CompTIA®A+ Core 2 Exam Notes : Features Of Various Microsoft Operating Systems

1. Windows Operating Systems

1.2 Features of various Microsoft operating systems

Features of Windows7:

1. Only 64 bit versions of windows 7 can handle over 4GB of memory (RAM).

2. The following table specifies the limits on physical memory for Windows 7.

Version	Limit on x86	Limit on x64
Windows 7 Ultimate	4 GB	192 GB
Windows 7 Enterprise	4 GB	192 GB
Windows 7 Professional	4 GB	192 GB
Windows 7 Home Premium	4 GB	16 GB
Windows 7 Home Basic	4 GB	8 GB
Windows 7 Starter	2 GB	2 GB

3. Both the 32 bit and 64 bit versions of Windows 7 require minimum 1 GHz

If you want to run Windows 7 on your PC, given below are the hardware requirements:

1. 1 GHz or faster 32-bit (x86) or 64-bit (x64) processor

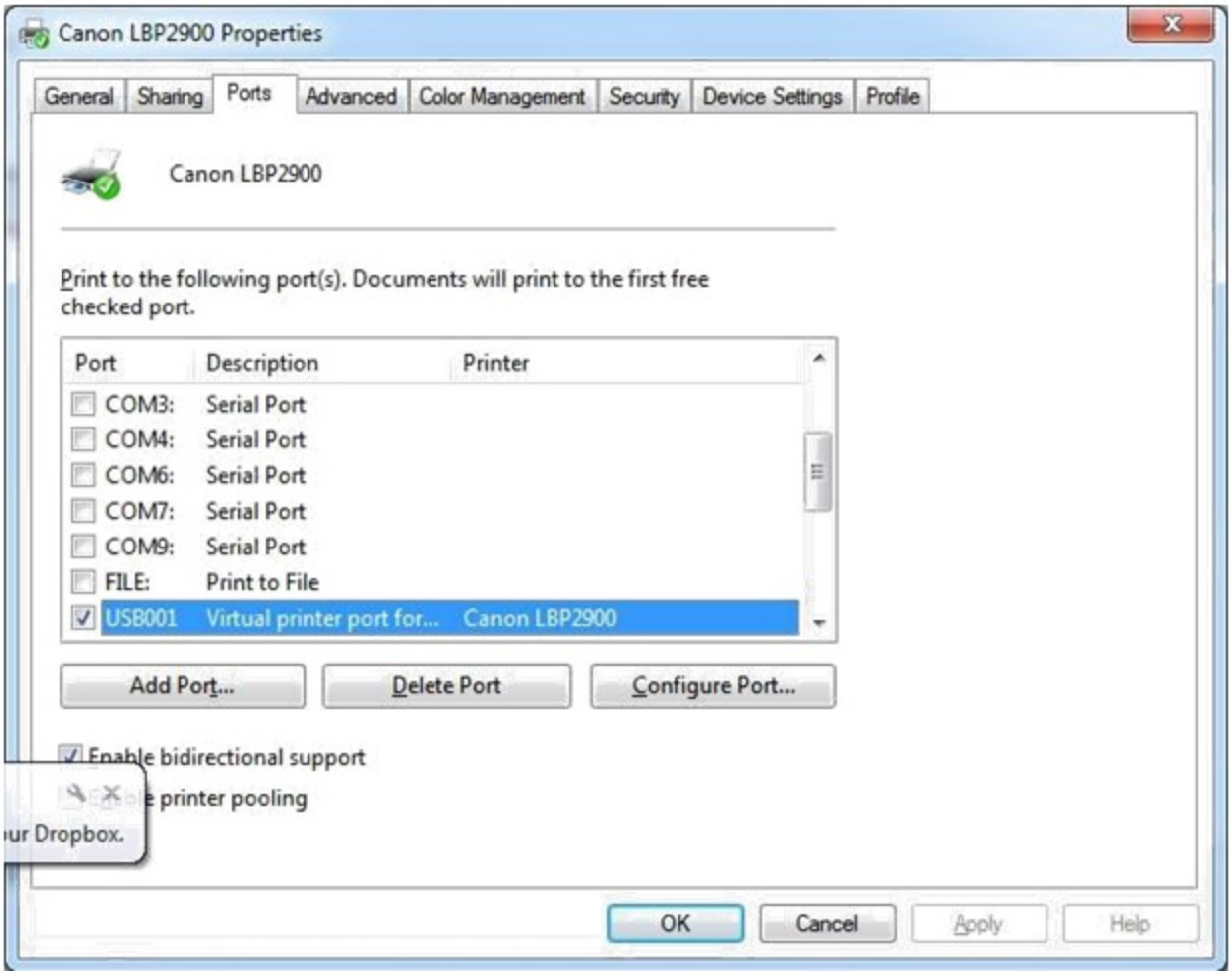
2. 1 GB RAM (32-bit) or 2 GB RAM (64-bit)

3. 16 GB available hard disk space (32-bit) or 20 GB (64-bit)

4. DirectX 9 graphics device with WDDM 1.0 or higher driver

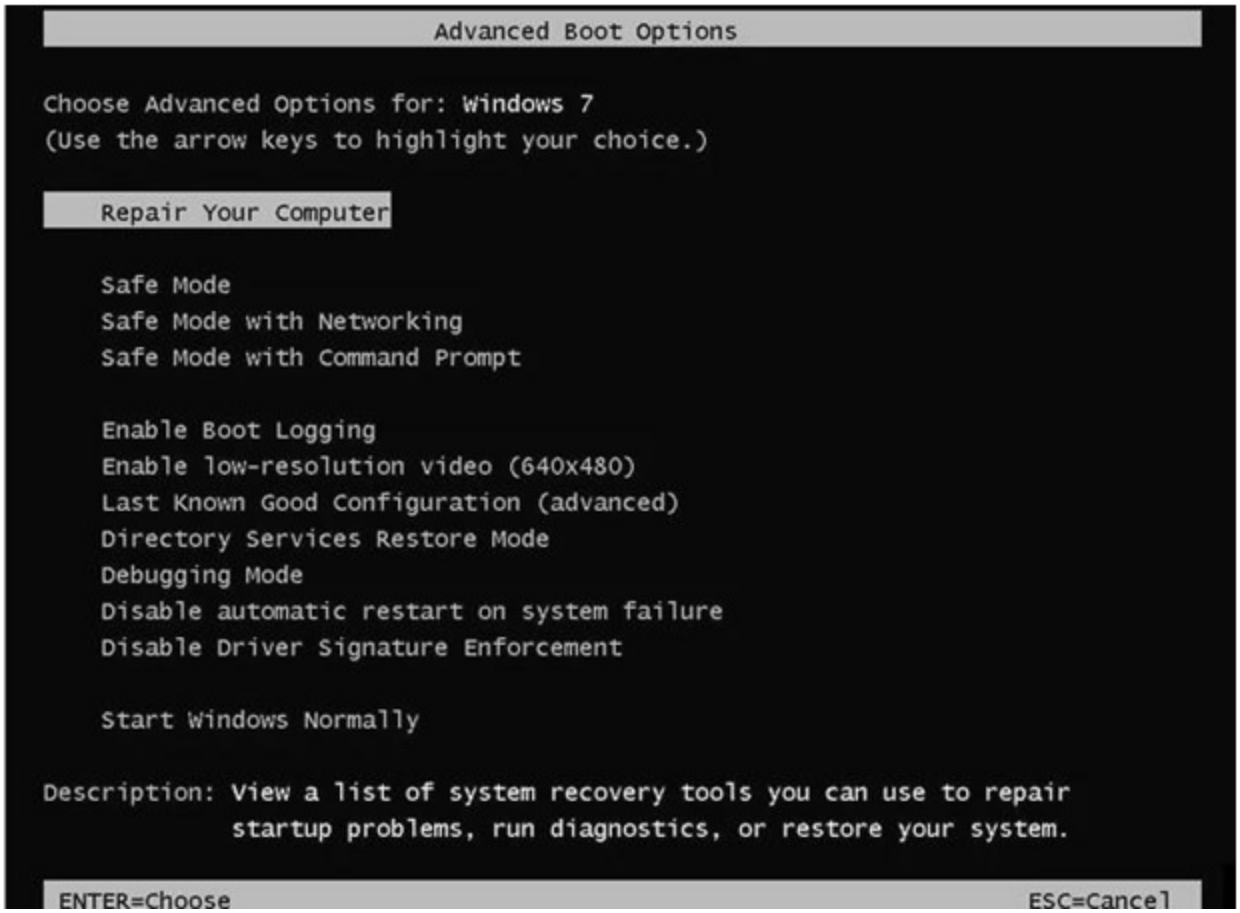
4.Automatic Restart on Major Error (Windows 7): The automatic restart option in Windows 7 is enabled by default. As a result, if there is any major error, the Operating System will automatically restart.

5. To Know the Port on which the Printer is connected: In a Windows 7 computer, go to Control Panel\Hardware and Sound\Devices and Printers and right click on appropriate printer. Click on "Printer Properties" to open the properties window of the chosen printer. Click on Ports tab to view the port on which a printer is connected. A typical screen-shot is shown below:



Windows 7 Start-Up Options:

Windows 7 advanced startup options can be accessed by pressing F8 key when prompted during the beginning of the Windows 7 boot process. The following options will be made available as shown in the below fig.



