A+ Core2 Cram Notes

Contents

Disclaimer: CompTIA® A+™ is a registered trademark of CompTIA® organization and duly acknowledged. CertExams.com is neither associated nor affiliated with CompTIA® Organization.

Please email wm@certexams.com for any suggestions or questions

Version 2.0

Disclaimer: CompTIA® A+™ is a registered trademark of CompTIA® organization and duly acknowledged. CertExams.com is neither associated nor affiliated with CompTIA® Organization.

Please email wm@certexams.com for any suggestions or questions

1. Windows Operating Systems

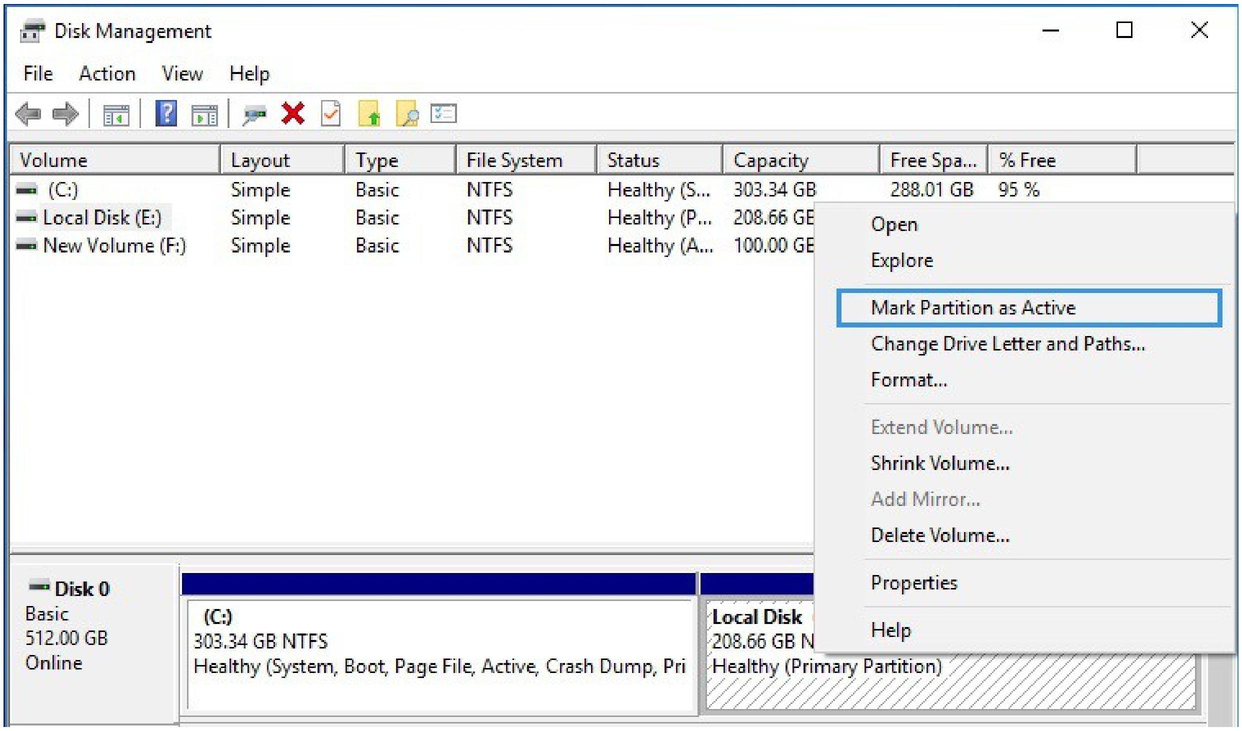
1.1 Installing Windows PC operating systems using appropriate methods

Partitioning: Marking a partition as active on a basic disk means that the computer will use the loader (an operating system tool) on that partition to start the operating system. The primary partition can be made bootable, by marking partition as active. The extended partition can not be marked as active partition.

Steps to mark partition as active in Windows 10

1. Press shortcut key WIN+R to open RUN box, type “diskmgmt.msc”, or Right-click the bottom-left corner (or Start button) on the desktop to open Quick Access Menu, and then choose Disk Management.
2. Right-click on the partition you want to set active, choose Mark partition as active.

The screenshot of “Disk Management” is shown below



Volume	Layout	Type	File System	Status	Capacity	Free Spa...	% Free
(C:)	Simple	Basic	NTFS	Healthy (S...	303.34 GB	288.01 GB	95 %
Local Disk (E:)	Simple	Basic	NTFS	Healthy (P...	208.66 GE		
New Volume (F:)	Simple	Basic	NTFS	Healthy (A...	100.00 GE		

Disk 0
Basic
512.00 GB
Online

(C:)
303.34 GB NTFS
Healthy (System, Boot, Page File, Active, Crash Dump, Pri

Local Disk
208.66 GB N
Healthy (Primary Partition)

__Note__: Do not mark a partition as active if it doesn't contain the loader for an operating system. Doing so will make your computer unbootable

First you need to partition the disk. A hard disk can have one Primary partition and one extended partition. An Extended partition can be divided into one or more logical partitions. After partitioning the hard disk, each partition need to be formatted.

Logical, Extended and primary are the order in which partitions must be deleted

Note: It is not necessary to create the Windows 10 partitions on a new (empty) hard drive or format the partitions before installing Windows 10 as the installer will do that automatically.

If you have two hard disk drives on your computer, a sample of drive letters that could be assigned are as shown below:

Drive 1: C (Primary Partition), E (First logical Drive), F (Second logical Drive)
Drive 2: D (Primary Partition), G(for Logical drive on Extended Partition)

Note: In Windows, drives can be identified by their names (such as "Windows7 OS") and their drive letters (such as "C:"). The important thing to remember is that Windows really only cares about the drive letter. That has to be unique; you can't have two drives labeled E: on the same computer. In Windows 7/8/8.1/10, it is possible to shrink the existing drive (say drive C:) and create a new drive out of the space available by shrinking the existing drive.

A spanned volume is a formatted partition in which data is stored on more than one hard disk drive or solid-state drive, yet appears as a single volume. Unlike RAID, spanned volumes have no fault tolerance, so if any disk fails, the data on the whole volume could be lost.

Types of Installation

When you install a disk in a computer that is running Windows 10, you can choose to select one of two partitioning schemes.

1. **Master Boot Record(MBR):** MBR based partitioning scheme contains the partition table for the disk and a small amount of executable code called the master boot code. MBR is stored on your hard drive but kept outside of Windows partitions and volumes. Crucially, the code in the MBR is run as your computer starts up (before Windows) which makes it an ideal place for a virus or rootkit to hide.

2. **Globally unique identifier (GUID):** GPT - based partitioning scheme is a newer partitioning scheme where each partition contains a Global Unique Identifier (GUID)

A Clean Install is characterized by the following:

1. You can replace an existing Operating System on a partition
2. You can install Windows 7/8/10 on a new partition

3. You can execute the "setup.exe" from the following locations

Telnet Server is a network service. When you install Windows 7/8/8.1/10, the files that make up the Telnet Server service are copied to your computer, however, the telnet service is disabled at first. We can use either “**services.msc**” snap-in or "**net start telnet**" command to start the telnet service at the command prompt. To stop the service, use “**net stop telnet**”.

when you suspect there may be a problem with a Windows 7/8/10 system file. For example, you get a dialog box informing you of a problem with a .dll file, or your program will just not load. It is therefore worth checking to see if there are any corrupt system files using scannow sfc.

To do this, go to the Run box on the Start Menu and type in: **“sfc /scannow”**

This command will immediately initiate the Windows File Protection service to scan all protected files and make sure of their correctness, replacing any files that it finds with a problem.

The following devices require periodic cleaning:

1. Floppy drives
2. Tape drives
3. Printers
4. Mouse

- It is recommended that you clean the LCD screen with clean water, using a soft cotton cloth. Do not spray water directly on the screen. First wet the cloth (no dripping of water), and wipe the LCD screen gently.

- The use of compressed air is most appropriate. Use of vacuum cleaner may tend to create ESD. A nylon brush also creates electrostatic charges. Soap water is not recommended to clean PCAs.

PXE: The process describes how to set up a third-party Preboot Execution Environment (PXE) server. The process includes copying Windows PE 2.0 source files to PXE server and then configuring your PXE server boot configuration to use Windows PE. The best ways to find whether a new hardware is supported by your Windows OS is to check the manufacturer's documentation first, and then the Windows Compatible Products List.

The following are usually hot pluggable devices

a. eSATA
b. USB
c. Expresscard/54

But you need to follow proper procedures if you want to remove a USB or eSATA device while the computer is on. The Personal Computer Memory Card International Association (PCMCIA) developed both the ExpressCard standard and the PC card standards. The host device supports both PCI Express and USB 2.0 connectivity through the ExpressCard slot; cards can be designed to use either mode. The cards are hot-pluggable.

Filesystem Types and Formatting: Microsoft Internet Explorer and Windows Explorer can be used for assigning Share and NTFS permissions on a Windows 7/8/8.1/10 computer. On readable/writable disks, Microsoft Windows 7/8/8.1/10 supports the NTFS file system and two file allocation table (FAT) file systems: FAT16, and FAT32.

Majority of USB flash drives you buy are going to come in one of the two formats: FAT32 or NTFS. The first format, FAT32, is fully compatible with Mac OS X.

FAT32: It works with all versions of Windows, Mac, Linux, game consoles, and practically anything with a USB port. FAT32 allows 4 GB maximum file size, 8 TB maximum partition size.

ExFAT: exFAT was introduced in 2006, and was added to older versions of Windows with updates to Windows XP and Windows Vista.

If you are formatting the device using any modern Windows OS, you will have options to format it using FAT32, exFAT, or NTFS.

Note that FAT (FAT16) has become obsolete due to file size and partition size limitations.

Back

1.2 Features of various Microsoft operating systems

Features of Windows 10

32 bit vs. 64 bit: Windows 10 64-bit supports up to 2 TB of RAM, while Windows 10 32-bit can utilize up to 3.2 GB. The memory address space for 64-bit Windows is much larger, which means, you need twice as much memory than 32-bit Windows to accomplish some of the same 1. Only 64 bit versions of windows 10 can handle over 4GB of RAM

The following table specifies the limits on physical memory for Windows 10.

Version	Limit on X86	Limit on X64

Windows 10 Enterprise	4 GB	2TB
Windows 10 Education	4 GB	2TB
Windows 10 Pro	4 GB	2TB
Windows 10 Home	4 GB	128 GB

As may be seen from the table above, at the minimum, you can install Windows 10 Home that supports up to 128 GB of RAM.

2. Both 32 bit and 64 bit versions of Windows 10 require minimum 1 GHz

If you want to run Windows 10 on your PC, given below are the hardware requirements:

- Processor: 1 gigahertz (GHz) or faster
- RAM: 1 gigabyte (GB) (32-bit) or 2 GB (64-bit)
- Hard disk space: 16 GB for 32 bit OS , 20 GB for 64 bit OS
- Graphics card: Microsoft DirectX 9 graphics device with WDDM driver
- Display: 800x600

3. In Windows 10 we can create multiple profiles and it can be applied to the private and public network. Each connection will use the assigned profile and it will use the rules that are configured in the profiles.

