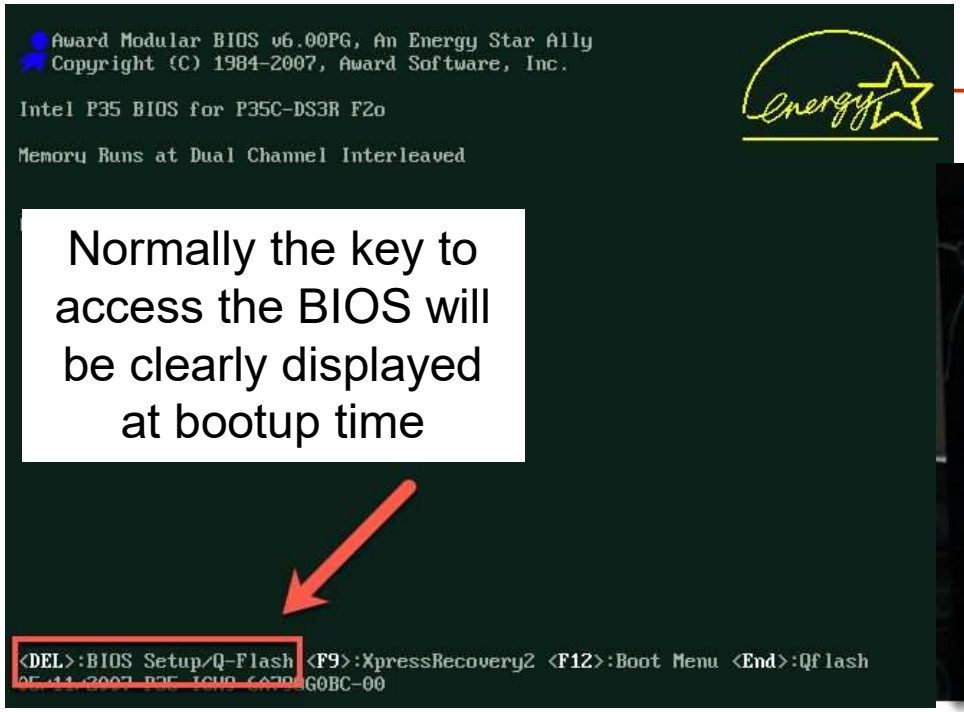
(or … just make sure you ALWAYS poweroff the VM)

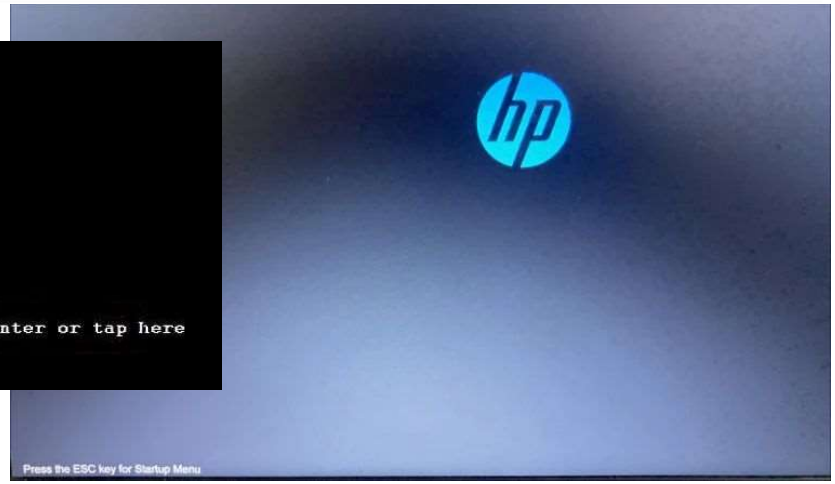
Logging in


ToClone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
The Virtual Machine reports that the guest OS supports mouse pointer integration. This means that you do not need to capture the
Welcome to TinyNet www.my-tiny.net mytyVM (avl)
Some useful commands:
mc .... to view - edit - copy - move - delete files
htop .... to check process and memory use
df -h .... to check free disk space
links .... browser (press [esc] for the menu)
mytyip .... for the name and IP address of this system
poweroff for system shutdown or reboot for system restart
To open a new login screen, use [Alt] F1 to [Alt] F6
Edit /etc/issue.mytyvm to stop advertising the root password!
To get started, login as root with password toor, both lowercase
mytyvm.net-v.tinynet.edu
10.0.2.15 /24 (eth0)
mytyvm login:
Right Ctrl
Click this square icon to get rid of these bars