1. **Repair Your Computer:** Shows a list of system recovery tools you can use to repair startup problems, run diagnostics, or restore your system. This option is available only if the tools are installed on your computer's hard disk. If you have a Windows installation disc, the system recovery tools are located on that disc.

2. **Safe Mode:** Starts Windows with a minimal set of drivers and services.

3. **Safe Mode with Networking:** Starts Windows in safe mode and includes the network drivers and services needed to access the Internet or other computers on your network.

4. **Safe Mode with Command Prompt:** Starts Windows in safe mode with a command prompt window instead of the usual Windows interface. This option is intended for IT professionals and administrators.

5. **Enable Boot Logging:** Creates a file, ntbtlog.txt, that lists all the drivers that are installed during startup and that might be useful for advanced troubleshooting.

6. **Enable low-resolution video (640x480):** Starts Windows using your current video driver and using low resolution and refresh rate settings. You can use this mode to reset your display settings.

7. **Good Configuration (advanced):** Starts Windows with the last registry and driver configuration that worked successfully.

8. **Directory Services Restore Mode:** Starts Windows domain controller running Active Directory so that the directory service can be restored. This option is intended for IT professionals and administrators.

9. **Debugging Mode:** Starts Windows in an advanced troubleshooting mode intended for IT professionals and system administrators.

10. **Disable automatic restart on system failure:** Prevents Windows from automatically restarting if an error causes Windows to fail. Choose this option only if Windows is stuck in a loop where Windows fails, attempts to restart, and fails again repeatedly.

11. **Disable Driver Signature Enforcement:** Allows drivers containing improper signatures to be installed.

12. **Start Windows Normally:** Starts Windows in its normal mode.

Application dock: The application dock is available in Windows 7. The application dock is an enhanced version of the taskbar. With this, you can hover over applications that are running in the taskbar and view their current status (for example, if you are downloading something). You can also click and drag applications to and from the dock and close apps if you wish. Docking applications is fairly standard practice nowadays, and several other operating system manufacturers have similar functionality.

Note the following important points regarding various versions of Windows Operating Systems:

1. In Windows 7, a user may hide any displayed Update by right clicking on it and selecting "hide" option.

2. In Windows 7, 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.

3. In Windows 7, a user may opt to manually update any Windows Updates by selecting appropriate options in the Updates applet.

4. 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

5. 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.

6. You need to migrate (do fresh installation) from XP to Windows 7, also you cannot upgrade from 32 bit to 64 bit.

7. You can enable or disable the CTRL+ALT+DELETE sequence for logging on in Windows 7, and 8/8.1/10

8. You can require users to press CTRL+ALT+DELETE before logging on to a Windows 7-based computer, or you can eliminate this requirement for a faster logon process. Note that you must be logged on with Administrator rights to enable or disable CTRL+ALT+DELETE login.

9. Disabling the CTRL+ALT+DELETE sequence creates a "security hole." The CTRL+ALT+DELETE sequence can be read only by Windows, ensuring that the information in the ensuing logon dialog box can be read only by Windows. This can prevent rogue programs from gaining access to the computer. Microsoft recommends that you enable CTRL+ALT+DELETE for login.

10. Set up the drive in the BIOS is incorrect because today's computer's BIOS should see the drive automatically with no configuration needed. In special cases a hard disk might require special drivers.

11. If your Microsoft Windows 7- 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.

12. Drivers developed for 32-bit versions of Windows 7 are not compatible with 64-bit versions of Windows 7, and vice a versa.

13. Windows 7 supports FAT16, FAT32, and NTFS file systems.

14. Windows 7 supports Media Center. Though Windows 7 Home Premium also supports it , it is advisable to go for Windows 7 Professional for company use.

15. Windows 7 Operating Systems use Service Packs. However, Microsoft had discontinued with the Service Packs from Windows 8 onwards. So, Windows 8, Window 8.1, and Windows 10 use only UPDATES to implement changes to the Operating Systems. For a big update to Windows 8, Microsoft released Windows 8.1. They have added a revision number instead of a Service Pack. The UPDATES are continual in nature, and usually referred to as Important, Recommended, and Optional.

16. In Windows 7, you can start the Windows Update applet by going to Control Panel > Windows Update.

Windows 7 feature a user interface termed as Aero by Microsoft. Aero interface is characterized by the following features:

1.Glass-like translucent design.

2.Dynamic windows: When you minimize a window, it animates to its place on the taskbar, so it's easier to find when you need it.

3.High dots-per-inch (dpi) support: Windows Aero supports high-resolution monitors, so you can get a laptop or flat-screen monitor that's smaller in size but shows visually richer, displaying high-resolution, easy-to-read images.

4.Live taskbar thumbnails: In Windows Aero, live taskbar thumbnail images display the actual contents of both windows that are currently open and those that are minimized in the taskbar.

5.When you rest your mouse pointer on a tile on the taskbar, you'll see the "live" contents of that window without having to bring it to the foreground.

6.Other features include Windows Flip 3D, and smooth scrolling desktop.

7.The GUI used in Windows 7 is named as Aero.

8.Advanced Boot Options is the menu that can be accessed by pressing F8, which is available in windows 7. It is also referred to as ABOM

BitLocker is available in the Enterprise and Ultimate editions of Windows 7. It is also available in the Pro and Enterprise editions of Windows 8 and windows 10. BitLocker drives can be encrypted with 128 bit or 256 bit encryption. BitLocker protects your hard drive from offline attack. This is the type of attack where a malicious user will take the hard drive from your mobile machine and connect it to another machine so they can harvest your data. BitLocker also protects your data if a malicious user boots from an alternate Operating System. With either attack method, BitLocker encrypts the hard drive so that when someone has physical access to the drive, the drive is unreadable.

BitLocker Drive Encryption: It is a full disk encryption feature included with the Ultimate and Enterprise editions of Microsoft's Windows 7 desktop operating systems.

In order for BitLocker to operate, the hard disk requires at least two NTFS-formatted volumes one for the operating system (usually C:) and another with a minimum size of 100MB from which the operating system boots. BitLocker requires the boot volume to remain unencrypted, so the boot should not be used to store confidential information.

Only the Ultimate version of Windows 7 comes with Bitlocker and BitLocker To Go. Improved for Windows 7 and available in the Ultimate edition, BitLocker helps to keep everything from documents to passwords safer by encrypting the entire drive that Windows and your data reside on. Once BitLocker is turned on, any file you save on that drive is encrypted automatically.

Trusted Platform Module(TPM): TPM is a microchip that is built into a computer. It is used to store cryptographic information, such as encryption keys. Information stored on the TPM can be more secure from external software attacks and physical theft.

BitLocker uses the TPM to help protect the Windows operating system and user data and helps to ensure that a computer is not tampered with, even if it is left unattended, lost, or stolen.

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.

In addition, please note the following:

DOS, and Windows 7/8/8.1/10 operating systems share the following criteria:

1. Each can have only one primary partition per hard disk.

2. The primary partition is automatically assigned a drive letter.

3. Each hard disk can have only one Extended partition

4. You can create one or more logical drives in the Extended partition.

5. When you create a logical drive in Windows 7, drive letter is automatically assigned. However, you can change the drive letter later.

Windows Firewall: Firewall is one of the most important security software on your Windows 7/8/8.1/10 computer. Windows 7/8/8.1/10 include firewall to protect the computer against Malware, Malicious software and unwanted programs from internet and intranet. Firewall monitors both the incoming and outgoing connections. Microsoft Windows 7/8/8.1/10 comes pre-installed with a software firewall utility.

Enabling the Windows 7/8/8.1/10 firewall:

Control panel -> System and security -> Windows Firewall -> Turn Windows Firewall on or off