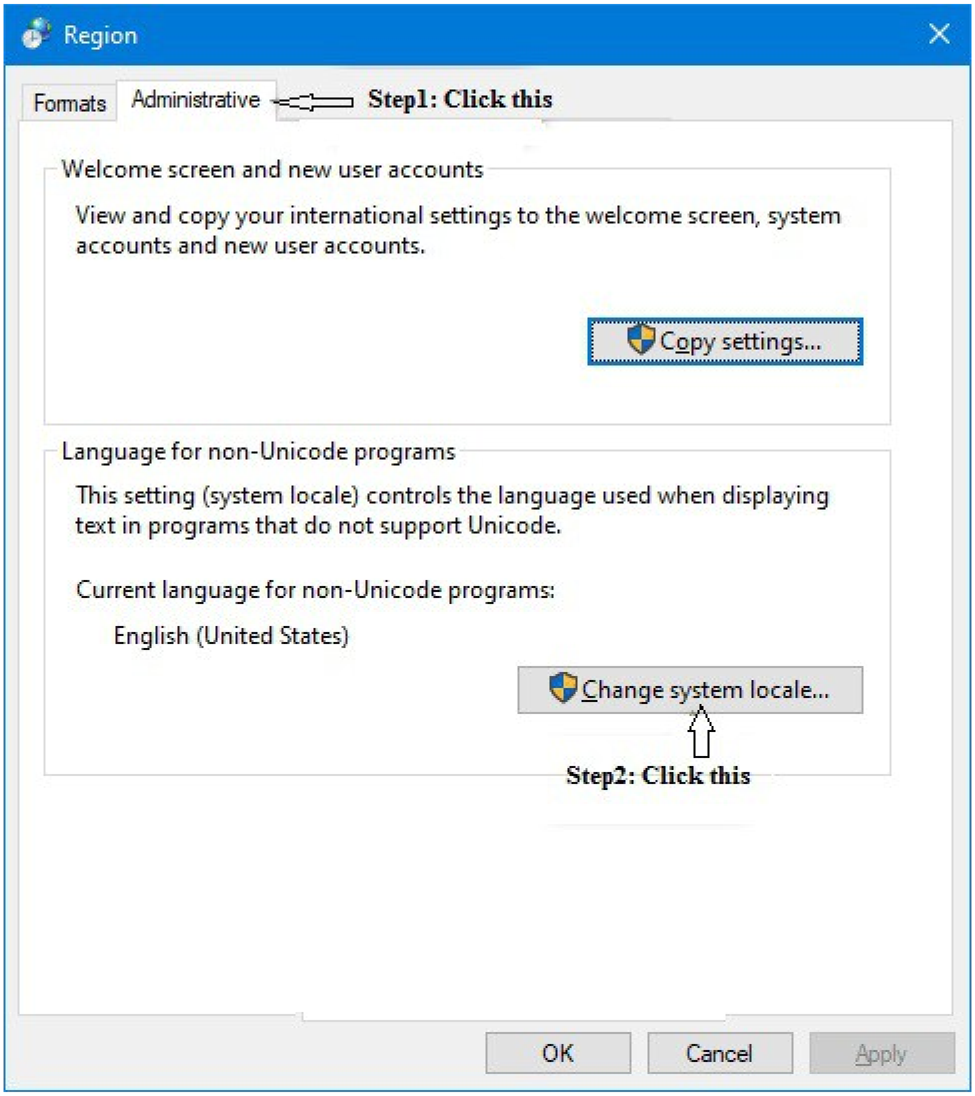
4. You can use Region and Language to support additional languages on your Windows 10 computer. With the support of additional languages, you will be able to edit documents written in those languages. You can also set locale specific to any region using this Option. To use desired Region and Language options, use the steps given below:

View the System Locale settings for Windows

1. Click **Start**, then **Control Panel**
2. Click **Clock, Language and Region**
3. Windows 10, Windows 8: Click **Region**
   Windows 7: Click **Region and Language**
   The Region and Language options dialog appears.
4. Click the **Administrative** tab
   If there is no Advanced tab, then you are not logged in with administrative privileges.
5. Under the **Language for non-Unicode programs** section, click **Change system locale** and select the desired language.

6. Click **OK**
7. Restart the computer to apply the change.

The screenshot of changing System local settings is shown below



Region
Formats
Administrative
Step1: Click this
Welcome screen and new user accounts
View and copy your international settings to the welcome screen, system accounts and new user accounts.
Copy settings...
Language for non-Unicode programs
This setting (system locale) controls the language used when displaying text in programs that do not support Unicode.
Current language for non-Unicode programs:
English (United States)
Change system locale...
Step2: Click this
OK
Cancel
Apply

Notes

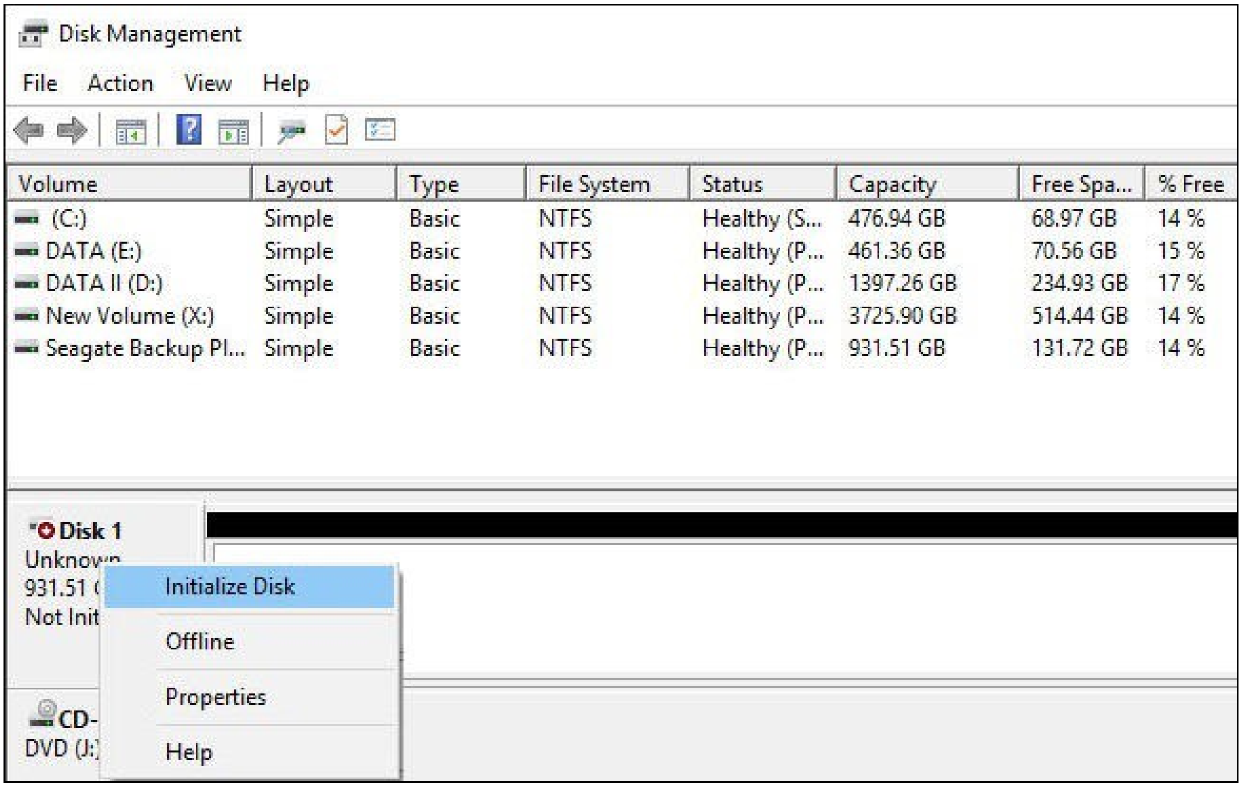
1. You must be logged in with an account that has administrative privileges in order to change the system locale.
2. The appropriate language packs should be installed on the operating system.

Disk partition in windows 10: To create a partition or volume (the two terms are often used interchangeably) on a hard disk, you must be logged in as an administrator, and there must be either unallocated disk space or free space within an extended partition on the hard disk. Open Disk Management and Right-click an unallocated region on your hard disk, and then select New Simple Volume. Then use appropriate options to format the partition.

To initialize a new disk using Disk Management use the steps given below:

1. Open Disk Management with administrator permissions.
2. To do so, in the search box on the taskbar, type **Disk Management**, select and hold (or right-click) **Disk Management**, then select **Run as administrator** > **Yes**. If you can't open it as an administrator, type **Computer Management** instead, and then go to **Storage** > **Disk Management**.
3. In Disk Management, right-click the disk you want to initialize, and then click **Initialize Disk** (shown here). If the disk is listed as Offline, first right-click it and select **Online**.

The screenshot of initializing the disk is shown below.



Volume	Layout	Type	File System	Status	Capacity	Free Spa...	% Free
(C:)	Simple	Basic	NTFS	Healthy (S...	476.94 GB	68.97 GB	14 %
DATA (E:)	Simple	Basic	NTFS	Healthy (P...	461.36 GB	70.56 GB	15 %
DATA II (D:)	Simple	Basic	NTFS	Healthy (P...	1397.26 GB	234.93 GB	17 %
New Volume (X:)	Simple	Basic	NTFS	Healthy (P...	3725.90 GB	514.44 GB	14 %
Seagate Backup Pl...	Simple	Basic	NTFS	Healthy (P...	931.51 GB	131.72 GB	14 %

USB connectivity: To achieve proper USB connectivity six basic system elements must be present and working correctly.

1. Support from the BIOS
2. Support from the Operating System
3. Physical USB ports
4. A USB Device
5. The correct USB cable for the device
6. Drivers either from the OS and/or the peripheral maker

Turn on a USB Port in BIOS:

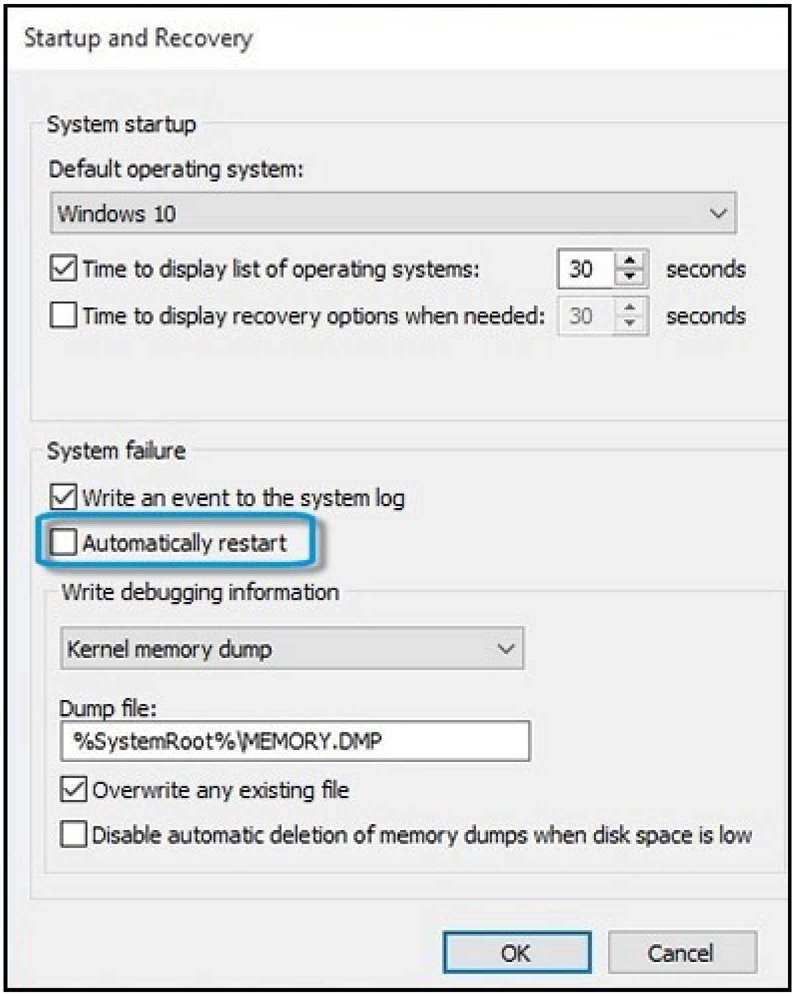
- Check the screen for instructions to boot to setup. Depending on the motherboard, the message might be "BIOS Setup: F8," "Press F8 to Enter BIOS." The keyboard command to enter the BIOS depends on the motherboard.
- Use the arrow key to select "Advanced”, "Onboard Devices" or "Integrated Peripherals" from the menu. Press "Enter."
- Select "USB Controller." Press "+" or "-" to change the setting to "Enabled."
- Press "F10" to save and exit the BIOS.