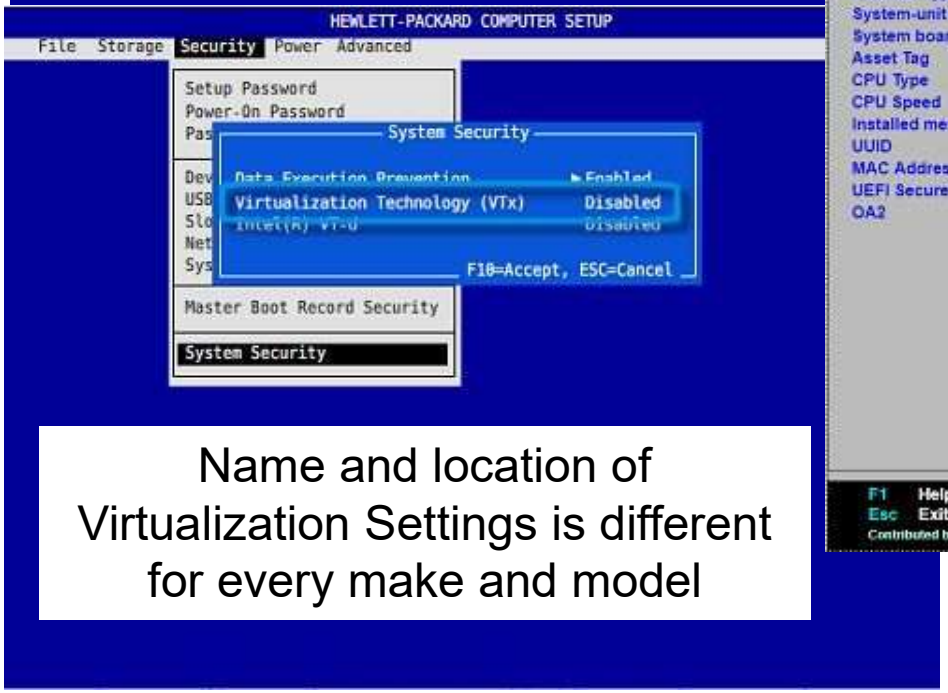

Q&A

Keep pressing the key 2 times per second until the BIOS Menu is displayed

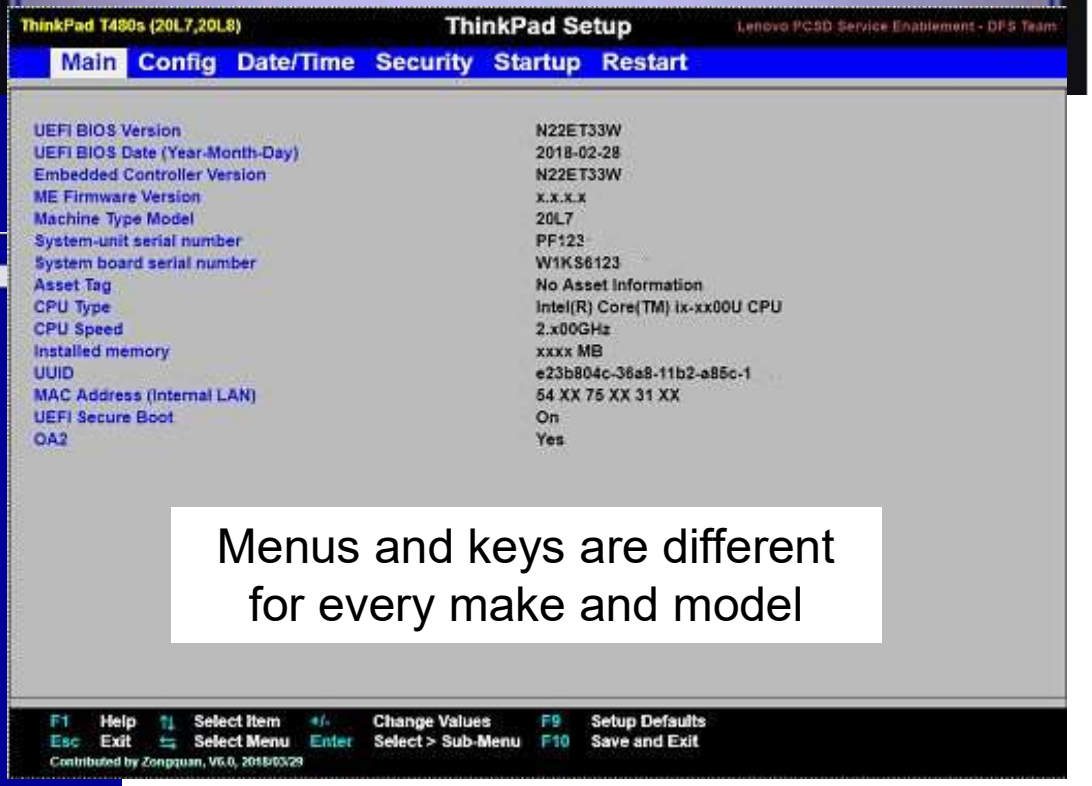




BIOS Setup Utility



Name and location of Virtualization Settings is different for every make and model