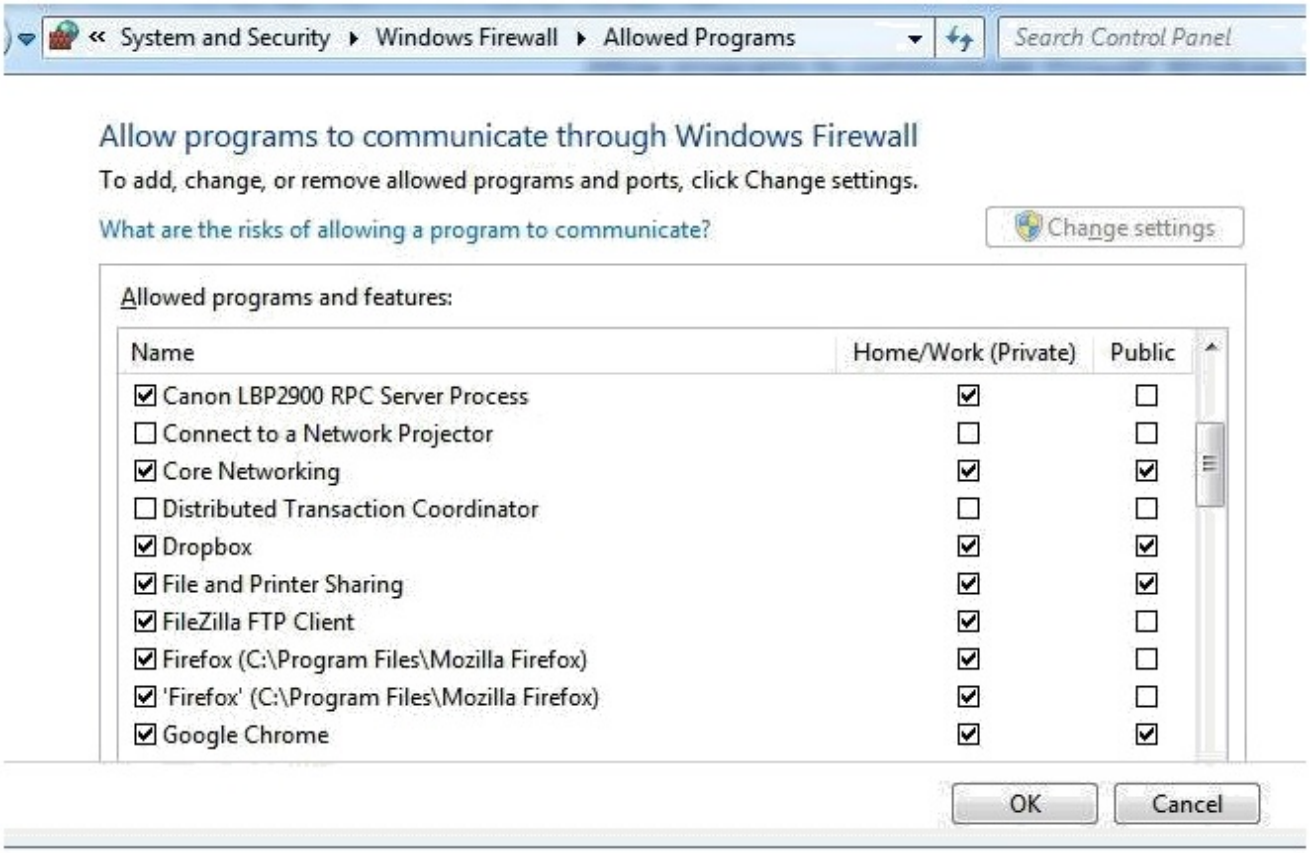
Windows lets you set each network you connect to as either a “Private” or “Public” network. When you connect to a network the first time, Windows 10 asks if you want your computer to be discoverable or not by other computers.

You can customize how Windows treats Private and Public networks, but here’s how it works by default.

On Private networks, Windows enables network discovery features. Other devices can see your Windows computer on the network, allowing for easy file sharing and other networked features. Windows will also use the Homegroup feature to share files and media between your PCs.

On Public networks like those in coffee shops you don’t want your computer to be seen by others, though, or share your files with them. So Windows turns off these discovery features. it won’t appear to other devices on the network and won’t try to discover them. Even if you’ve set up a Homegroup on your PC, it won’t be enabled on a public network. By default it will notify the unauthorized incoming connection to the computer.

It is possible to configure programs that are allowed/dis-allowed. A sample screen-shot of allowed/disallowed programs is shown below:



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 tasks.

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

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

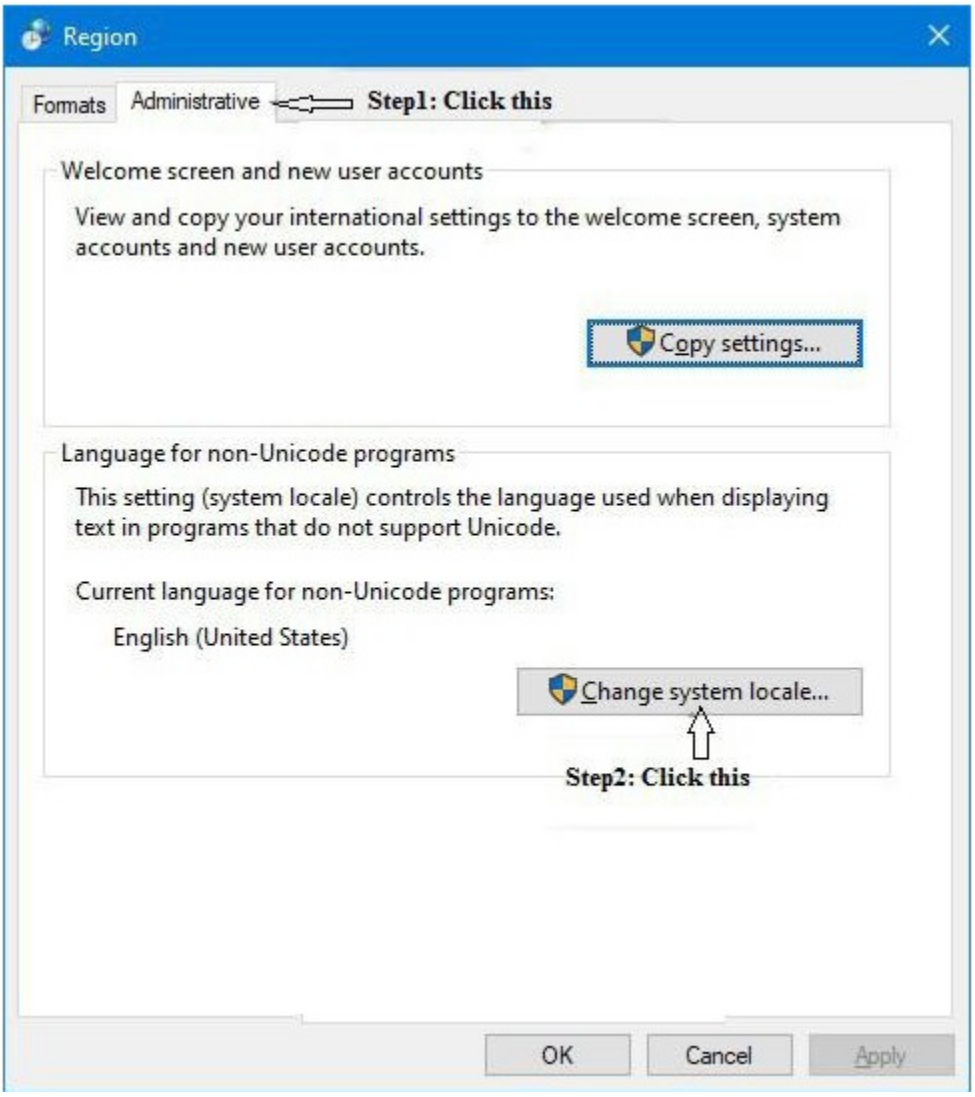
If there is no Advanced tab, then you are not logged in with administrative privileges.

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



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.

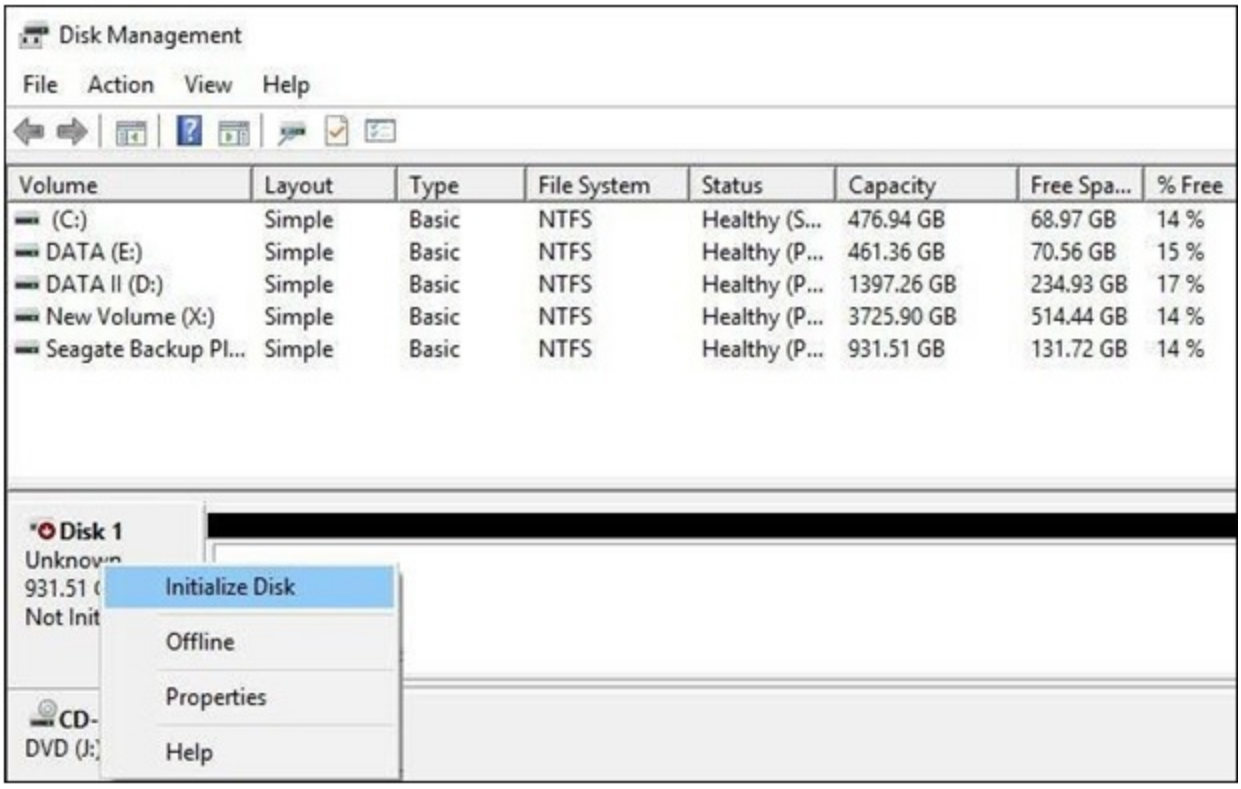
To initialize a new disk using Disk Management use the steps given below:

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.