Automatic restart: The automatic restart option in Windows 10 is enabled by default. Errors might occur but not display with **Automatic restart** enabled. Disable this option to allow the computer to display error messages instead of restarting.

Steps to disable Automatic restart option in windows 10

1. In Windows, search for and open View advanced system settings.
2. Click Settings in the Startup and Recovery section.
3. Remove the check mark next to Automatically restart, and then click OK.
4. Restart the computer.

The screenshot of disabling automatic restart option in windows 10 is shown below


Startup and Recovery

System startup

Default operating system:

Windows 10

☑ Time to display list of operating systems: 30 seconds

□ Time to display recovery options when needed: 30 seconds

System failure

☑ Write an event to the system log

□ Automatically restart

Write debugging information

Kernel memory dump

Dump file:

%SystemRoot%\MEMORY.DMP

☑ Overwrite any existing file

□ Disable automatic deletion of memory dumps when disk space is low

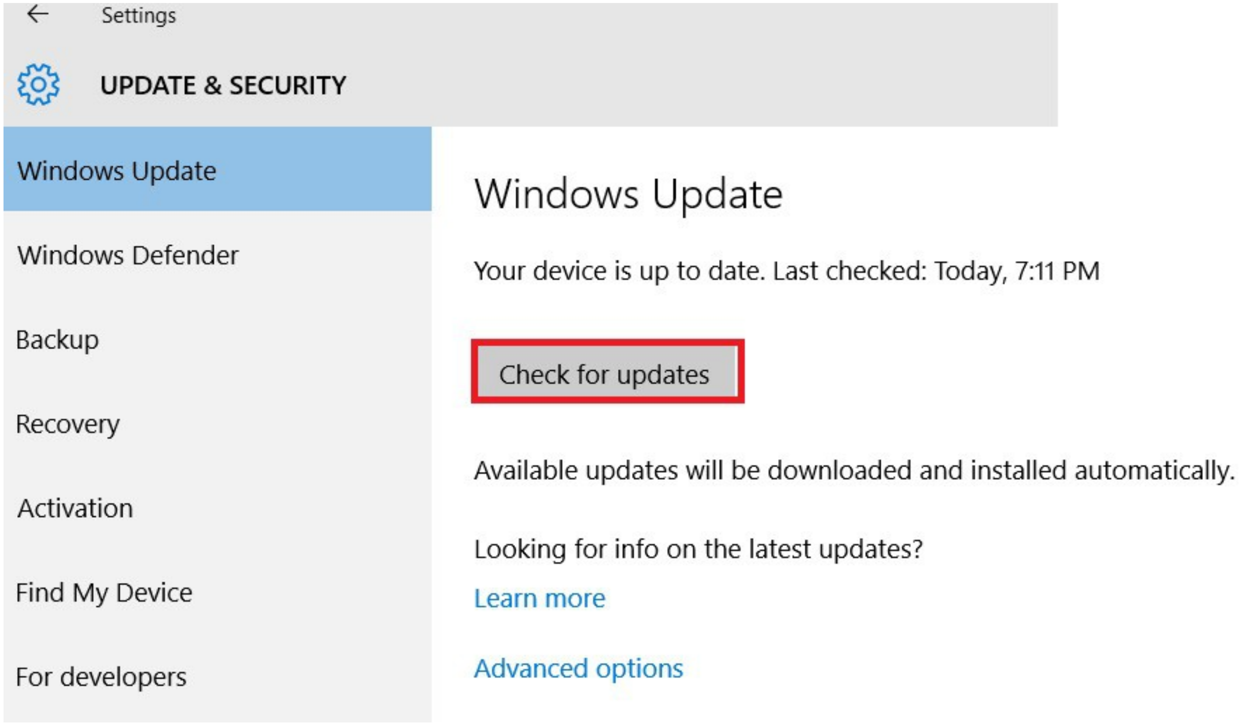
The ability to choose the restart options is very convenient as you can view any error messages and restore failed hardware.

Windows 10 Updates: In Windows 10, Updates are commonly known as "Important", "Required", and "Optional". Important updates are those that relate to security and stability of the Operating System. Required updates are those that relate to added features, etc. Optional updates are the ones that pertain to device drivers, language packs, etc.

1. In Windows 10, updates are mandatory. However, a user may opt to manually update any Windows Updates by selecting appropriate options in the Updates applet.

2. Windows 10 periodically checks for updates. If you want to check manually, select the Start button , then select Settings > Update and security > Windows Update > Check for updates. If Windows Update says that your PC is up to date, then you have all the updates that are currently

available for your PC.



Windows Update

Your device is up to date. Last checked: Today, 7:11 PM

Available updates will be downloaded and installed automatically.

Looking for info on the latest updates?

3. All updates in Windows 10 are automatically downloaded and installed. You cannot selectively update here or disable Windows 10 update. However, there is a way to prevent Windows 10 OS to notify and ask for downloading the updates. If the data connection is marked as "metered" then Windows 10 will not download and install the updates automatically. It will only notify when the updates are available.

The possible upgrade scenarios from one edition of windows 10 to another edition of windows 10 are given below

From Windows 10	Any time Upgrade to Windows 10
Windows 10 Home	Windows 10 Home, Windows 10 Pro,Windows 10 Education, Windows 10 Enterprise
Windows 10 Pro	Windows 10 Pro,Windows 10 Education, Windows 10 Enterprise

Windows 10 Education	Windows 10 Education
Windows 10 Enterprise	Windows 10 Education, Windows 10 Enterprise

Boot options in windows 10: Pressing F8 or the SHIFT + F8 keys on your keyboard to enter Safe Mode, no longer work on windows 10. These methods stopped working because the Windows 10 start procedure became faster than ever before. However, that does not mean that Windows 10 has no Safe Mode. It is just that to get to it you have to follow other procedures. Here are all the ways you can start Windows 10 in Safe Mode:

Steps for starting Safe Mode from the sign-in screen:

1. Restart your computer.
2. On the sign-in screen, select 'Power' > 'Restart' while holding down the Shift key.
3. Your computer will restart again but this time will load an options screen. Select 'Troubleshoot' > 'Advanced options' > 'Startup Settings' > 'Restart'.
4. After Windows 10 restarts one more time, you can choose which boot options you want to be enabled. To get into Safe Mode, you have three different options:

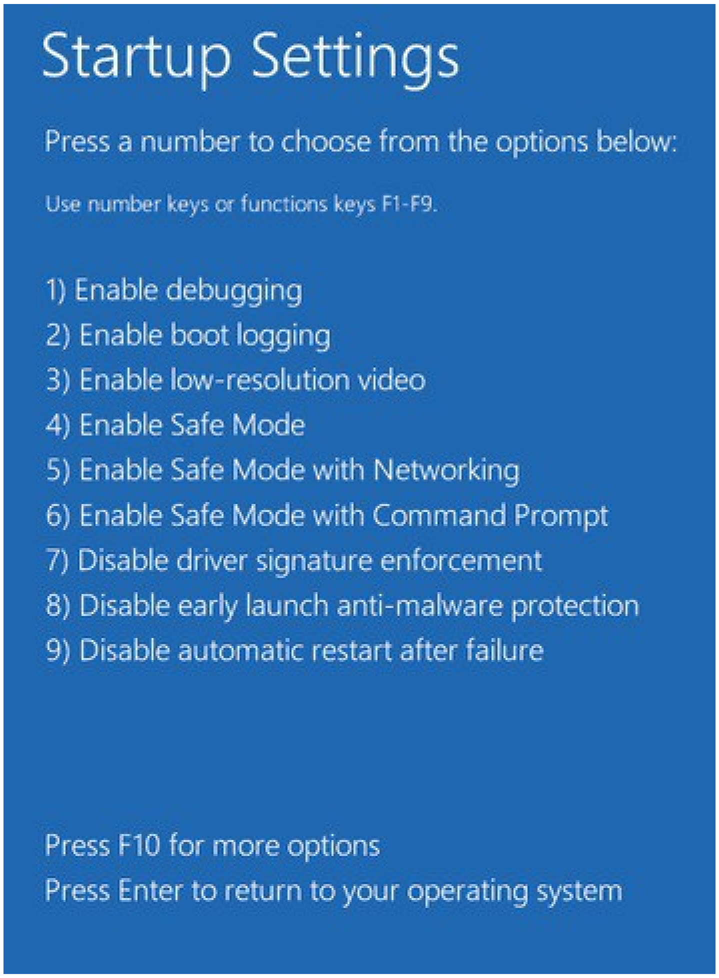
1. Standard Safe Mode - press the 4 or the F4 key on your keyboard to start it
2. Safe Mode with Networking- press 5 or F5
3. Safe Mode with Command Prompt- press either 6 or F6

Log into Windows 10 Safe Mode with a user account that has administrator permissions, and perform the changes you want.

The Advanced Boot Options menu lets you start Windows in advanced troubleshooting modes. The options available are

1. Enable debugging
2. Enable boot logging
3. Enable low-resolution video
4. Enable Safe Mode
5. Enable Safe Mode with Networking
6. Enable Safe Mode with Command Prompt
7. Disable driver signature enforcement
8. Disable early launch anti-malware protection
9. Disable automatic restart after failure

The screenshot of advanced boot option in windows 10 is shown below



Startup Settings

Press a number to choose from the options below:

Use number keys or functions keys F1-F9.

1) Enable debugging
2) Enable boot logging
3) Enable low-resolution video
4) Enable Safe Mode
5) Enable Safe Mode with Networking
6) Enable Safe Mode with Command Prompt
7) Disable driver signature enforcement
8) Disable early launch anti-malware protection
9) Disable automatic restart after failure

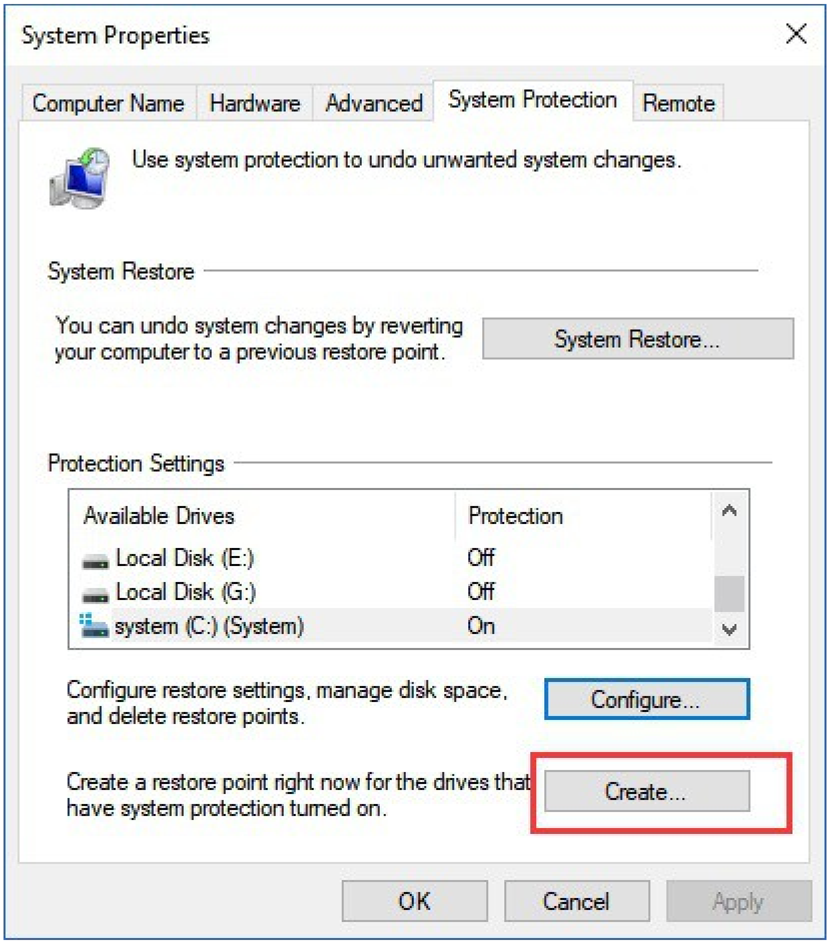
Press F10 for more options

Press Enter to return to your operating system

System Restore in windows 10: If your Microsoft Windows 10 based computer does not start correctly or if it does not start at all, you can use the Windows Recovery Options to help you recover your system software. Backup useful files and documents when you are trying to perform System Restore on your computer.