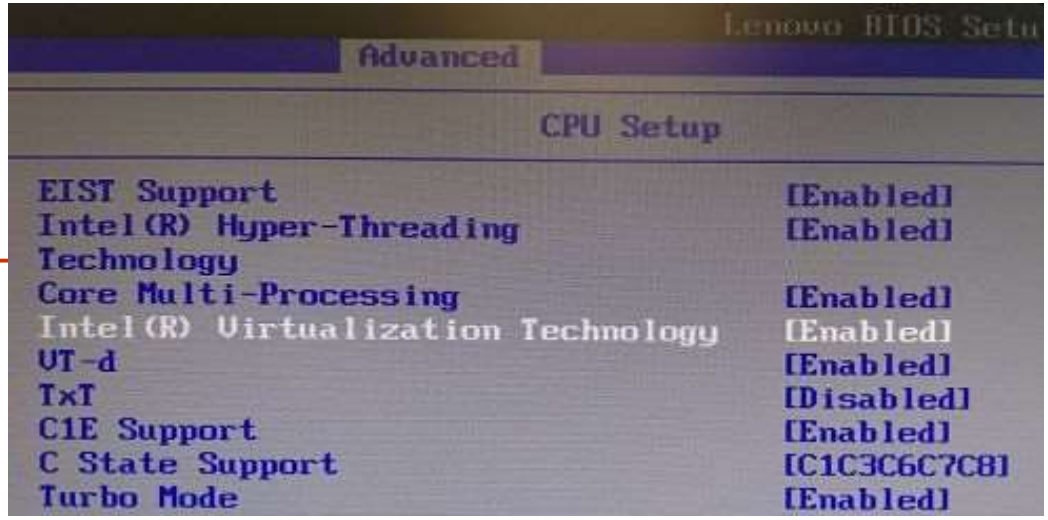
Menus and keys are different for every make and model

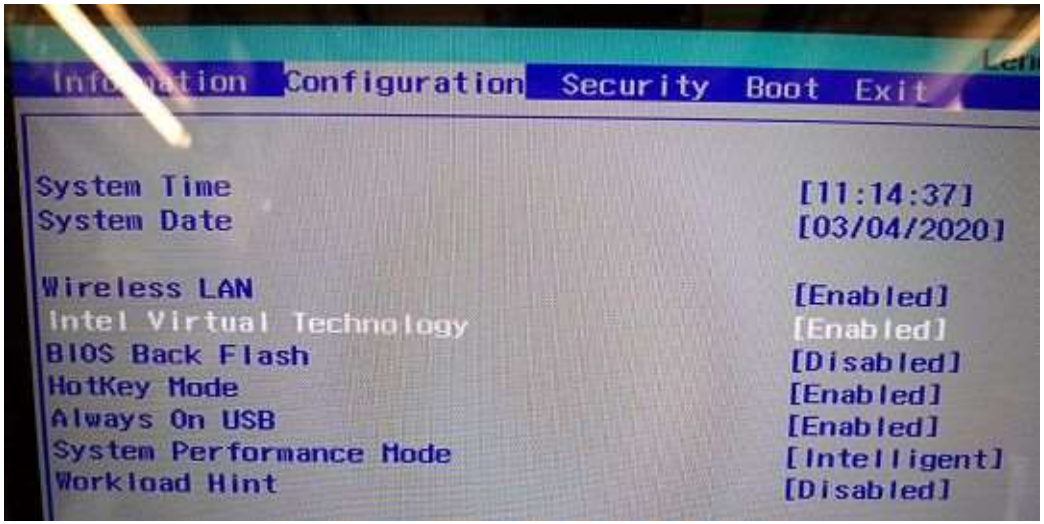
The option *should be called something like*