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:

1. 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.

2. Use the arrow key to select "Advanced", "Onboard Devices" or "Integrated Peripherals" from the menu. Press "Enter."

3. Select "USB Controller." Press "+" or "-" to change the setting to "Enabled."

4. 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

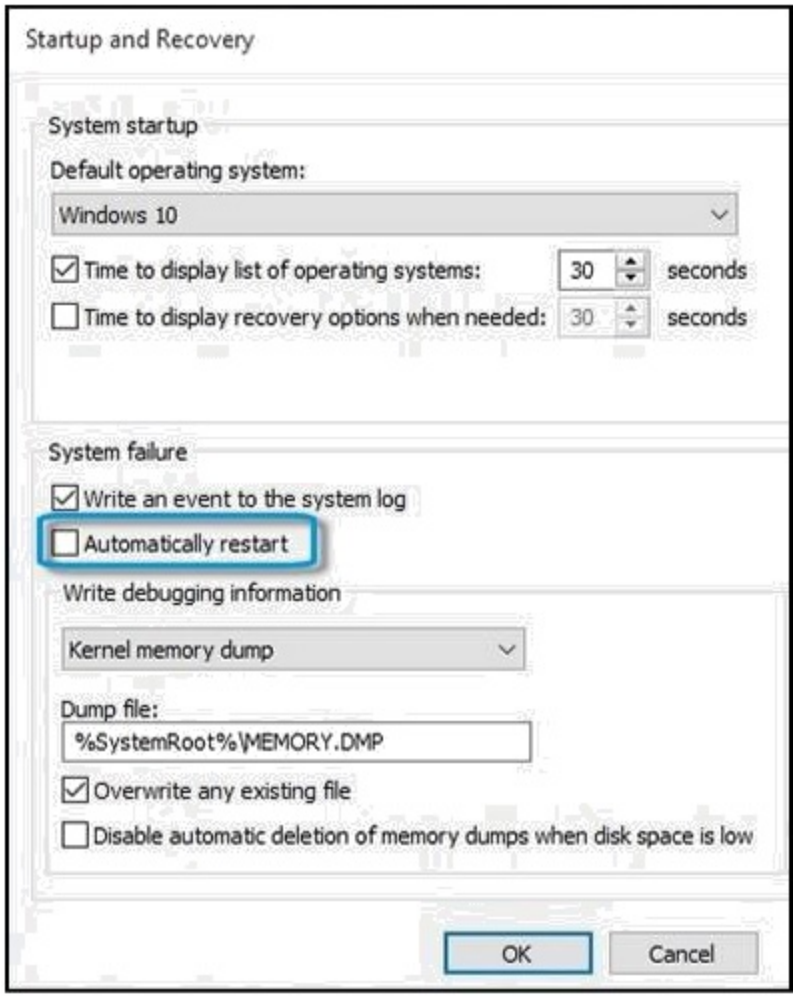
1. In Windows, search for and open View advanced system settings.

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

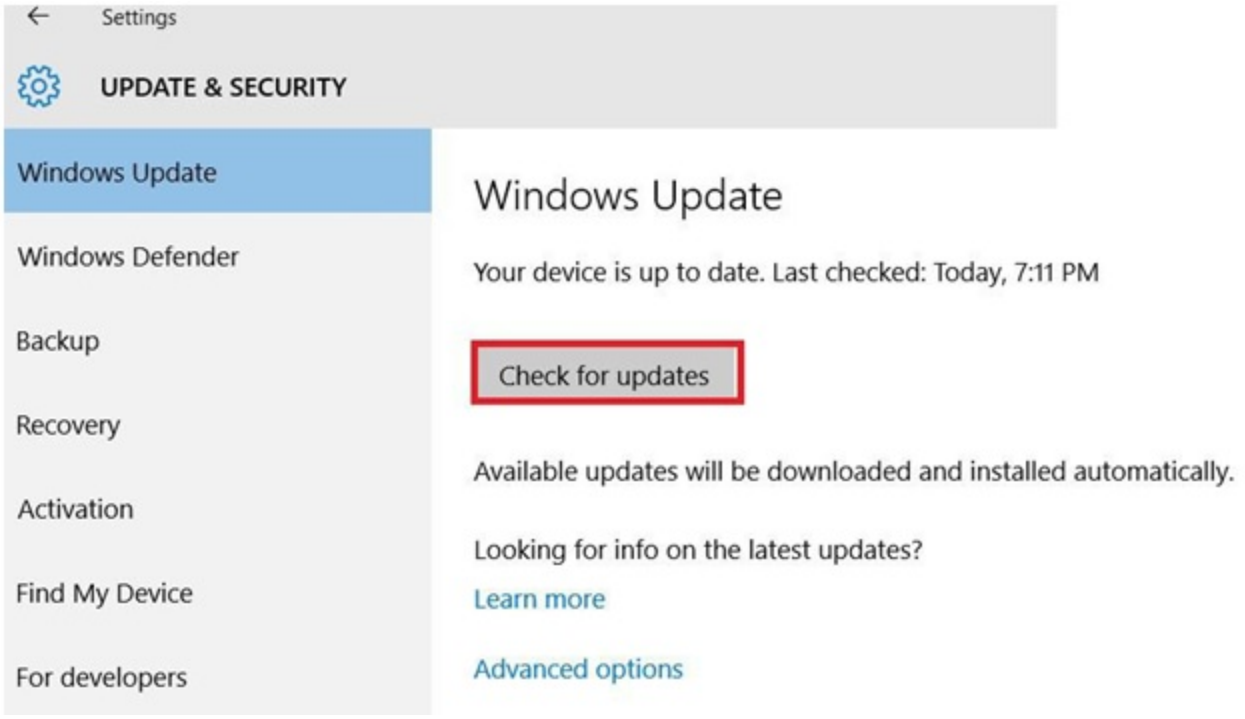


The ability to choose the restart options is very convenient as you can view any error messages and restore failed hardware.

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.



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

More info: https://docs.microsoft.com/en-us/windows/deployment/upgrade/windows-10-upgrade-paths

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:

- Standard Safe Mode - press the 4 or the F4 key on your keyboard to start it
- Safe Mode with Networking- press 5 or F5
- 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