1. System Restore Tool: System Restore available in the Recovery option in Control Panel in Windows 10. And you won't be able to use it if you haven't turned it on. Here is the path where you can find System Restore tool in Windows 10:

1. Go to Control Panel and click on System and Security.
2. Click System > System protection > Select the drive that you want to create a restore point for and click Create.



Use system protection to undo unwanted system changes.

System Restore

You can undo system changes by reverting your computer to a previous restore point.

Protection Settings

Available Drives	Protection
Local Disk (E:)	Off
Local Disk (G:)	Off
system (C:) (System)	On

Configure restore settings, manage disk space, and delete restore points.

Create a restore point right now for the drives that have system protection turned on.

2. System Repair recovery tool: Startup Repair is a Windows recovery tool that can fix certain system problems that might prevent Windows from starting. Startup Repair scans your PC for the problem and then tries to fix it so your PC can start correctly.

Startup Repair is one of the recovery tools in **Advanced Startup options**. This set of tools is located on your PC's hard disk (recovery partition), **Windows installation media**, and a **recovery drive**.

How to use BitLocker Drive Encryption in windows 10

Windows 10, similar to previous versions, includes BitLocker Drive Encryption, a feature that allows you to use encryption on your PC's hard drive and on removable drives to prevent prying eyes from snooping into your sensitive data.

- BitLocker Drive Encryption is available only on Windows 10 Pro and Windows 10

Enterprise.

- For best results your computer must be equipped with a Trusted Platform Module (TPM) chip. This is a special microchip that enables your device to support advanced security features.
- You can use BitLocker without a TPM chip by using software-based encryption, but it requires some extra steps for additional authentication.
- Your computer's BIOS must support TPM or USB devices during startup. If this isn't the case, you'll need to check your PC manufacturer's support website to get the latest firmware update for your BIOS before trying to set up BitLocker.
- Your PC's hard drive must contain two partitions: a system partition, which contains the necessary files to start Windows, and the partition with the operating system. If your computer doesn't meet the requirements, BitLocker will create them for you. Additionally, the hard drive partitions must be formatted with the NTFS file system.
- The process to encrypt an entire hard drive isn't difficult, but it's time-consuming. Depending the amount of data and size of the drive, it can take a very long time.
- Make sure to keep your computer connected to an uninterrupted power supply throughout the entire process.

Some of the windows 10 features

- One of the standout new features found in Windows 10 is the addition of Cortana. For those unfamiliar, Cortana is a voice-activated personal assistant. You can use it to get weather forecasts, set reminders,send email, find files, search the Internet and so on.
- For privacy issues, Windows 10 Education does not include Cortana, since this edition is used for academic organizations. Windows 10 Home, Pro, and Enterprise all contain Cortana.
- With the launch of Windows 10 comes Edge , Microsoft's new built-in browser that's meant to replace Internet Explorer. Microsoft Edge is the default browser for all Windows 10 devices. It’s built to be highly compatible with the modern web. For some enterprise web apps and a small set of sites that were built to work with older technologies like ActiveX, you can use Enterprise Mode to automatically send users to Internet Explorer 11.
- Deployment Image & Servicing Management or commonly you know as DISM is the tool which settles down component store falsification. However, this utility is also capable of rectifying and handling Windows image. In addition, it can also manage Windows Recovery Environment, Windows Setup and Windows PE.

- In Windows 10, you can enable wake on authentication. If you don't want to sign back, you can turn it off. When turned off, when the PC wakes up from Sleep mode, it won't prompt for password. If you use your PC in public places, it is recommended to turn on wake-up authentication to avoid unscrupulous people accessing your computer.

Back

1.3 Microsoft command line tools

1.4 Microsoft operating system features and tools

1.5 Important Windows Control Panel utilities

1.6 Configure Windows networking on a client/desktop

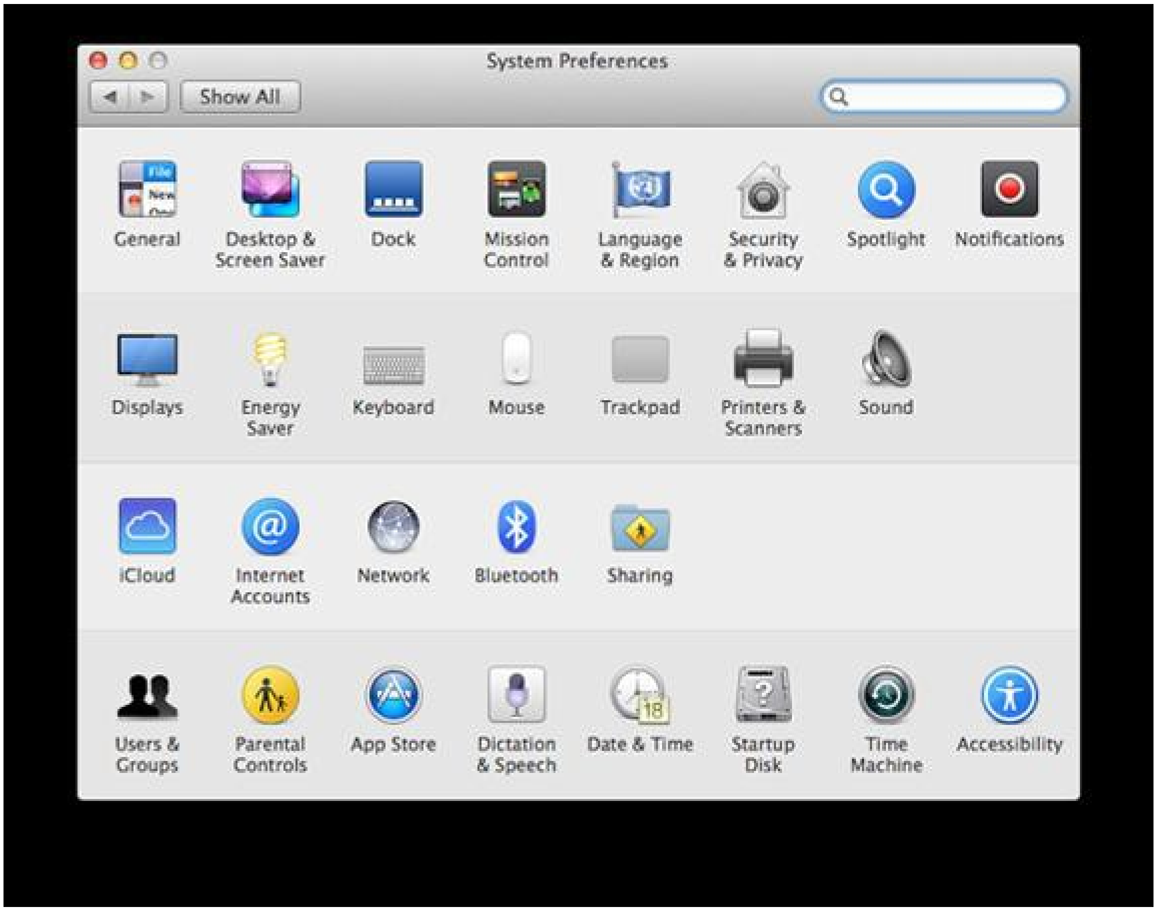
1.7 Common preventive maintenance procedures using the appropriate OS tools.

2. Other Operating Systems & Technologies

2.1 Important features, and functionality of the Mac OS and Linux operating systems

You can access the update in Mac OS X computer in the following way

System Preferences controls system-wide settings ("global" settings), and is available from the Apple menu at the upper-left corner of the screen. System Preferences lets you adjust things like your screen resolution, keyboard control, mouse control, sound, printer settings, sharing settings, accounts, and more. The figure below shows the applets that are available in System Preferences window.



You can quickly locate the settings you want to change by typing the desired subject in the search field. For example, to change your login password, type "password." The preferences related to password appear below the search field, and one or more preferences are spotlighted in the System Preferences window.

In OS X, you can run a background job on a timed schedule in two ways: launchd jobs and cron jobs. The preferred way to add a timed job is to use launchd. Each launchd job is described by a separate file. This means that you can manage launchd timed jobs by simply adding or removing a file. Although it is still supported, cron is not a recommended solution. It has been deprecated in favor of launchd.
Task scheduler is a Windows tool and not to be confused with Apple Mac or Ubuntu Linux. Similarly, Software Updater is a Ubuntu Linux graphical tool to check for updates, etc.

The following are true about MAC OS X

1. You can manage Startup Applications from System preferences > Users and Groups pane in MAC OS X
2. You can use Task Manager in Windows 7 for managing Startup Applications

3. In Ubuntu Linux, you can search for Startup by clicking on the Search button (top left), and initiate configuring Startup applications by clicking on the Startup applications.
4. Mac OS X allows user level configuration of Startup Applications
5. You can configure Startup Applications in Windows 8/8.1 using Task Manager (Ctrl+Alt+Del).
6. In Windows 7/Vista, you use msconfig command. You may use it in command prompt or go to Start > Search bar, and type msconfig and enter.

Removal and restoration of an app from a MAC OS X computer

Install apps

- To install apps from a disc, insert the disc into your computer's optical drive (or an optical drive connected to your computer).

- To install apps downloaded from the Internet, double-click the disk image or package file (looks like an open box). If the provided installer doesn't open automatically, open it, then follow the onscreen instructions.

Update apps

To manually check for app updates, choose Apple menu > App Store, then click Updates.

Uninstall apps

- You can uninstall apps you got from the Mac App Store, from other websites, or from discs. You can't uninstall apps that are part of OS X, such as Safari and Mail.

- Apps downloaded from the Mac App Store: Click the Launchpad icon in the Dock, hold down an app's icon until all the icons begin to jiggle, then click an app's delete button . If you later want the app, you can reinstall it from the Mac App Store.

- If an icon doesn't have a delete button, it can't be uninstalled in Launchpad.

- Apps that have an uninstaller: In the Finder sidebar, click Applications. If an app is inside a folder, it might have an Uninstaller. Open the app's folder. If you see Uninstall [App] or [App] Uninstaller, double-click it and follow the onscreen instructions.

- Apps that don't have an uninstaller: In the Finder sidebar, click Applications. Drag the app from the Applications folder to the Trash (located at the end of the Dock), then choose Finder > Empty Trash.

- If you change your mind, before emptying the Trash, select the app in the Trash, then choose File > Put Back.

- The Dock is located at the bottom of your screen by default. It's a convenient place to keep items you use frequently. You can add or remove apps and documents, make it larger or smaller, move it to the left or right side of your screen, or even set it to hide when you're not using it.

- To add an item to the Dock, just drag the item and drop it where you want it. Place apps to the left of the line in the Dock, and documents to the right.

- To remove an item, just drag it out of the Dock. Removing an item from the Dock doesn't remove it from your Mac.

The command line option checks for update in Ubuntu Linux for all the packages currently installed is

Sudo: The one command to rule them all. It stands for super user do Pronounced like sue doug. As a Linux system administrator or power user, it's one of the most important commands in your arsenal.

sudo apt-get: Update is used to install the newest versions of all packages currently installed on the system
sudo reboot: It is used to reboot the Ubuntu Linux operating system.
Sudo l: It is simply lists the current directory files and folders.

There is no "get updates" command in Ubuntu.

Tools commonly used for downloading and installing any updates to device drivers on a Linux Ubuntu computer

Mac OS X will notify about available system updates including any device driver updates. You can visit the app store and update the software.
Ubuntu Linux also notifies about available software updates. You can visit Software Updater to download and install available updates, including device driver software updates.
Device Manager is commonly used on Windows 7 to update any system components such as driver updates. It also allows you install a driver, or disable/enable a device.