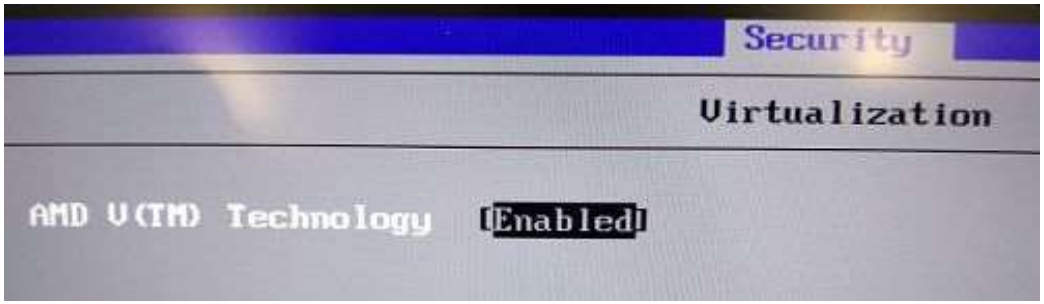
- Virtualization
- Intel VT-x
- AMD V
- Secure Virtual Mode
- SVM Mode

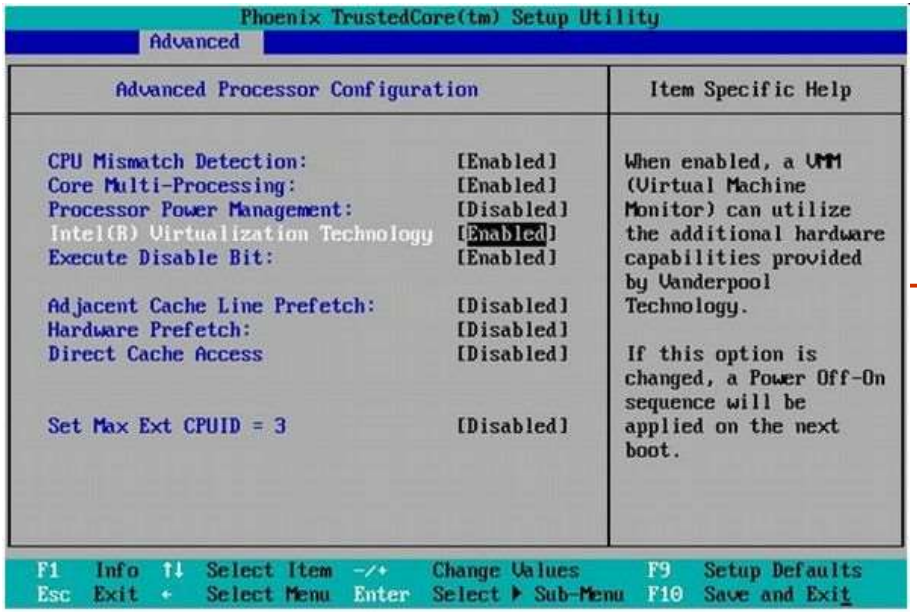
The option *is usually* in

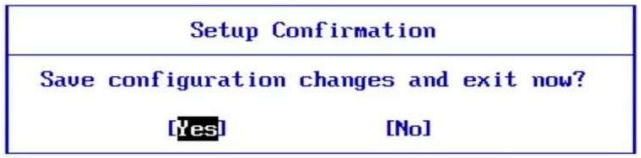
- Security
- Configuration
- Advanced

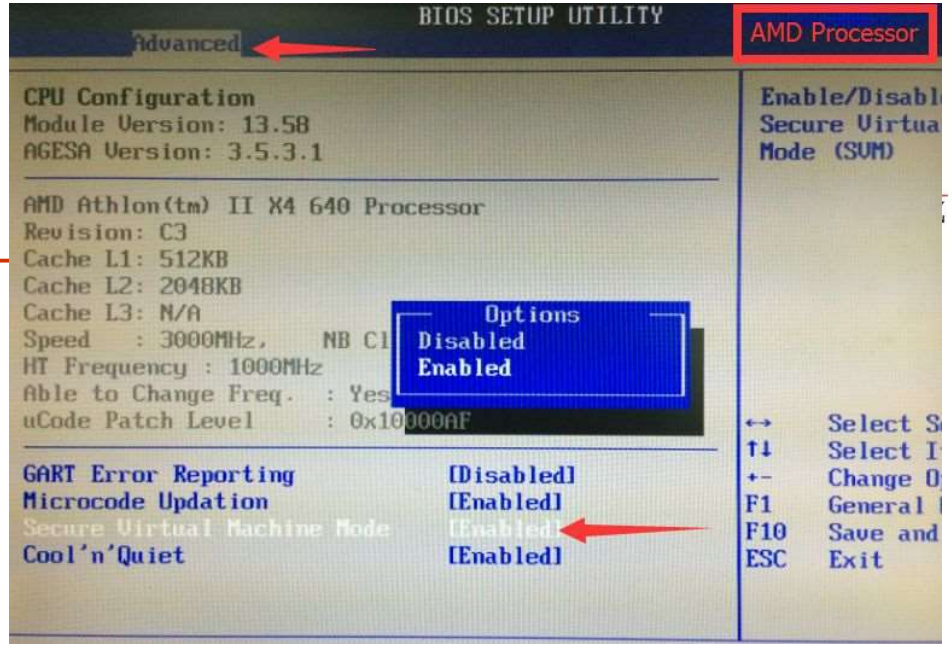




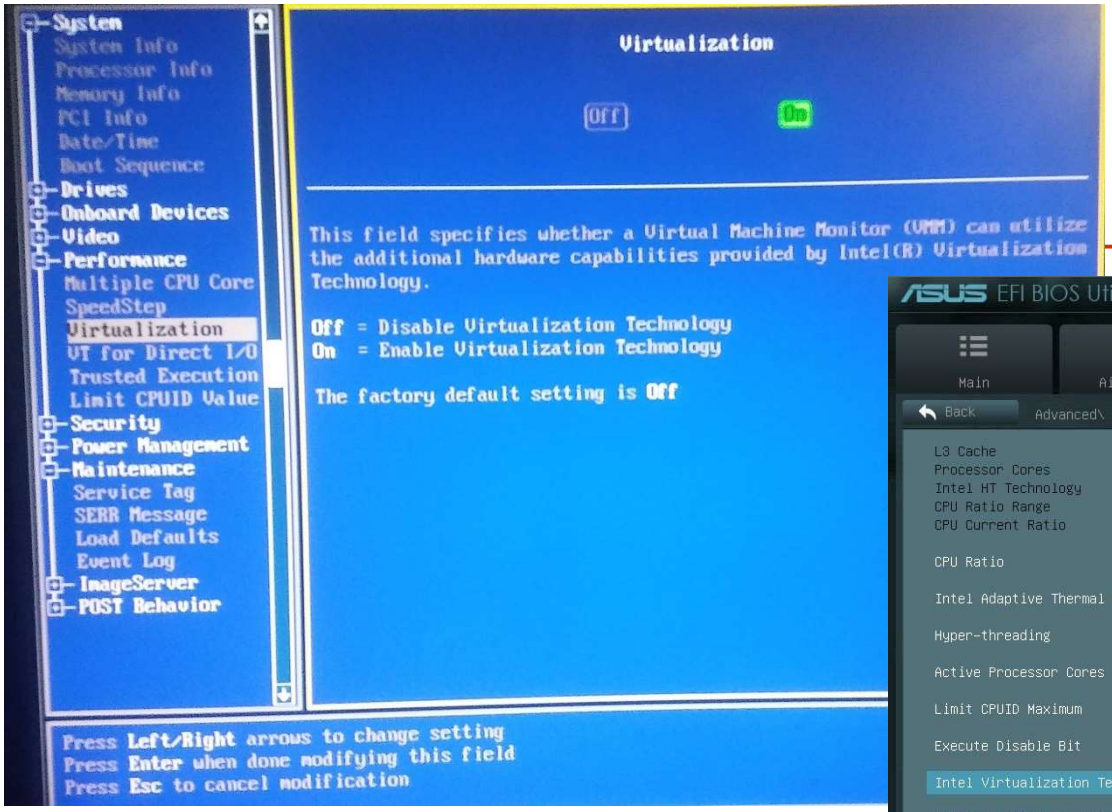


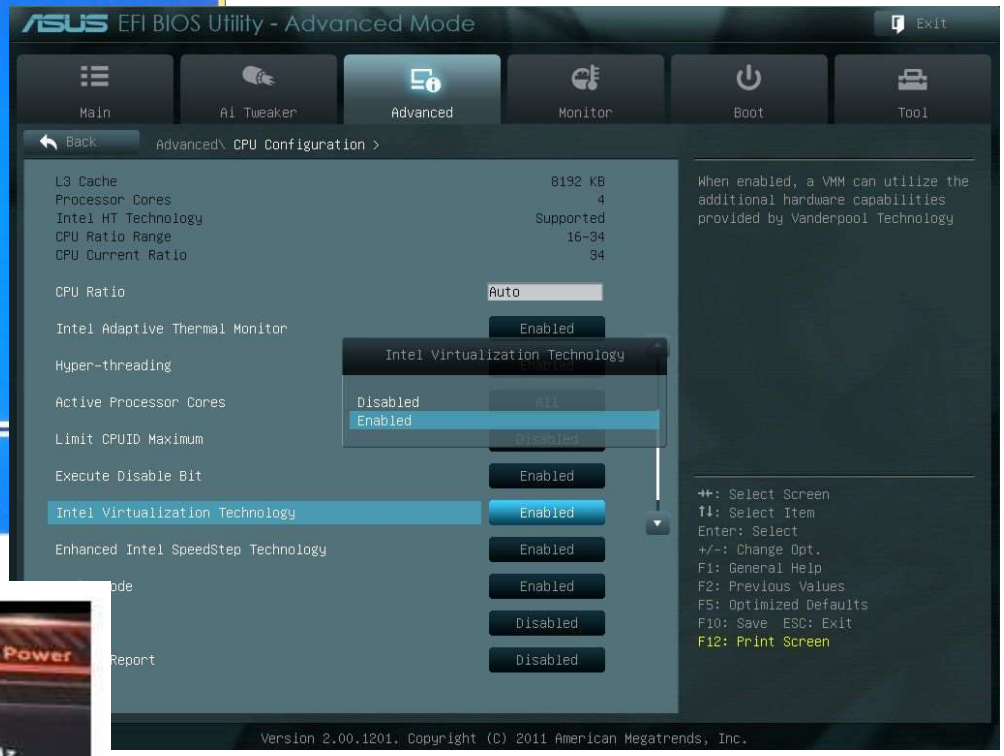






"Virtual Directed I/O" (Intel VT-d/AMD-Vi) is a different thing, the default is OK


System
System Info
Processor Info
Memory Info
PCI Info
Date/Time
Boot Sequence
Drives
Onboard Devices
Video
Performance
Multiple CPU Core
SpeedStep
Virtualization
VT for Direct I/O
Trusted Execution
Limit CPUID Value
Security
Power Management
Maintenance
Service Tag
SERR Message
Load Defaults
Event Log
ImageServer
POST Behavior