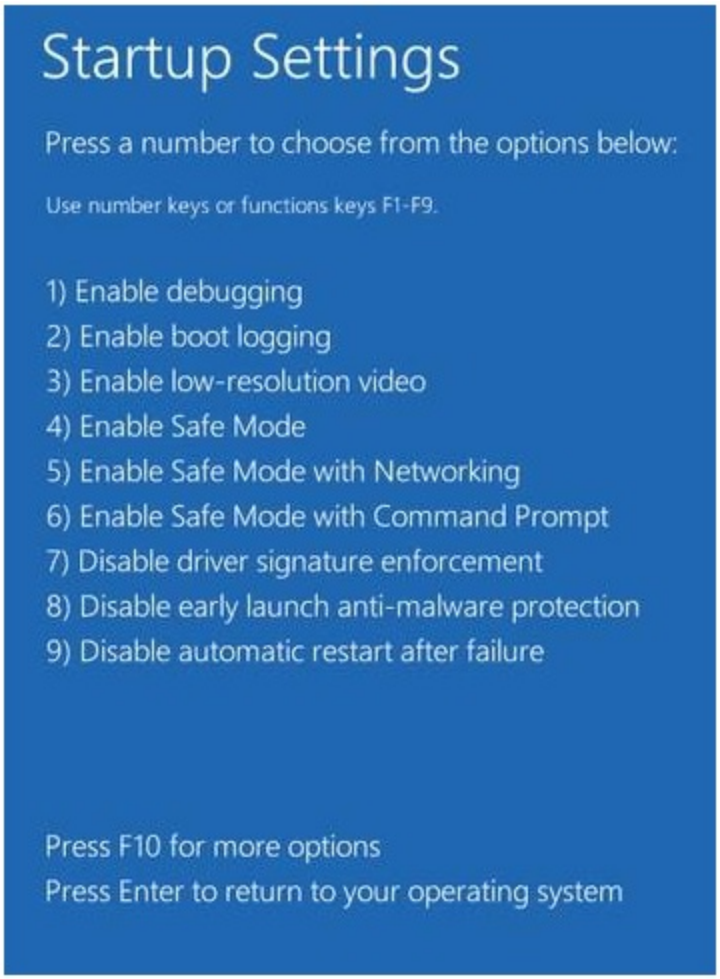
7. Disable driver signature enforcement

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

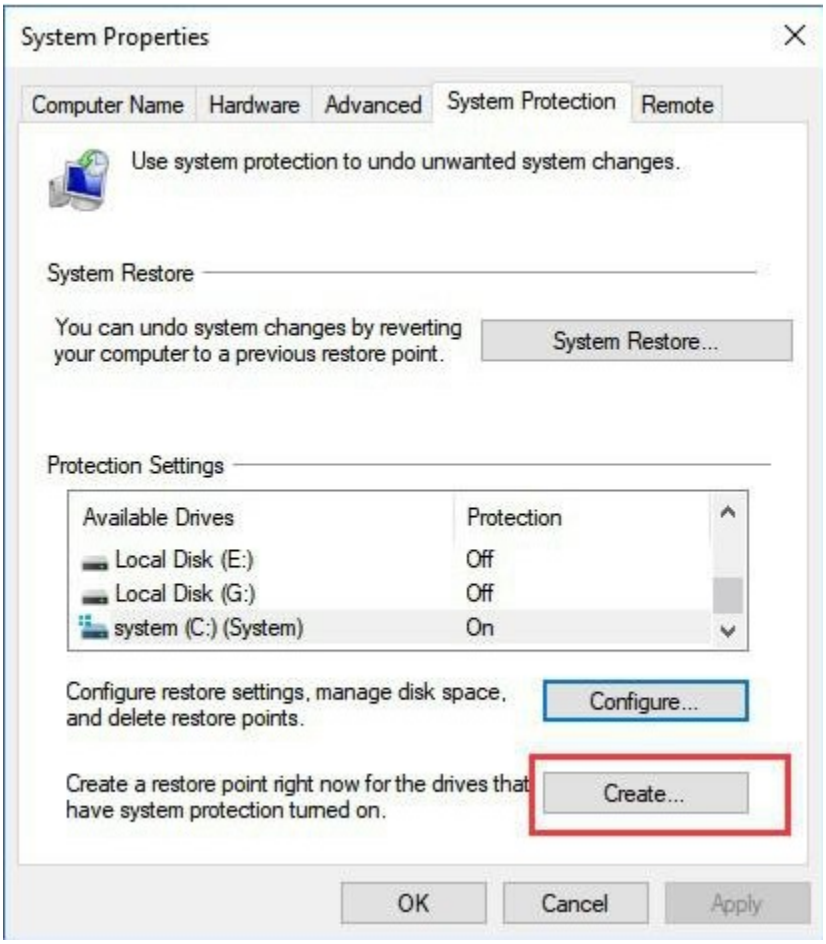
System Restore in windows 10: If your Microsoft Windows 10 based computer does not start correctly or if it does not start at all, you can use the Windows Recovery Options to help you recover your system software. Backup useful files and documents when you are trying to perform System Restore on your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



https://www.easeus.com/backup-recovery/system-restore-in-windows-10-with-system-restore-freeware-tool.html

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.

https://www.tenforums.com/tutorials/27649-run-startup-repair-windows-10-a.html

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

Previous Contents Next

CompTIA®A+ Core 2 Exam Notes : Installing Windows Pc Operating Systems Using Appropriate Methods

examguides.com/Aplus-Core2/aplus-core2-1.htm

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.

To Mark a Partition as Active in Windows 7:

1. You must be logged on as an administrator to mark a partition as active.

2. You can't make a logical drive or an extended partition active. Only a primary partition can be made active.

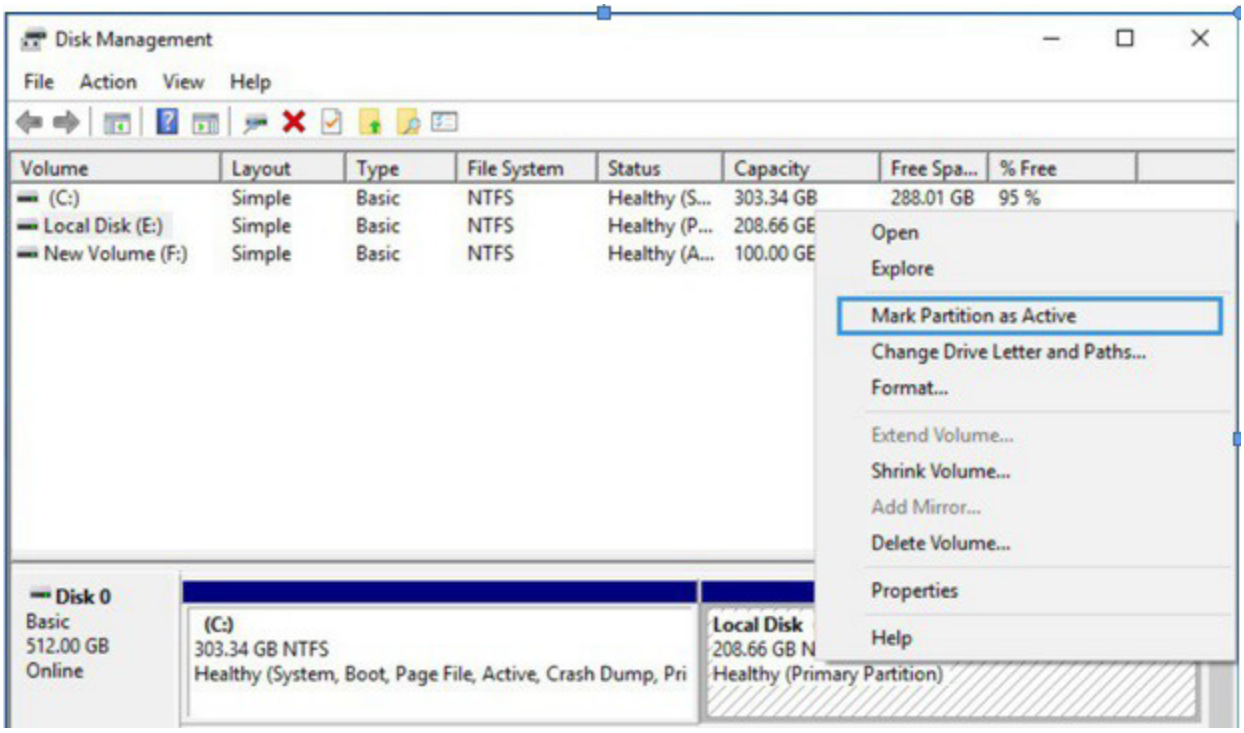
3. There can be only one active partition per physical hard disk.

4. If you have multiple hard disks installed on your computer, it's possible for each hard disk to have a partition set as active. However, the active partition on the first hard disk that your computer's BIOS detects is the one that will start the computer.

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



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: 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”.

Note: 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 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

1. eSATA

2. USB

3. 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.

AT32: 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.

Previous Contents Next

CompTIA®A+ Core 2 Exam Notes : Microsoft Command Line Tools Reference

examguides.com/Aplus-Core2/aplus-core2-3.htm

1. Windows Operating Systems

1.3 Microsoft command line tools

Boot Methods: If you fail to boot, first try to boot in Safe Mode. If it doesn't work, try booting to Last Known Good Configuration. If both fail, you can try using Recovery Console. You need to install the Recovery options for choosing this option on your Win 7 computer. If the option is not installed, you may get to the Recovery options by using the Win 7 installation CD ROM.

The file **ntbtlog.txt** file contains information collected if you choose to boot using "Boot Logging" startup option. The file shows which drivers are loaded and which have failed to load.

Windows 7 Boot Sequence

After the BioS start up and the MBR and boot sector of the hard drive have been located and accessed, The windows Boot Manager is started. The following files are required to start windows 7.

1. Bootmgr(Windows Boot Manager): This is the Windows loader program. It takes the place of NTLDR in earlier version of windows and determines which operating system to start.

2. BCD(Boot Configuration Data): Located in \boot\bcd. It furnishes the windows Boot Manager with information about the operating system(s) to be booted. It is the successor to boot.ini and can be modified with MSCONFIG or with the bcdedit.exe program. BCD was developed to provide an improved mechanism for describing boot configuration data and to work better with newer firmware models such as the Extensible Firmware Interface (EFI).

3. Ntoskrnl.exe: The Windows kernel, which completes the boot process after being initialized by the Windows boot Manager.

4. Hal.dll: The Hardware Abstraction Layer, a software translator between Windows and system hardware.

5. SYSTEM key in the Registry: This is read to determine the system configuration.

6. Device drivers: Thease are loaded according to the information stored in the Registry.

To restore Windows Boot Loader in Windows 7 computer, do the following:

The Bootrec.exe tool supports the following options. Use the option that's appropriate for your situation.

/FixMbr: This option writes a Windows 7 compatible MBR to the system partition. It does not overwrite the existing partition table. Use this option when you must resolve MBR corruption issues, or when you have to remove nonstandard code from the MBR.

/FixBoot: This option writes a new boot sector to the system partition by using a boot sector that's compatible with Windows 7. Use this option if one of the following conditions is true:

- The boot sector was replaced with a nonstandard Windows Vista or Windows 7 boot sector.
- The boot sector is damaged.
- An earlier Windows operating system was installed after Windows Vista or Windows 7 was installed. In this situation, the computer starts by using Windows NT Loader (NTLDR) instead of Windows Boot Manager (Bootmgr.exe).

3. /ScanOs: This option scans all disks for installations that are compatible with Windows 7. It also displays the entries that are currently not in the BCD store. Use this option when there are Windows 7 installations that the Boot Manager menu does not list.

4. /RebuildBcd: This option scans all disks for installations that are compatible with Windows 7.

Additionally, it lets you select the installations that you want to add to the BCD store. Use this option when you must completely rebuild the BCD store.

Recovery Console provides command prompt options for recovering failed operating system boot process. If the OS is not recognized at all, you may start with FixMBR command as below: bootrec.exe /FixMbr: Repairs the Master Boot Record

Though the above command fixes the MBR, there still might be an error with the system partition's boot sector and Boot Configuration Data (BCD). This might occur if you have tried to install another operating system alongside Windows 7, such as Windows XP. Use the FixBoot command as below:

bootrec.exe /FixBoot : If you are still faced with your Windows 7 installation not being detected during start up, or if you wish to include more than one operating system choice to your system's boot list, you can try the following command to rebuild your BCD.

bootrec.exe /RebuildBcd: This command will scan all your disks for other operating systems compatible with Windows 7 and allow you to add them to your system's boot list.