MacBookPro comes natively with MiniDisplayPort. You need to buy MiniDisplayPort to DVI adapter separately. You may also need to update the software drivers, if necessary.
The Mini DisplayPort (MiniDP or mDP) is a miniaturized version of the DisplayPort audio-visual digital interface. It was announced by Apple in October 2008. As of 2013, all new Apple Macintosh computers had the port.

Prefered File system used in MAC computer running Osx:

- HFS: HFS (Hierarchical File System) was the primary filesystem format used on the Macintosh Plus and later models, until Mac OS 8.1, when HFS was replaced by HFS Plus.

- HFS+: HFS+ is the preferred file system on Mac OS X. HFS+ is architecturally similar to HFS, with several important improvements such as:

1. 32 bits used for allocation blocks (instead of 16). HFS divides the disk space on a partition into equal-sized allocation-blocks. Since 16 bits are used to refer to an allocation-block, there can be at most 216 allocation blocks on an HFS file system. Thus, using 32 bits for identifying allocation blocks results in much less wasted space (and more files).
2. Long file names up to 255 characters
3. Unicode based file name encoding
4. File/Directory attributes can be extended in future (as opposed to being fixed size)
5. In addition to a System Folder ID (for starting Apple operating systems), a dedicated startup file that can easily be found (its location and size are stored in the volume header in a fixed location) during startup, is also supported so that non-Apple systems can boot from a HFS+ filesystem
6. Largest file size is 263 bytes

Ubuntu's default file system is ext4, since 9.10. Ext4 is an evolution of ext3, which was the default file system before. Ext4 is often noticeably faster than Ext3 even for ordinary desktop use.

Given below is a very brief comparison of the most common file systems in use with the Linux world.

File System	Max File Size	Max Partition Size	Notes
Fat16	2 GiB	2 GiB	Legacy
Fat32	4 GiB	8 TiB	Legacy
NTFS	2 TiB	256 TiB	For Windows Compatibility
ext2	2 TiB	32 TiB	Legacy

ext3	2 TiB	32 TiB	Standard linux filesystem for many years until Ubuntu 8
ext4	16 TiB	1 EiB	Modern iteration of ext3. Default file system in Ubuntu 9, 10
XFS	8 EiB	8 EiB	Created by SGI.

A Linux system, just like UNIX, makes no difference between a file and a directory, since a directory is just a file containing names of other files. Programs, services, texts, images, and so forth, are all files. Input and output devices, and generally all devices, are considered to be files, according to the system.
In Linux environment, the following files have special meaning:

1. **Directories:** Files that are lists of other files.
2. **Special files**: the mechanism used for input and output. Most special files are in /dev, we will discuss them later.
3. **Links:** A system to make a file or directory visible in multiple parts of the system's file tree. We will talk about links in detail.
4. **(Domain) sockets**: a special file type, similar to TCP/IP sockets, providing inter-process networking protected by the file system's access control.
5. **Named pipes**: Act more or less like sockets and form a way for processes to communicate with each other.

Iwconfig/ifconfig: A Linux system, just like UNIX, makes no difference between a file and a directory, since a directory is just a file containing names of other files. Programs, services, texts, images, and so forth, are all files. Input and output devices, and generally all devices, are considered to be files, according to the system.

In Linux environment, the following files have special meaning:

1. Directories: files that are lists of other files.
2. Special files: the mechanism used for input and output. Most special files are in /dev, we will discuss them later.
3. Links: a system to make a file or directory visible in multiple parts of the system's file tree. We will talk about links in detail.
4. Domain sockets: a special file type, similar to TCP/IP sockets, providing inter-process networking protected by the file system's access control.
5. Named pipes: act more or less like sockets and form a way for processes to

communicate with each other.

Some important Linux commands are given below. Try them on the Linux machine to get acquainted.

clear: Removes all previous commands and output from consoles and terminal windows. (DOS: cls)

cp: Copies files and directories.

df: Reports the amount of space used and available on currently mounted filesystems.

du: Shows the sizes of directories and files.

grep: Searches text.

hostname: Shows or sets a computer's host name and domain name.

kill: Terminates stalled processes without having to log out or reboot.

killall: Terminates all processes associated with programs whose names are provided to it as arguments.

man: Formats and displays the built-in manual pages.

mkbootdisk: Creates an emergency boot floppy.

mkdir: Creates new directories.

mkfs: Creates a filesystem on a disk or on a partition thereof.

mv: Renames and moves files and directories.

ps: (short for process status) Lists the currently running processes and their process identification numbers (PIDs).

Passwd: Use the passwd command to change user password.

pwd: (short for present working directory) Displays the full path to the current directory.

reboot: Restarts a computer without having to turn the power off and back on.

rm: Deletes the specified files and directories.

rmdir: Deletes the specified empty directories.

runlevel: Reports the current and previous runlevels.

shred: destroys files.

spell: checks spelling.

strings: returns each string of printable characters in files.

su: (short for substitute user) changes a login session's owner without the owner having to first log out of that session.

Tar: converts a group of files into an archive.

touch: the easiest way to create new, empty files.

uname: provides basic information about a system's software and hardware.

uptime: shows the current time, how long the system has been running since it was booted up, how many user sessions are currently open and the load averages.

w: shows who is logged into the system and what they are doing.
wc: by default counts the number of lines, words and characters that are contained in text.

whatis: provides very brief descriptions of command line programs and other topics related to Unix-like operating systems.

whoami: returns the user name of the owner of the current login session.

Back

2.2 Set up and use client-side virtualization

2.3 Basic Cloud Concepts

2.4 Basic features of mobile operating systems

2.5 Configure basic mobile device network connectivity and email.

3. Security

3.1 Common security threats

1. **Boot Sector virus**: A boot sector virus stays resident by infecting the boot sector of the computer

2. **MBR Virus:** A Master boot record (MBR) virus infect the first physical sector of all affected disks

3. File viruses either replace or attach themselves to executable files, and most commonly found virus

4. Macro virus attaches itself to documents in the form of macros.

5. Memory viruses are viruses that execute and stay resident in memory. Trojan Horse is an example of memory virus.

6. **Trojan Horse:** A trojon is not a virus. The principal of variation between a Trojan horse, or Trojan, and a virus is that Trojans don't spread themselves. Trojan horses disguise themselves as valuable and useful software available for download on the internet. Trojan may work as a client software on your computer communicating with the Trojan server over the Internet.

7. **Social Engineering:** Social engineering is a skill that an attacker uses to trick an innocent person such as an employee of a company into doing a favor. For example, the attacker may hold packages with both the hands and request a person with appropriate permission to enter a building to open the door. Social Engineering is considered to be the most successful tool that hackers use.

8. **Script file virus:** Note that script files may include viruses hidden inside. Therefore, it is not wise to open any script file attachments such as file.scr or file.bat etc.

9. **Malware:** Malware includes computer viruses, worms, trojan horses, spyware, dishonest adware, and other malicious and unwanted software.

10. **Browser Hijacker:** A browser hijacker is a form of malware, spyware or virus that replaces the existing internet browser home page, error page, or search page with its own. These are generally used to force hits to a particular website.

Social Engineering involves following threats

1. **Shoulder surfing**: shoulder surfing refers to using direct observation techniques, such as looking over someone's shoulder, to get information. It is commonly used to obtain passwords, PINs, security codes, and similar data. Shoulder surfing is particularly effective in crowded places because it is relatively easy to observe someone as they fill out a form, enter their PIN at an automated teller machine or a POS terminal, or enter a password at a cybercafe, public and university libraries, or airport kiosks. Shoulder surfing can also be done at a distance using binoculars or other vision-enhancing devices. Inexpensive, miniature closed-circuit television cameras can be concealed in ceilings, walls or fixtures to observe data entry. To prevent shoulder surfing, it is advised to shield paperwork or the keypad from view by using one's body or cupping one's hand.

2. Phishing phone calls: Cybercriminals might call you on the phone and offer to help solve your computer problems or sell you a software license. Neither Microsoft nor our partners make unsolicited phone calls (also known as cold calls) to charge you for computer security or software fixes.

3. Social Engineering: Social Engineering threats involve gaining trust of an employee or an insider of an organization. Once they've gained your trust, cybercriminals might ask for your username and password or ask you to go to a website to install software that will let them access your computer to fix it. Once you do this, your computer and your personal information is vulnerable. You may reduce the threat due to social engineering by treating all unsolicited phone calls with skepticism and not providing any personal information on such calls.

Some of the common attacks

Zero day attack: A Zero day attack is an exploit of an operating system or software vulnerability that is unknown to and unpatched by the author of the product. The name comes from the fact that there is no warning of the attack and this is compounded by the fact that the attack will be successful until it is discovered and patched by the vendor. It does not take long for a zero day attack to be effective considering the time it takes to program a patch and get it distributed to the public. These attacks can take place between the time they are discovered and when the patch is issued.

Zombie/botnet: When discussing a Zombie and its relationship to a botnet, think of an army of zombies. With your PC as one of the potentially millions of PCs infected with the same malware and commandeered by a single host. The entity that controls the botnet can literally use the machines for a single purpose like a DDoS, Spam or malware distribution. Hundreds of billions of dollars in losses or damage can be attributed to botnets.

Brute forcing: Brute forcing (Brute Force Cracking) can be best described as cracking a username, password, or even a Wi-Fi encryption protocol or decryption key by using trial, error and result evaluation using a pre-defined set of values for the attack. Use long and complex passwords to defend against this attack.

Dictionary attacks: Dictionary attacks are a form of brute force attack that uses words found in the dictionary to attempt to discover passwords and decryption keys. Here you need to avoid words found in the dictionary for your security. It is helpful to use a mix of upper and lower case letters along with numbers and special characters (!@#$%).

Tailgating attack: Another social engineering attack type is known as tailgating or "piggybacking." These types of attacks involve someone who lacks the proper authentication following an employee into a restricted area. In a common type of tailgating attack, a person impersonates a delivery driver and waits outside a building. When an employee gains security's approval and opens their door, the attacker asks that the employee hold the door, thereby gaining access off of someone who is authorized to enter the company. Tailgating does not work in all corporate settings, such as in larger companies where all persons entering a building are required to swipe a card. However, in mid-size enterprises, attackers can strike up conversations with employees and use this show of familiarity to successfully get past the front desk.

Back

3.2 Common Prevention methods

3.3 Basic Windows OS security settings

3.4 Securing wireless and wired network

3.5 Implementing methods for securing mobile devices

Back

4. Software troubleshooting

4.1 Troubleshoot PC operating system problems with appropriate tools

- Windows RE (Short for Recovery) is new for Windows 7/8/10 and completely replaces the recovery console in Windows XP. You should be able to perform most tasks of recovery console from Windows RE.
  Windows RE (Recovery Environment) is stored as ***winre. wim*** file on device hard drive or SSD in Windows 7, 8/8.1 and 10. Windows 7 normally keeps it on the same partition/volume with Windows, while Windows 8 and later usually keep it on the hidden System Reserved partition that also contains boot files and Boot Configuration Data (BCD).

- Microsoft recommends that you regularly create Automated System Recovery (ASR) sets as part of an overall plan for system recovery so that you are prepared if the system fails. ASR should be a last resort for system recovery. Use ASR only after you have exhausted other options. For example, you should first try Safe Mode Boot and Last Known Good.

- A hard disk should never be low level formatted at the customer premises. It is highly recommended that it is done at the manufacturer's or at any authorized center.

- To get into the Windows 7 Safe Mode, as the computer is booting press and hold your "F8 Key" which should bring up the "Windows Advanced Options Menu". Use the arrow keys to move to "Safe Mode" and press Enter key.

- There are two main ways to boot your computer in Windows 10 Safe Mode. If your computer loads the sign-in screen, you can boot Windows 10 in Safe Mode from startup. If you only get a blank screen when you open up your computer, you can try the instructions to booting to Safe Mode from a blank screen.