Virtualization
Off
On
This field specifies whether a Virtual Machine Monitor (VMM) can utilize the additional hardware capabilities provided by Intel(R) Virtualization Technology.
Off = Disable Virtualization Technology
On = Enable Virtualization Technology
The factory default setting is Off
Press Left/Right arrows to change setting
Press Enter when done modifying this field
Press Esc to cancel modification


ASUS EFI BIOS Utility - Advanced Mode
Exit
Main
Ai Tweaker
Advanced
Monitor
Boot
Tool
Back
Advanced\ CPU Configuration >
L3 Cache 8192 KB
Processor Cores 4
Intel HT Technology Supported
CPU Ratio Range 16-34
CPU Current Ratio 34
CPU Ratio Auto
Intel Adaptive Thermal Monitor Enabled
Hyper-threading
Active Processor Cores All
Limit CPUID Maximum Disabled
Execute Disable Bit Enabled
Intel Virtualization Technology Enabled
Enhanced Intel SpeedStep Technology Enabled
Enabled
Disabled
Disabled
Intel Virtualization Technology
Disabled
Enabled
When enabled, a VMM can utilize the additional hardware capabilities provided by Vanderpool Technology
→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F5: Optimized Defaults
F10: Save ESC: Exit
F12: Print Screen
Version 2.00.1201. Copyright (C) 2011 American Megatrends, Inc.


M.I.T.
System
BIOS
Peripherals
Chipset
Power
CPU Clock Ratio
CPU Frequency
Auto
3.20GHz
Core Performance Boost
AMD Cool&Quiet function
SVM Mode
Global C-state Control
Power Supply Idle Control
Opcache Control
Downcore Control
SMT Mode
Auto
Enabled
Disabled
Auto
Auto
SVM Mode
Disabled
Enabled


Setup Confirmation
Save configuration changes and exit now?
[Yes]
[No]