Boot from Windows Vista installation disc, select language and keyboard or input method, click Next and choose to Repair your computer. Then you will need to select the operating system that you want to repair. In the System Recovery Options dialog box click Command Prompt and type the following:

Bootrec.exe /FixMbr
Bootrec.exe /Fix Boot

SFC/SCANNOW: SFC/SCANNOW is used to scan to see if you have any missing, corrupted, or modified Windows system files. If any are found, then SFC will attempt to repair them by replacing them with a clean copy from the component store if the component store is not corrupted as well. Usually you would only need to run a SFC scan if you suspect an issue caused by as issue with your system files in Windows. The LDR option is one of several specific switches available in the sfc command, the Command Prompt command used to run System File Checker. Sfc /scannow is the most common way that the sfc command is used. 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.

Check Disk or chkdsk: Check Disk is used to see if a hard drive has any file system errors and bad sectors on it, and attempt to repair or isolate them if found. Usually it's a good idea to run chkdsk at least once a month, or as needed. CHKDSK command line is a free built-in hard drive repair software designed for scanning hard drives for errors or corruption and

repair them if necessary. So, whenever you find your hard drive performs poorly or Windows asks you to repair drive errors, you can first try to run CHKDSK to do the job. Here's how to run CHKDSK /f through This PC in Windows 10.

1. Press Windows Key + X button to bring up the power users menu.

2. In the power users menu, select the "Command Prompt (Admin)" option.

3. Click "Yes" when you are presented with a UAC window requesting permission to launch the Command Prompt as Administrator.

4. In the new Command Prompt window, type chkdsk E: /f /r /x. Here you should replace E with your drive letter.

This option will run CHKDSK to check and repair disk errors in Windows 10. The "/f" parameter tells CHKDSK to fix any errors it finds; "/r" tells it to locate the bad sectors on the drive and recover readable information; "/x" forces the drive to dismount before the process starts.

DEFRAG: Fragmentation makes your hard disk do extra work that can slow down your computer. Removable storage devices such as USB flash drives can also become fragmented. Disk Defragmenter in Windows rearranges fragmented data so your disks and drives can work more efficiently. In other words, DEFRAG utility arranges the clusters of data on the hard drive to achieve better performance by placing all of the clusters for a given file together in a contiguous order. Disk Defragmenter runs on a schedule, but you can also analyze and defragment your disks and drives manually. DEFRAG does not do any repair on your disk, and errors, if any will remain on the disk.

compmgmt.msc: This command opens computer management console.

The switch /s will make all the files and sub directories to be marked as archive.

HKEY_LOCAL_MACHINE: It is the hive where the information specific to the machine will be stored. The information may include, network settings, hardware drivers etc. HKEY_LOCAL_USER hive stores data specific to user configuration, such as desktop color schemes, screen savers, wall paper, and user specific application settings.

Previous Contents Next

CompTIA®A+ Core 2 Exam Notes : Microsoft Operating System Features And Tools

1. Windows Operating Systems

1.4 Microsoft operating system features and tools

Computer management: You can access Computer Management screen through:

1. Start -> Run -> compmgmt.msc

2. Start -> Control Panel-> System and security -> Administrative Tools -> Computer Management.

One of the frequently used resource in "Computer Management" screen is System Tools. System tools contain the following:

1. Task Scheduler

2. Event Viewer

3. System Folders

4. Local Users and Groups

5. Performance

6. Device Manager

These are very useful tools to a system administrator.

Use the disk management plug-in in the computer management applet.

Start -> Control Panel-> System and security -> Administrative Tools -> Computer Management -> Disk Management.

A simpler way to find Disk Management, is to type "disk management" in the search box of the control panel. You will be displayed with the Disk Management applet. Just click on it to open disk management. The Search utility is very handy in finding the applet that does the required job.

Computer Management -> Shared Folders can be used to view some very useful information like

1. Shares information: Here you can see all of the shares that have been configured on the computer.

2. Session Information: Allows you to see username, computer name etc that has connected to a share currently

3. Open Files : Allow you to see currently opened files

MSTSC: Connect and login to a remote machine using the Remote Desktop Protocol (RDP) also known as Terminal Server Connection (TSC).

example : mstsc /f - Starts in full screen mode.

Options include the following:

ConnectionFile	The name of an RDP file for connection
/v:	The remote computer to connect to
/console	Connect to the console of a server (NT/XP)
/Admin	Connect to a session for administering the server (Vista/2008)
/f	Start in Full Screen mode
/w:width	Width of the RDP screen
/h:height	Height of the RDP screen
/span	Match the Remote Desktop width and height with the local virtual desktop, spanning across multiple monitors if necessary. (Vista/2008)
/public	Run Remote Desktop in public mode. Vista/win7/8/Server2008) In public mode, passwords and bitmaps are not cached.
/edit	Open the RDP file for editing.
/migrate	Convert a legacy Client connection file into an .RDP file

Disk Management: Disk Management is used to manage the drives installed in a computer - like hard disk drives (internal and external), optical disk drives, and flash drives. It can be used to partition drives, format drives, assign drive letters, and much more. To enter disk management, click on the Start button and then choose Control Panel

1. Click on the System and Security link.

2. In the System and Security window, click on the Administrative Tools.

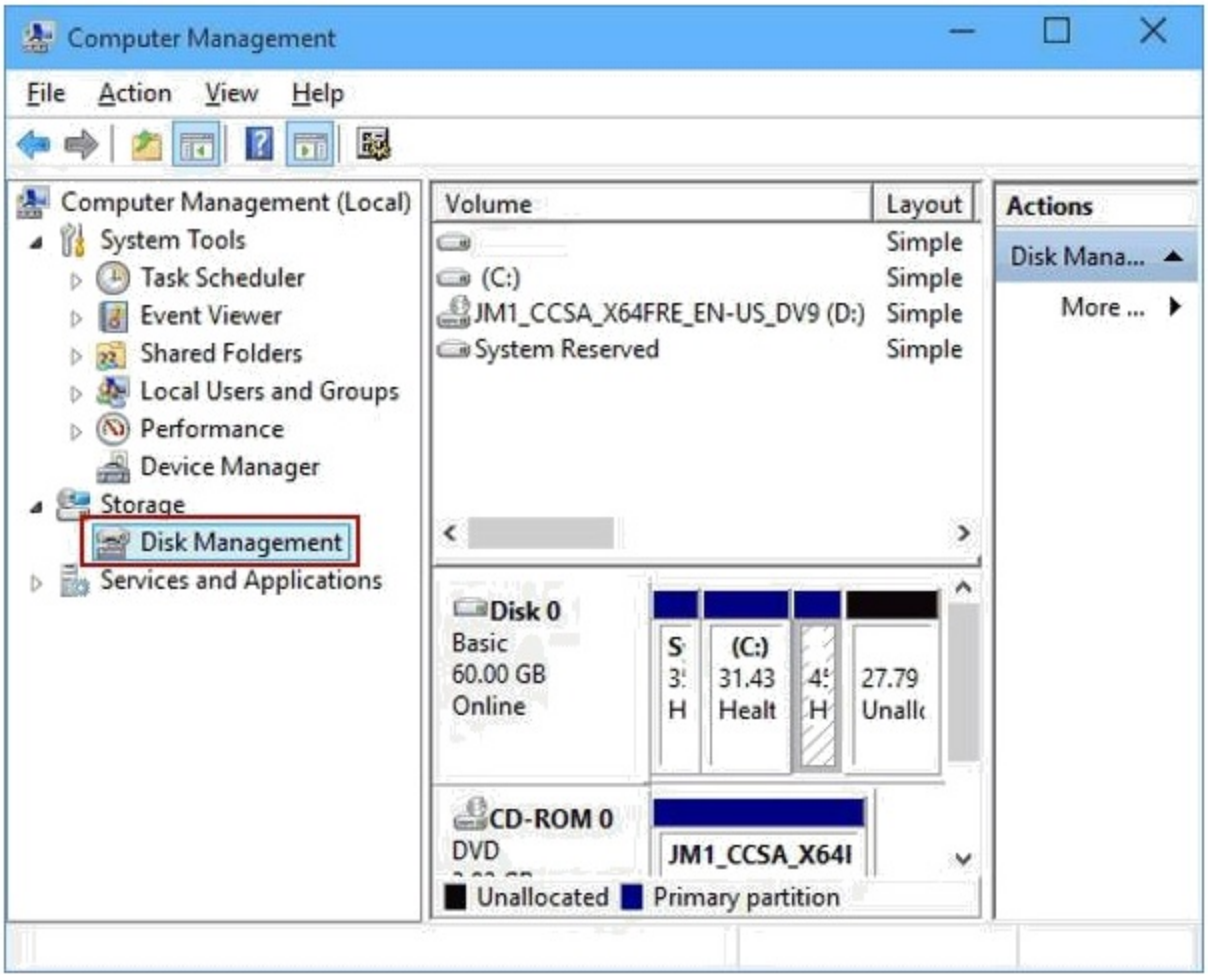
3. In the Administrative Tools window, double-click on the Computer Management icon.