Steps for starting Safe Mode from the sign-in screen:

1. Restart your computer.
2. On the sign-in screen, select 'Power' > 'Restart' while holding down the Shift key.

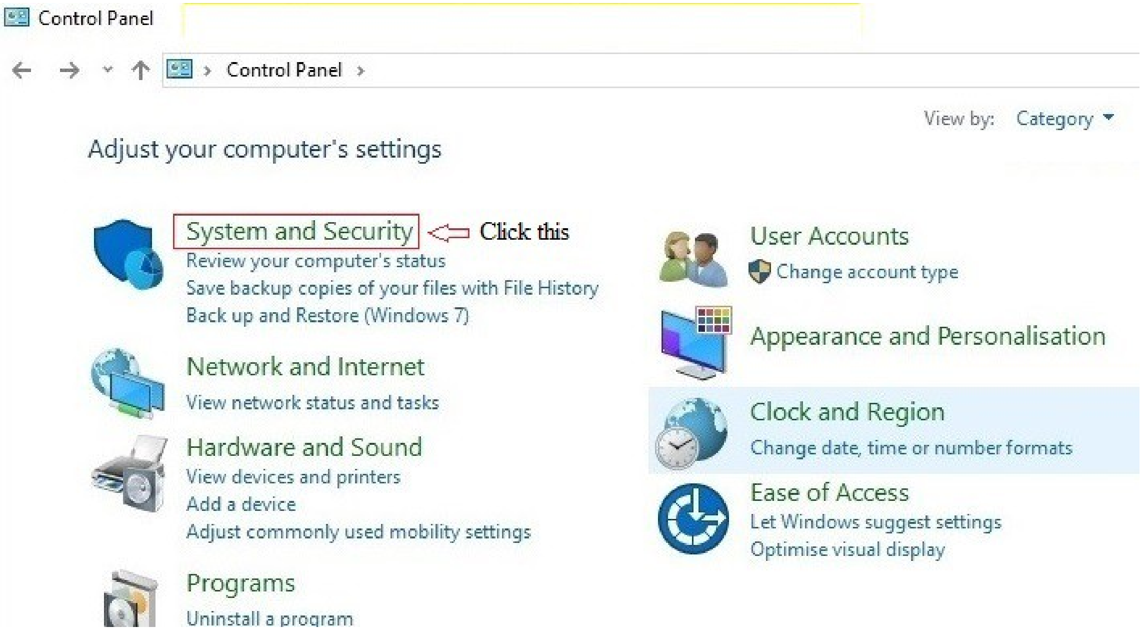
Steps for starting Safe Mode from a blank screen:

1. Hold down the Windows logo key (normally between CTRL + ALT on your keyboard) at the same time as pressing Ctrl, Shift + B. If you're running Windows 10 on a tablet, you'll need to press the increase volume and decrease volume buttons together three times within a two-second period.
2. You should see the screen dim or flutter and hear a beep, which means that Windows is trying to refresh.

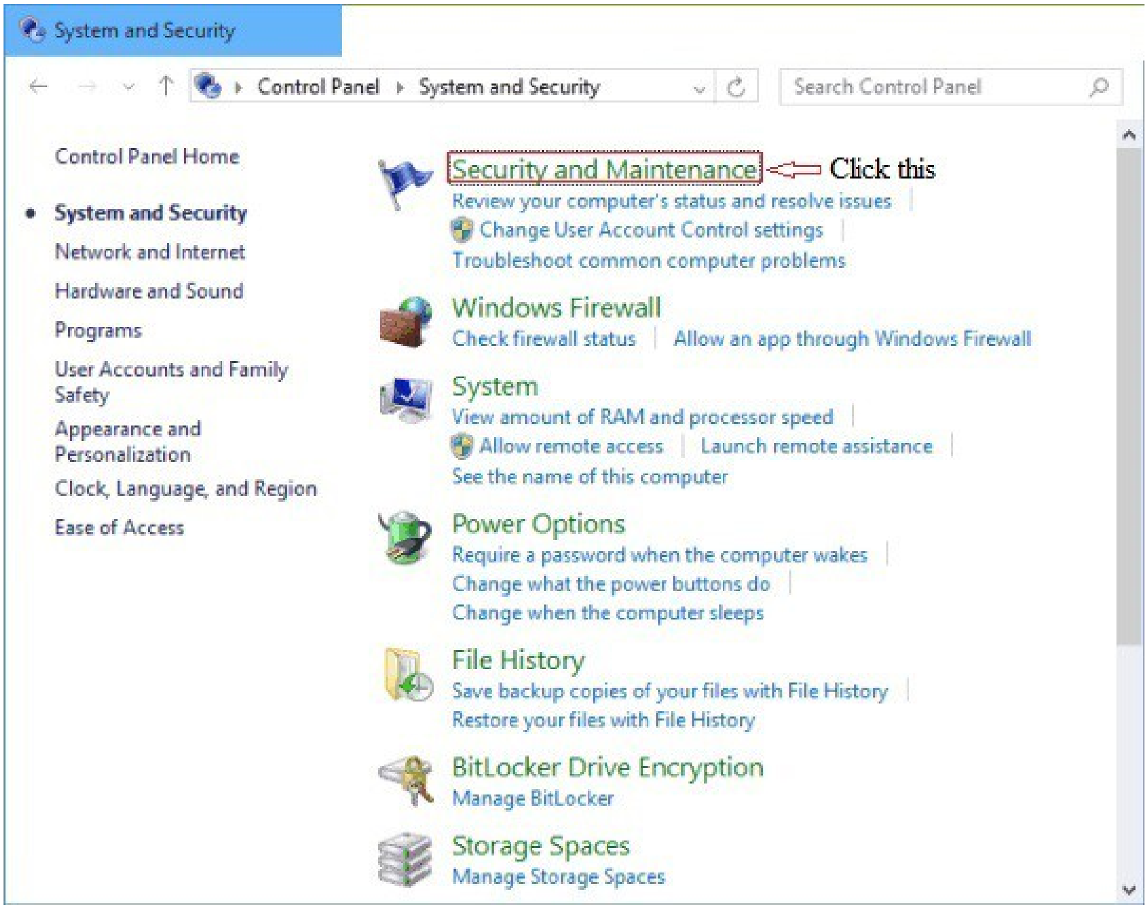
- Since Windows 7/8/10, Microsoft added a new security feature called User Account Control (UAC). It tries to prevent malicious apps from doing potentially harmful things on your PC. Before the administrator-level (elevated) action is allowed, UAC asks permission from the user to go ahead with it, or cancel the request.

To change UAC settings in windows 10

1. In the control panel window click **"System and Security"**


Control Panel
Control Panel >
View by: Category
Adjust your computer's settings
System and Security
Click this
Review your computer's status
Save backup copies of your files with File History
Back up and Restore (Windows 7)
Network and Internet
View network status and tasks
Hardware and Sound
View devices and printers
Add a device
Adjust commonly used mobility settings
Programs
Uninstall a program
User Accounts
Change account type
Appearance and Personalisation
Clock and Region
Change date, time or number formats
Ease of Access
Let Windows suggest settings
Optimise visual display

2. Under System and Security window click **"Security and Maintenance"**



System and Security

Control Panel ▸ System and Security

Search Control Panel

Control Panel Home

- **System and Security**

Network and Internet

Hardware and Sound

Programs

User Accounts and Family Safety

Appearance and Personalization

Clock, Language, and Region

Ease of Access

Security and Maintenance ⇐ Click this

Review your computer's status and resolve issues | Change User Account Control settings | Troubleshoot common computer problems

Windows Firewall

Check firewall status | Allow an app through Windows Firewall

System

View amount of RAM and processor speed | Allow remote access | Launch remote assistance | See the name of this computer

Power Options

Require a password when the computer wakes | Change what the power buttons do | Change when the computer sleeps

File History

Save backup copies of your files with File History | Restore your files with File History

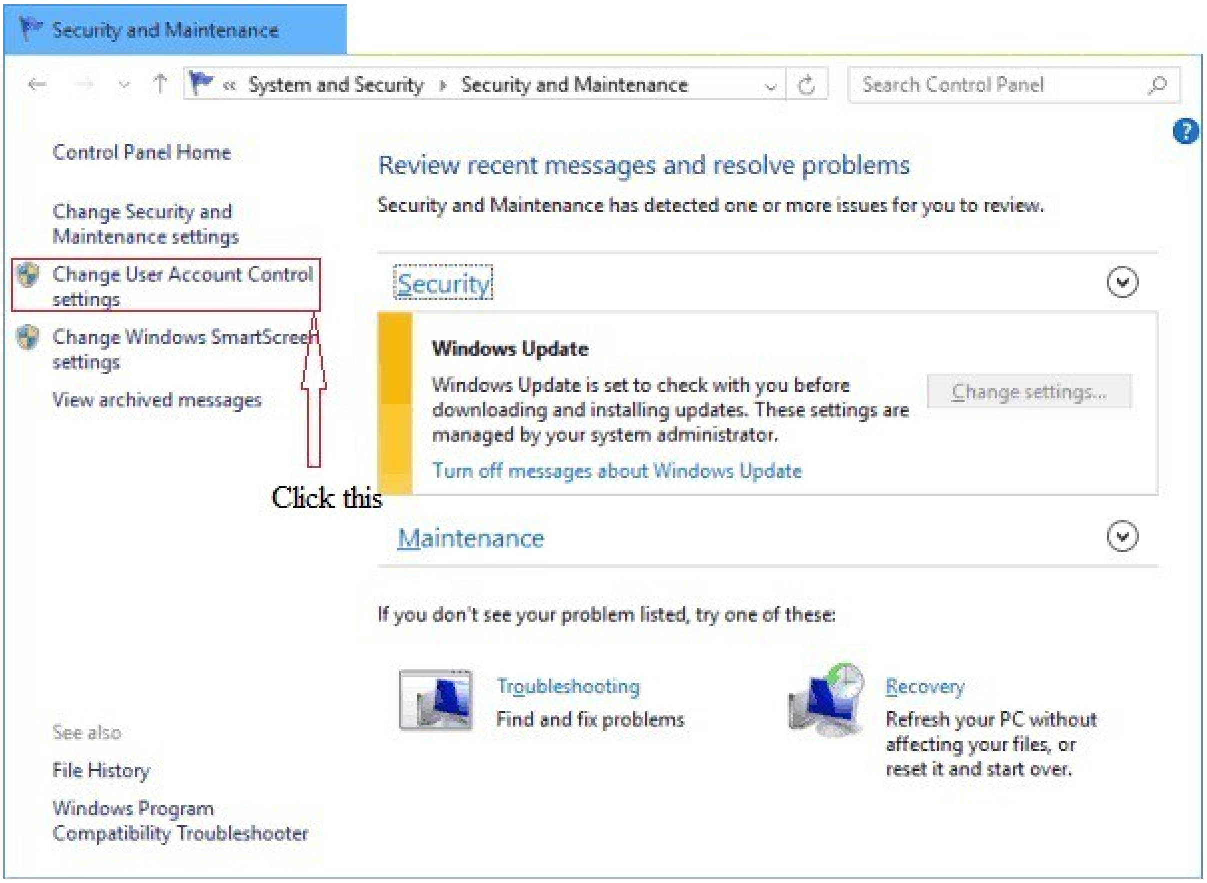
BitLocker Drive Encryption

Manage BitLocker

Storage Spaces

Manage Storage Spaces

3. Tap "**Change User Account Control settings**" on the left to continue.



Review recent messages and resolve problems

Security and Maintenance has detected one or more issues for you to review.

Windows Update

Windows Update is set to check with you before downloading and installing updates. These settings are managed by your system administrator.