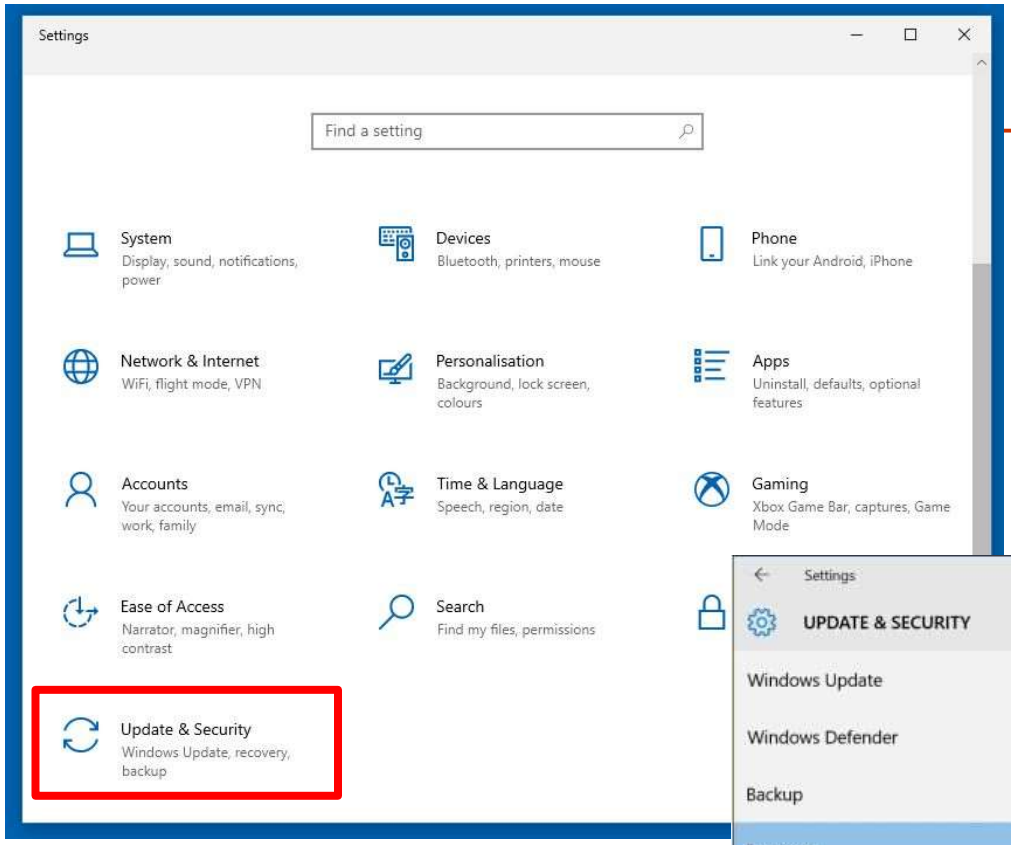
Getting Started: BIOS Settings

BIOS Settings

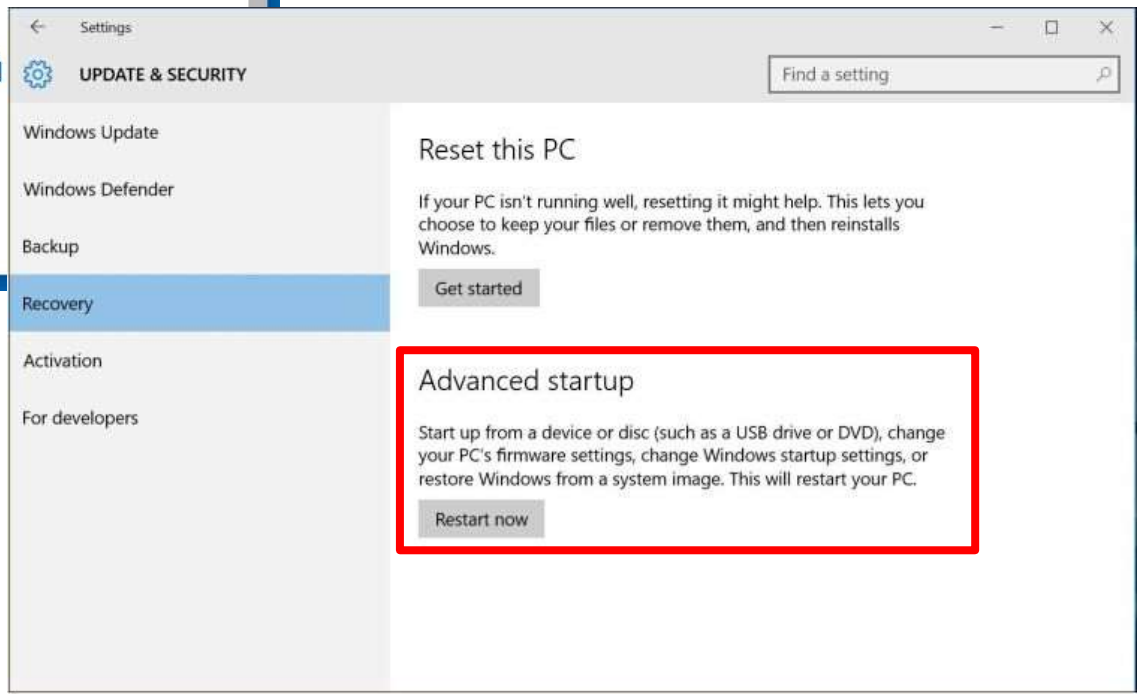
- A full restart from power off is best after saving BIOS changes
- just rebooting or resuming may not do the job.