4. When Computer Management opens, click on Disk Management on the left side of the window, located under Storage.

5. If you don't see Disk Management listed, you may need to click on ">" (expand icon) displayed to the left of "Storage"

6. For secondary hard disk we need to partition the drive, format and initialize the drive.

Alternatively, type “computer management” in the Windows Start menu search box, and click on the “Computer Management” search result. When Computer Management opens, click on Disk Management on the left side of the window, located under Storage. You can use Disk Management for configuring the second hard drive for data redundancy. Windows have built in functionality to set up a software RAID (Redundant Array of Inexpensive Disks) without any additional tools. This makes it easy to turn your existing spare hard drives to provide redundancy and fault tolerance.



Dynamic disks: Dynamic disks provide features that basic disks do not, such as the ability to create volumes that span multiple disks(spanned and striped volumes) and the ability to create fault-tolerant volumes (mirrored and RAID-5 volumes).

The following operations can be performed only on dynamic disks:

1. Create and delete simple, spanned, striped, mirrored, and RAID-5 volumes.

2. Extend a simple or spanned volume.

3. Remove a mirror from a mirrored volume or break the mirrored volume into two volumes.

4. Repair mirrored or RAID-5 volumes.

5. Reactivate a missing or offline disk.

Dynamic disk can create 5 types of volumes:

1. Simple volume

2. Spanned volume

3. Striped volume

4. Mirrored volume

5. RAID-5 volume.

Basic disk: Basic disk uses MBR (Master Boot Record) or GPT (GUID Partition Table) partition style to manage partitions and data on the disk. It is the most commonly used disk type in Windows.

Disk quotas

- Disk quotas are a means of controlling the storage space available on a NTFS drive or partition. By setting quotas, an administrator can set the amount of information a user can store on that drive or partition.

- Disk quotas track and control disk usage on a per-user, per-drive (partition or volume) basis. You can apply disk quotas only to NTFS formatted drives under Windows XP, Windows 7/8.1 and 10 and other Windows Server OSes. Quotas are tracked for each drive letter, even if drive letters reside on the same physical disk.

- The per-user feature enables you to track every user's disk space usage regardless of which folder the user stores files in. Whenever a user exceeds its disk quota, he or she will not be able to store new data on it. Furthermore, the administrator can also set warning levels, so that they know beforehand when a user is getting close to its quota limit.

- Disk quotas do not take compression into account, so users cannot obtain more space simply by compressing their data.

You need to remember the following when setting up disk quotas:

- In order to be able to set disk quotas and enforce quota limits, you need to use a Windows account that has administrative privileges. Standard users cannot set quotas.

- Your hard drives (or SSDs) must use the NTFS file system. On older, FAT32 formatted drives, you cannot set disk quotas.

- You can set quotas for disks or partitions. You cannot set quotas on folders.

Device Manager: The device manager lists all the hardware devices installed on your system. You can also update any existing drivers, as well as change the hardware settings. You use Add/Remove Hardware to install new hardware. Accessibility options is primarily used to configure the keyboard, display, and mouse options on a computer to accommodate the users who are physically handicapped. The Add/Remove Programs is used to install/uninstall 3rd party software. This is also used for installing/uninstalling Windows XP optional components. The Device Manager provides the status of the devices installed in the system.

Disk Defragmenter: Disk Defragmenter: Disk Defragmenter in Windows rearranges fragmented data so your disks and drives can work more efficiently. When defragmenting a disk partition, Windows rearranges the files stored on the disk so that they occupy contiguous storage locations. Doing this increases the access speed to your files by minimizing the time required to read and write files to/from the disk and by maximizing the transfer rate. You might also see improved startup times. If you use a disk drive that was previously configured as a dynamic drive in another computer, it may show up as foreign drive. You need to import the foreign drive to show up in the device manager as local.

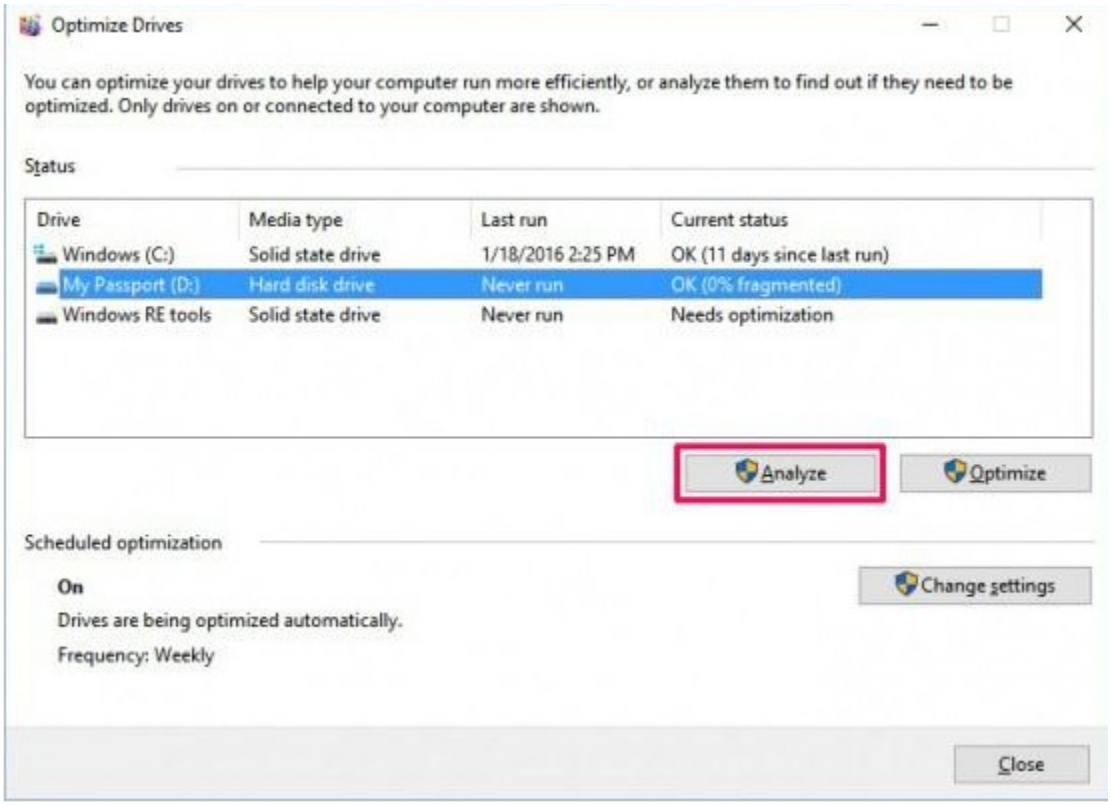
You use Disk Defragmenter to analyze and defragment disk volumes. The easiest way to start disk defrag is to type “defragment” in the search box, and select "Disk Defragmenter" option.

In Windows 8.1/10, it is called by slightly different name: "Defragment and Optimize

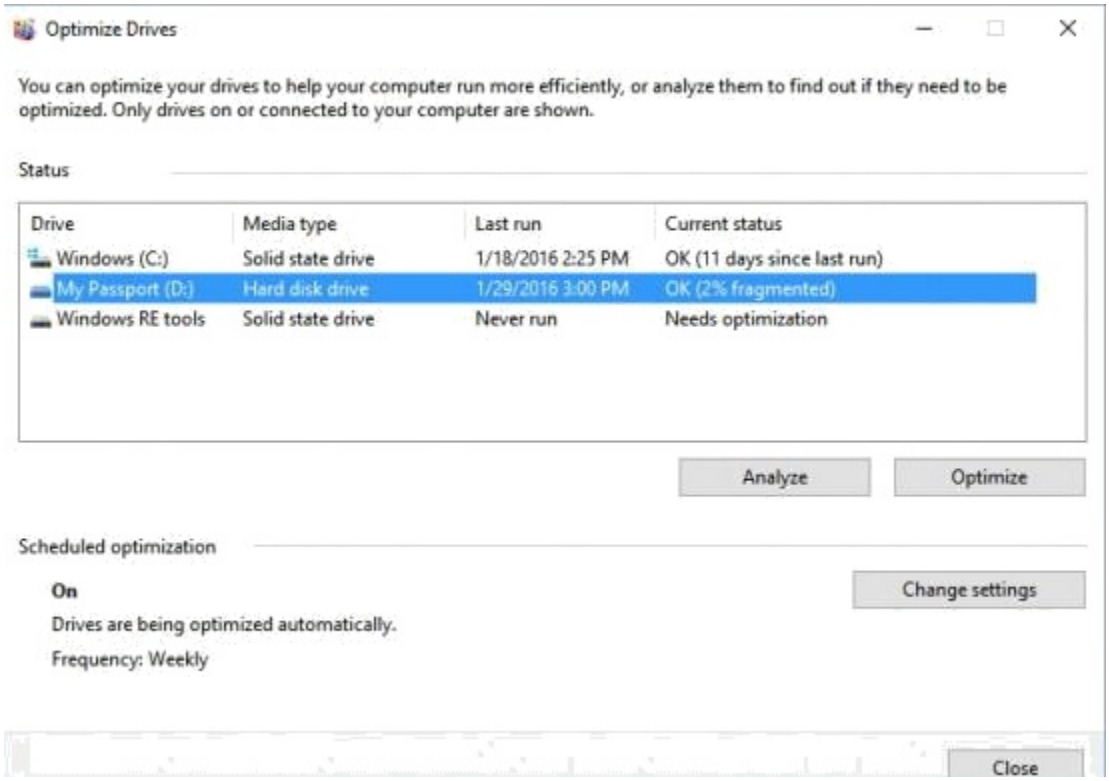
Drives" **How to Defrag Your Hard Drive in Windows 10**