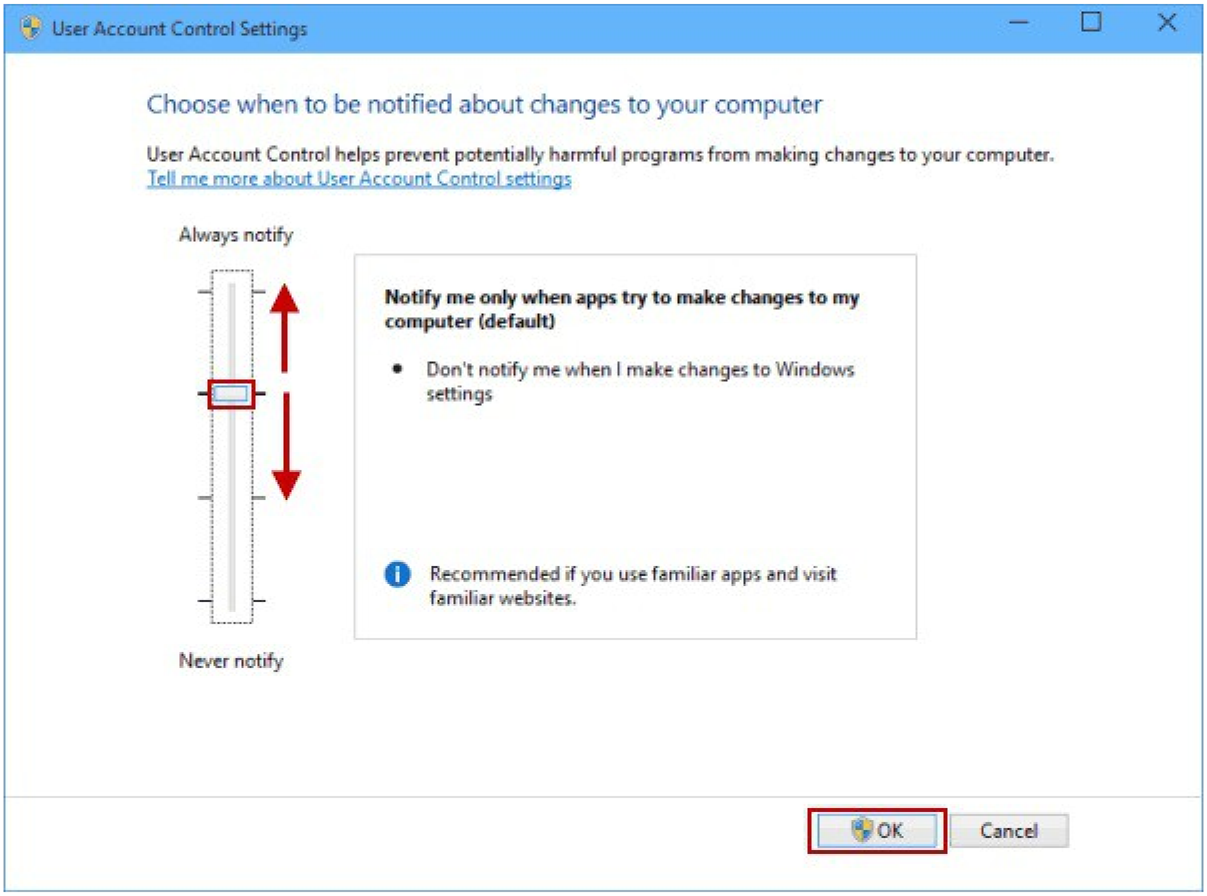
If you don't see your problem listed, try one of these:

Troubleshooting: Find and fix problems

Recovery: Refresh your PC without affecting your files, or reset it and start over.

Click this

4. Move the scale up or down to choose when to be notified about changes to your computer and click OK.


User Account Control Settings

Choose when to be notified about changes to your computer

User Account Control helps prevent potentially harmful programs from making changes to your computer.
Tell me more about User Account Control settings

Notify me only when apps try to make changes to my computer (default)

- Don't notify me when I make changes to Windows settings

Recommended if you use familiar apps and visit familiar websites.

User Account Control notifies you when potentially harmful programs try to make changes to your PC, and you can choose when to be notified about changes to your computer through changing its settings

1. By default, User Account Control will notify you only when apps try to make changes to your computer. And this setting is recommended if you use familiar apps and visit familiar websites, referring to the picture above.
2. If you move the scale to the top to select Always notify, you will be notified when apps try to install software or make changes to your PC and when you make changes to Windows settings. BTW, the setting is recommended if you routinely install new software and visit unfamiliar websites.
3. You can move the scale to choose the third option to ask User Account Control not to dim your desktop when notifying you about apps' up-coming changes to your computer if it takes a long time to dim the desktop.
4. Supposing that you don't want to be notified when apps try to install software and make changes to your PC and when you make changes to Windows settings, move the scale to the bottom to choose Never notify.

There are four possible UAC settings, described as follows:

Always notify: This is the most secure option. It notifies you anytime a program tries to make changes to your computer or to Windows settings. When you are notified of a pending change, your desktop is dimmed (to prevent other programs from running until a decision is made), and you must either approve or deny the change in the UAC dialog box.

Notify me only when programs try to make changes to my computer: This is the default setting Windows notifies you anytime a program tries to make changes to your computer or if a program outside of Windows attempts to make changes to a Windows setting.

Notify me only when programs try to make changes to my computer (do not dim my desktop): Same as the previous setting, except the desktop is not dimmed, which may allow some malicious programs to alter the appearance of the dialog box.

Never notify: This is the least secure setting. If you're logged on as a standard user, changes that require administrator permissions will be denied. If you're logged in as an administrator, those changes will be automatically permitted, potentially exposing your computer, network, and personal information to security risks.

Attempt to install legacy (older) applications in compatibility mode: Select the older OS that the application was originally written for. It is less likely that updates or the latest service pack(SP) will help in this situation. Security updates probably won't have an effect on this scenario either.

The problems such as video card, network card, and modem card can be resolved by booting to Safe Mode. While in Safe Mode, troubleshoot the problem. In Safe Mode, you can uninstall the driver(s) that is causing problem with normal boot process.

If your PC is slow, check for excessive paging. The most likely cause for excessive paging is due to insufficient Memory. Increase the physical Memory on your computer.

Traditionally, workstations can have multiple operating systems installed on them but run only one at a time. By running virtualization software, the same workstation can be running Window 7 along with Windows Server 2008 and Red Hat Enterprise Linux (or almost any other operating system) at the same time, allowing a developer to test code in various environments as well as cut and paste between them within a virtual machine (VM).

If you are unable to remove a suspect file, boot in Safe Mode. In Safe Mode, only required services are loaded. It would typically be possible to remove the file in Safe Mode.

Email sending spam: If a user reports that several emails are being sent using his account without his knowledge. Actually, it might occur in two ways,

1) The spammer has hijacked your email address,
2) He spoofed your email address.

First step in resolving the problem is to change the account password. This would eliminate that some one hijacking your email account. In the second case, the attacker doesn't have access to your email account, but using your email ID as “From” address to send spam. The IP address, host name etc. would be different.
There is actually, no simple solution to this problem One feature that may be useful is DKIM. DKIM short for Domain Keys Identified Mail, is an email authentication method designed to detect email spoofing. It is a way to sign and verify email messages at the message transfer agent (MTA) level using public and private keys. The public keys are published in DNS TXT records. DKIM authenticates the source and its contents.

Email spam (Receiving email): Unsolicited mail is a big problem these days and there is no single solution to this problem. Sender Policy Framework (SPF) is an open standard specifying a technical method to prevent sender address forgery. SPF uses a DNS TXT record in the DNS zone file to limit the number of servers that are allowed to send email on behalf of a domain name. Basically, this tells the receivers, “messages for my domain should only come from these servers.” Messages that are coming from servers other than those specified in the SPF record will be viewed as spam and ignored. Below is an example of an SPF record for an example domain:

```
IN TXT "v=spf1 ip4:192.0.2.12 ip4:192.0.2.130 -all"
```

This record tells us that the IPv4 addresses 192.0.2.1 and 192.0.2.129 are allowed to send email for the designated domain. With the use of “-all,” we stress that only mail that matches this pattern of IPv4 addresses is allowed.

IsoPropyl Alcohol (IPA) is recommended for cleaning PCAs such as motherboards. Mild detergent can be used for cleaning the outside cabinet or the keyboard.

When attending to the computer maintenance or repair (other than the monitor), ensure that you work in a static free environment. Always wear wrist strap. You should not wear clothes/shoes that produce static charges. You should not use an Electrostatic Discharge (ESD) wrist strap when working on an open Cathode Ray Tube (CRT) display. An ESD wrist strap grounds your body to protect components from an ESD shock. However, a CRT display is highly charged, so you do not want to be grounded when you work inside one. In fact, only specially trained personnel should ever open a CRT display.

DLL stands for Dynamic Link Library. DLL is a special form of application code loaded into memory by request. A DLL is not executable by itself. More than one application may use the functions offered by a DLL.

Boot Options: The Advanced Boot Options menu lets you start Windows in advanced troubleshooting modes. The options available are

1. Repair your computer
2. Safe mode
3. Safe mode with networking
4. Safe mode with command prompt
5. Enable boot logging
6. Enable low resolution video (640 x 480)
7. Last Known Good Configuration (advanced)
8. Directory services restore mode
9. Debugging mode
10. Disable automatic restart on system failure
11. Disable Driver Signature Enforcement
12. Start Windows normally

NTLDR (New Technology Loader) Missing error:
If your Microsoft Windows 10-based computer does not start correctly or if it does not start at all, you can use the Windows Recovery Options to help you recover your system software. The causes for an error message like: 'NTLDR is Missing, Press any key to restart', may be due to any of the following reasons:

1. Computer is booting from a non-bootable source.
2. Computer hard disk drive is not properly setup in BIOS.
3. Corrupt NTLDR and/or NTDETECT.COM file.
4. Attempting to upgrade from a Windows 95, 98, or ME computer that is using FAT32.
5. Corrupt boot sector / master boot record.
6. Loose or Faulty IDE/EIDE hard disk drive cable.

To start recovery options

1. Insert the Windows 7 installation disc or USB flash drive, or a system repair disc, and then shut down your computer.
2. Restart your computer using the computer's power button.

Automated System Recovery(ASR): ASR is a part of an overall plan for system recovery so that you are prepared if the system fails. ASR should be a last resort for system recovery. Use ASR only after you have exhausted other options. It is recommended that you use ASR only if all other options to repair the system (such as Last Known Good, and Safe Boot) have failed.

Steps to create Windows Automated System Recovery Disk on Windows 7

1. From the Start menu, select Control Panel.
2. Click Backup and Restore, and then on the left, choose Create a system repair disc.
3. Select a drive, and then click create

MSCONFIG: Short for Microsoft System Configuration Utility is designed to help you troubleshoot problems with your computer, MSCONFIG can also be used to ensure that your computer boots faster. Every time you boot your computer a lot of "hidden" programs load in the background. Some of these hidden programs are essential, but most aren't. Turning off some of these hidden programs (or services) can significantly increase your computer's performance and reliability.

For example, you want to disable DLP program from your computer from startup. To do so, you access MSconfig (System Configuration utility), and then the Services and Startup tabs in order to disable the two components of DLP 2.0 (DLP short for Data Loss Prevention).

1. The Startup tab will allow you to disable the actual application stored in Program Files, stopping the application from starting up when the user logs in.
2. The Services tab will allow you to disable the underlying service so that fewer resources are used, and there is less chance of system issues.
3. The General tab gives you several different startup selections.
4. The Boot tab allows you to modify how the system boots.
5. The Tools tab enables you to launch various OS utilities directly from Msconfig.

Event Logs: Event Log Explorer helps you to quickly browse, find and report on problems, security warnings and all other events that are generated within Windows.

Available logs in Windows 7 are:

1. **Application(program):** Events are classified as error, warning, or information, depending on the severity of the event. An error is a significant problem, such as loss of data. A warning is an event that isn't necessarily significant, but might indicate a possible future problem. An information event describes the successful operation of a program, driver, or service.

2. **Security:**These events are called audits and are described as successful or failed depending on the event, such as whether a user trying to log on to Windows was successful.

3. **Setup:** Computers that are configured as domain controllers will have additional logs displayed here.

4. **System:** System events are logged by Windows and Windows system services, and are classified as error, warning, or information.