.

Access the BIOS from Windows

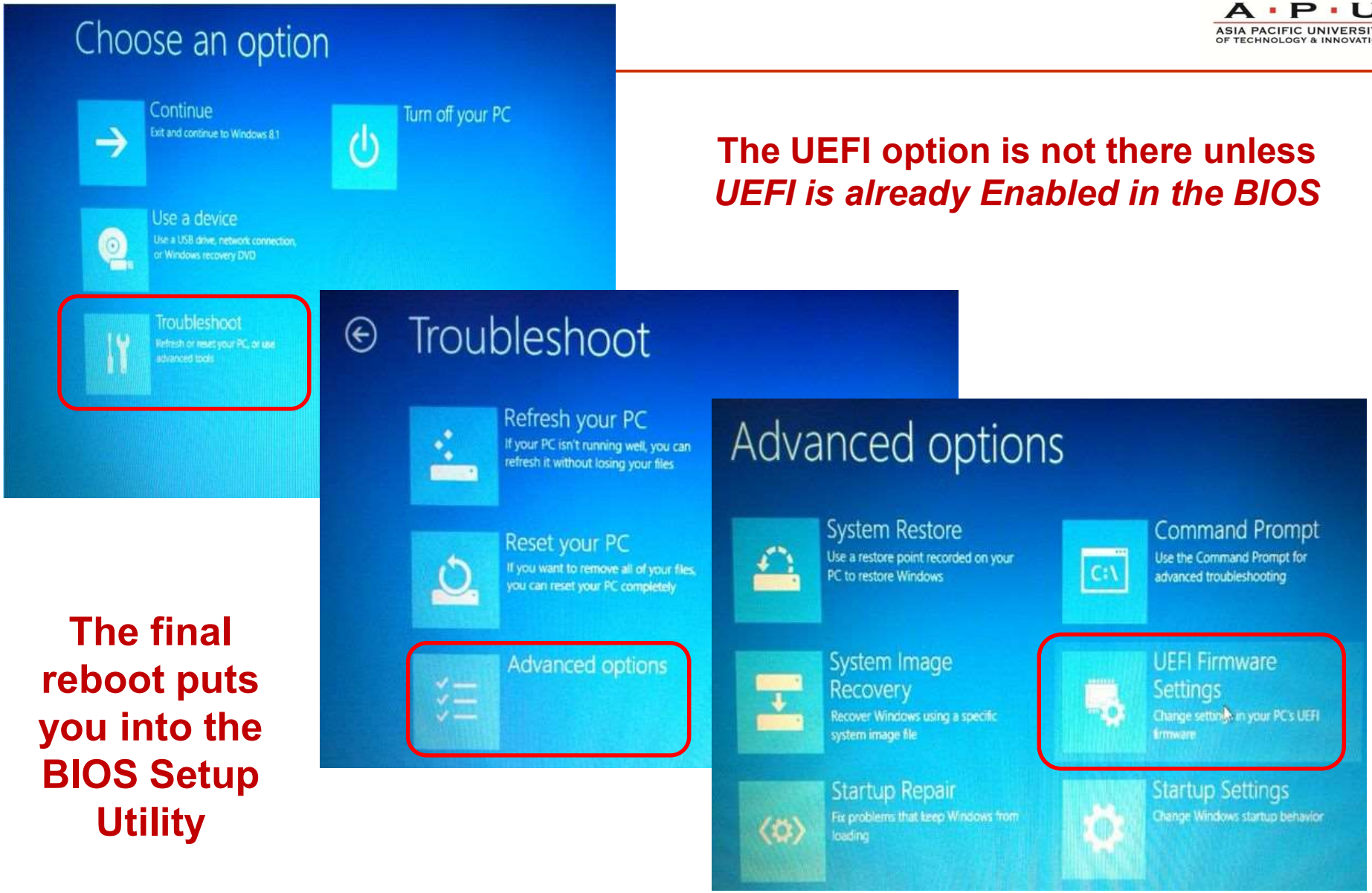


- Start menu
- Settings



Lots of people describe this process but forget to mention that UEFI is a BIOS setting

Access the BIOS from Windows



The UEFI option is not there unless *UEFI is already Enabled in the BIOS*

The final reboot puts you into the BIOS Setup Utility