5. **Forwarded Events:** These events are forwarded to this log by other computers.

Some of the troubleshooting tools

1. **Log files**: A log file (or simply log) is a file that records either the events which happen while an operating system or other software runs. The act of keeping a logfile is called logging. When a failure occurs in Windows Setup, review the entries in the Setuperr.log file, then the Setupact.log file, and then other log files as appropriate.

2. **Setuperr.log:** It contains information about setup errors during the installation of Windows 7. Start with this log file when troubleshooting. A file size of 0 bytes indicates no errors during installation.

3. **Setupact.log:** It contains the events that occurred during the installation. There are several instances of the Setupact.log file, depending on what point in the installation process the failure occurs.

4. **Unattend.xml:** It is the answer file used by Windows 7 during unattended installations.

5. **Setuplog.txt:** It records events that occurred during the text portion installation of Windows XP. Windows 7 does not have a text portion during installation.

Process Kill: If you prefer to kill processes using the Command Prompt, you can do it. You have to run the Command Prompt as Administrator. To do this just right click command prompt from "All Programs > Accessories > Command Prompt" then select "Run as Administrator" on the pop-up menu.

On the Command Prompt, perform the following.

1. Type "tasklist" and press enter. It will show you a list of all the running processes.
2. Now you can End any particular process by executing the "Task kill" command.
   For Example: To kill Chrome just type "**Task kill /IM chrome.exe /F**"

Where:
/IM - Kill by Image Name
/F - Kill the process forcefully.

Of course, you can also do this using Task Manager without going to the command prompt.

System recovery Options:

1. The Windows 10 recovery environment (WinRE) is also known as System recovery options and recovery console.

2. Windows 10's Recovery Environment enables users to perform a variety of system and data recovery tasks on a system that won't boot normally, including:

    1. Fixing boot-level startup problems (Startup Repair)

    2. Returning your system to a previous configuration (System Restore)

    3. Recovering your computer with a previously-created system image (System Image Recovery)

    4. Checking for defective memory (Windows Memory Diagnostic)

    5. Running command-prompt programs (Command Prompt)

3. Advanced Boot Options is the menu that can be accessed by holding down the Shift key on your keyboard and restart the PC. Windows will automatically start in advanced boot options after a short delay.

📍 *It is very important that you verify that the backup is working properly. It may so happen that you have several backup tapes, but none of them is good.*

SFC: Sfc /scannow will inspect all of the important Windows files on your computer, including Windows DLL files. If System File Checker finds an issue with any of these protected files, it will replace it. You must be logged in as a user with administrator rights in order to run the sfc /scannow command.

Driver Verifier: Driver Verifier monitors Windows kernel-mode drivers and graphics drivers to detect illegal function calls or actions that might corrupt the system. Driver Verifier can subject Windows drivers to a variety of stresses and tests to find improper behavior. You can configure which tests to run, which allows you to put a driver through heavy stress loads or through more streamlined testing. You can also run Driver Verifier on multiple drivers simultaneously, or on one driver at a time. You can use this tool to troubleshoot driver issues. It is available in all versions of Windows starting with Windows 2000. Each version introduces new features and checks for finding bugs in Windows drivers. This section summarizes the changes and provides links to related documentation.

Caution:

- Running Driver Verifier could cause the computer to crash.
- You should only run Driver Verifier on computers that you are using for testing and debugging.
- You must be in the Administrators group on the computer to use Driver Verifier.
- Driver Verifier is not included in Windows 10 S, so we recommend testing driver behavior on Windows 10 instead.

You can start the tool by going to Run > verifier.exe

1. You can start verification of any driver without rebooting, even if Driver Verifier is not already running.
2. You can start the verification of a driver that is already loaded.
3. You can activate or deactivate most Driver Verifier options without rebooting.

PC Security Issues with appropriate tools

- Traditionally, antivirus software relies upon signatures to identify malware. This can be very effective, but cannot defend against malware unless samples have already been obtained, signatures generated and updates distributed to users. Because of this, signature-based approaches are not effective against zero-day viruses.
- A zero-day (or zero-hour or day zero) attack or threat is an attack that exploits a previously unknown vulnerability in a computer application, meaning that the attack occurs on "day zero" of awareness of the vulnerability. This means that the developers have had zero days to address and patch the vulnerability.
- It is possible that sensitive information is relayed to the hacker unless the infected system is disconnected from the network. It may also infect other systems by remote triggering.
- System Restore automatically track changes to your computer and creates restore points before major changes are to occur. To create a restore point, System Restore takes a full snapshot of the registry and some dynamic system files. For example, restore points are created before new device drivers, automatic updates, unsigned drivers, and some applications are installed. To create a System Restore Point in Windows 10, use the sequence, Start | All Apps|Windows Accessories | System Tools, and then click System Restore. Alternatively, you may just type "restore" in the search box, and click on the "System Restore" option that appears above.

Back

4.2 Troubleshooting mobile OS and application issues

4.3 Troubleshooting mobile OS and application security issues

5. Operational Procedure

5.1 Given a scenario use appropriate safety procedures

- If an older program doesn't run correctly, use the Program Compatibility Wizard to simulate the behavior of earlier versions of Windows.

- **Installing peripheral devices such as printers at customer premises**: Expect that your customers are not very familiar with the usage of the device. Show the customer how to use the device. For example, if you had installed a printer, show the customer how to use the printer and also print a test page. Relevant manuals (hard copy or electronic version) along with drivers need to be provided to the customer.

- **Hot-Swapping:** Usually, you need to consult the manufacturer's documentation to verify which components are hot-swappable. Therefore, it is recommended to refer the documentation, and if the power supply is hot-swappable, there is no need to switch off the server computer, thus preventing any inconvenience to the users.

- **Slow system response or start up problems:** Possible reasons for slow running of a computer may include insufficient memory, viruses and Trojan horses, too many TSRs (Terminate and Stay Resident) running at the same time, etc. Ensure that your computer has sufficient memory, hard disk space, and anti-virus software installed (particularly if connected to the Internet).

- Windows Logo'd Products List provides compatibility information with existing software, and MS recommends that you check the same.

- Placing the paging file on different physical disks is optimal. This will improve faster access to the Paging file, and also distribute the load.

- By default, Windows 7 stores a user's profile in the C:\Users\<user_name> folder on the computer the user logs on. When a new user logs on, his initial user profile is an exact copy of either the local or domain-wide "default user" profile folder. The local default user profile folder is located in %root%\Users. If you have installed Windows 7 in C drive, it is C:\Users\ <user_name>.

- The proper options for throwing away the old equipment

1. Donate to a charity
2. Recycle it by giving it to a recycle center
3. Give it to a training school in the neighborhood

- Batteries contain environmentally hazardous chemicals and therefore, should not be disposed through dustbin. Always refer to the manufacturer's instructions or the relevant State guidelines. The same is true when you are disposing chemical solvents.

- Electrostatic discharge (ESD) can damage the component at as little as 110 volts. CMOS chips are the most susceptible to ESD. Static electricity builds up more in cold and dry places. Use humidifiers to keep room humidity at about 50% to help prevent static build up.

- MSDS stands for Material Safety Data Sheet. It is US state department document that contain information on any substance that is hazardous, and proper use/disposal.

- When working on computers, use special ESD wrist strap. Do not directly ground yourself with a piece of wire. An ESD wrist strap has built-in resistor to prevent electric shock. Use specially designed grounded ESD mats. Do not wear synthetic clothing. Place all electronic components into anti static bags. Anti static bags can be reused. Keep your workplace clean.

- Follow anti-static precautions before touching any electronic components inside a PC.

- As the humidity decreases, static build up will increase and vice versa. A level of 50% is considered safe. Below 50% humidity, static build up will be more.

- To clean a keyboard soak it in a distilled demineralized water as soon as possible after the spill. Take precaution to remove the keyboard before doing so, and dry it before connecting back.

- The MSDS contains wealth of information including Product and Company information, First aid measures, Handling and storage, Physical and chemical properties, etc.

- Laptop batteries (and most other batteries) consist of hazardous material. You need to dispose them according to the hazardous material disposal procedures. Enquire local authorities about disposal procedure.

- Sensitive discussions overheard are confidential, and should be treated accordingly.

- While repairing failed boot problem some folder containing user data were lost during the repair process , in such a case you need to take the customer in to confidence, and apologize to him/her for having lost some important files/folders.

Proper component handling and storage:

Antistatic wrist strap: A technician can prevent ESD by using a variety of methods. The most common tactic is to use an antistatic wrist strap. One end encircles the technician's wrist. At the other end, an alligator clip attaches to the computer. The clip attaches to a grounding post or a metal part such as the power supply.

Antistatic bag: Antistatic bags are good for storing spare adapters and motherboards when the parts are not in use. However, antistatic bags lose their effectiveness after a few years. Antistatic mats are available to place underneath a computer being repaired; such a mat may have a snap for connecting the antistatic wrist strap. Antistatic heel straps are also available.

Self-grounding: Electrical outlets are designed to protect you from electrical shock. Modern building codes require all outlets to be either self-grounded or ground-fault circuit interrupters.

Personal safety:

Disconnect power before repairing PC: Always be absolutely sure that that your unit is completely disconnected from the power source before you begin any internal service. It is also good to discharge any energy stored in the components. After unplugging the unit hold the power button down for a few seconds. This will cause the PC to initiate the boot process. Without a power source, the unit will not boot but will dump any energy stored in the capacitors. Performing this simple procedure will reduce the possibility of any electrical shorts or harmful accidental discharge.

Remove jewelry: Remove your jewelry before any electronic service. Doing this will eliminate the possibility of damage caused by shorts and accidental discharges. You will be safer and so will the unit you are working on. If you have an ID badge around your neck or even a necktie, be sure to tuck it inside your clothing while you are servicing. You don't want to catch on any mechanical components like fans or optical drives.

Lifting techniques: When lifting take a second or two to consider the weight of the object its location (floor, desk or shelf). Now think about the best practices for lifting. For example, keep your back straight and use your legs to lift. Use leverage instead of muscle. A little forethought can spare you weeks of pain.

Weight limitations: Your job description could cover lifting minimums but you will see that rarely is there a maximum limit. Here again, planning will give you the opportunity to perform the task without injury. Plan for items like carts or hand trucks to help manage heavy weights or long distances.

Electrical fire safety: In the event of an electrical fire, you should make every effort to remove the power. Many fires are a result of someone bypassing or ignoring simple electrical safety procedures. For example, don't overload the outlets. Use extension cords as a temporary solution only and never plug one extension cord into another. Examine the plug and cord of a device for signs of wear and replace before using. Never run a cable of any type under a rug or mat. Fire safety codes require fire extinguishers of the types indicated in specific locations. Electrical fires can be either of two classes depending on their state. When energized the fire is Class C, then once the power is removed it becomes the class of the burning material i.e. plastic or Class B. here is a clearly labeled Carbon dioxide fire extinguisher.

Cable management: As mentioned above that you should not run cables under rugs or mats. Then how do you keep people from tripping on cables? You don't run them across the floor, period. There is no condition that justifies running cables across the open floor or walkways. Bundle cables together using Velcro straps or zip ties.

Safety goggles: You should be in the habit of wearing eye protection at all times in the workplace. Choose the right style for the type of protection you require. Safety eyewear has impact resistant properties and there are designs that offer additional protection against chemical splashes and airborne contaminants like dust or laser printer toner. In a dusty or dirty environment, you should always protect your lungs. Irritants suspended in the air may be invisible. You will be able to see the effectiveness of a filter mask by examining the mask after a period of use. Any particulate matter filtered out of the air will be visible on the mask. You may be surprised.

Compliance with local government regulations: When you are in the workplace keep in mind that certain activities like cable routing and disposing of hazardous waste are regulated under local codes or ordinances. You should be aware of these regulations in order to comply with them.

Back

5.2 Demonstrate proper communication techniques and professionalism

5.3 Processes for addressing prohibited content/activity, and privacy, licensing, and policy concepts

6. Appendix

6.1 Windows7 Upgrade & Other features