1. Open the disk optimization tool by searching for "optimize" or "defrag" in the taskbar.

2. Select your hard drive and click Analyze. Note that if you have a SSD, this option is grayed out and not available.

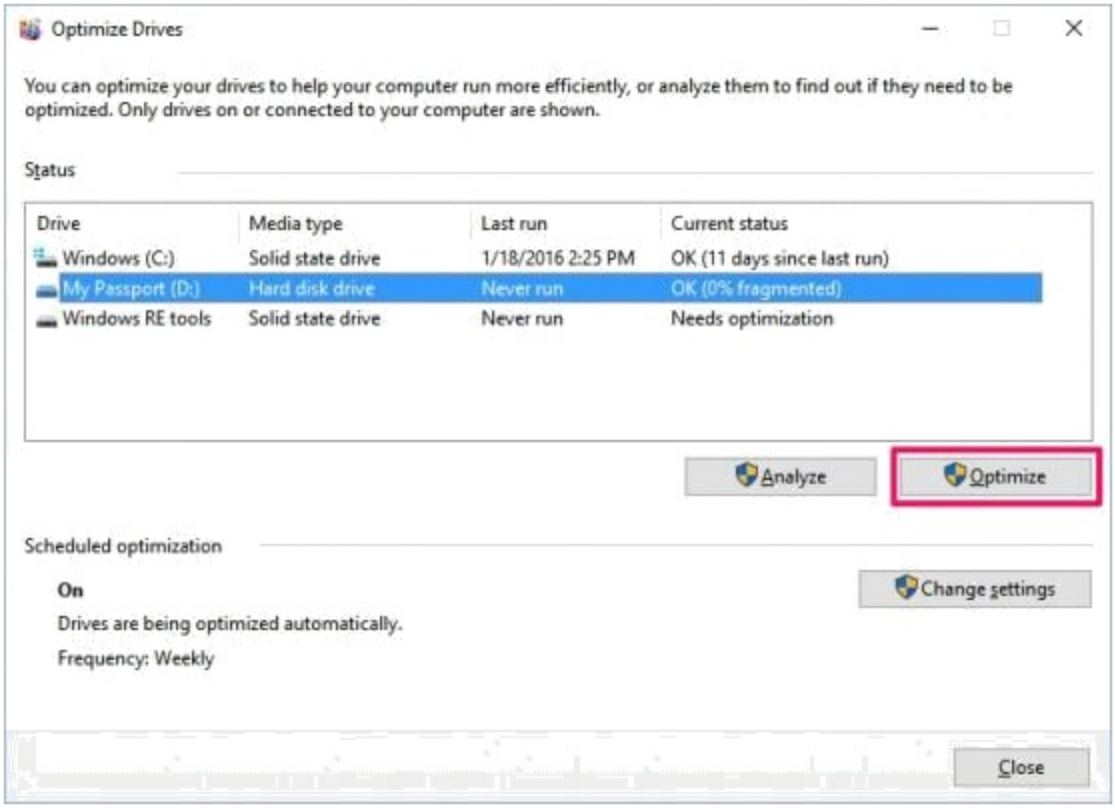


3. Check the percentage of fragmented files in the results.



4. If you want to defragment your drive, click Optimize. It's best to do this when you don't need to use your computer for anything else, so you can let Windows defragment the drive efficiently. If the files stored on your PC's hard drive are scattered everyone and defragmentation is needed, then click the Optimize button. Once the process complete, the current status should display "0% fragmented".

Note: You always want to analyze the drive first to figure out if the drive needs optimization. If the result shows less than 10% fragmented, you probably don't need to optimize the drive.



Do not defragment SSDs or USB drives. These types of drives have a different way of allocating files and they have a limited number of read/write cycles before they stop working. Hence, defragmenting them will decrease their lifespan. Given the high read and write speeds provided by SSDs, you shouldn't encounter slowdowns anyway, so there's no reason to defragment them

Note: Keep in mind that depending on the number of files, the size of the drive, and fragmentation, the defragmentation tool may take some time to complete the task. It's also recommended to perform this task when you know, you won't be around your computer.

DirectAccess: It is a welcome addition to Windows 7 for any user who connects to a corporate VPN. Rather than input all the credentials manually, DirectAccess now streamlines the process of securely connecting to a corporate network. It also maintains that secure connection throughout the process, ensuring that no data leaks out during the transmission.

Applocker: AppLocker is a useful tool for IT admins. The software gives administrators the opportunity to decide exactly what applications users can run on the network. It's a great way for the IT department to maintain some control over the security of employee computers.

B**ranchcache:** BranchCache is a new feature of Microsoft Windows 7 designed specifically for businesses that operate from multiple office locations. It provides a file caching service for professional network administrators to use at their branch offices. The main purpose however is to decrease the time branch office users spend waiting to download files across the network.

Bitlocker: Windows 7 users can have more control over the encryption of their hard drives. Using BitLocker Drive Encryption is one of the best ways to protect portable systems such as laptops from loss of data and information when the laptops themselves are lost or stolen. Microsoft's BitLocker automatically encrypts new data while it's running and it is considered as a hands-off tool that should improve security in Windows 7.

MSCONFIG: One use of this utility is that you can identify the startup programs, and remove those that are not required to be loaded at the startup. By doing this, you can improve the speed of the system.

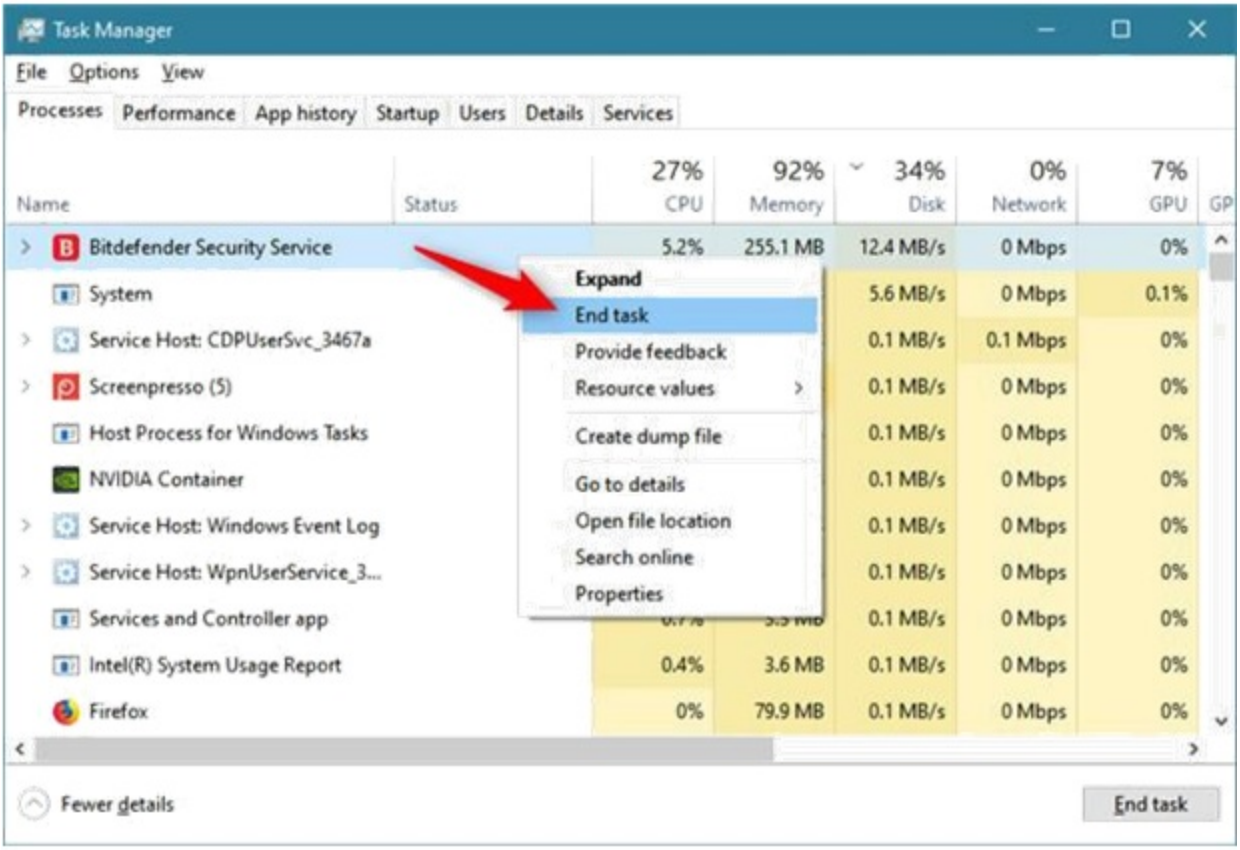
REGEDIT: Windows OS provides a Registry Editor by name “regedit.exe”. You can also call this program by giving the command “regedt32.exe”.

1. Regedt32.exe (32-bit) and

2. Regedit.exe (16-bit).

Regedt32.exe is automatically installed in the systemroot\system32 folder, while Regedit.exe is automatically installed in the systemroot folder. Regedit.exe is primarily used for its search capabilities as it doesn't support all functions and data types.

Task manager: CTRL-ALT- DELETE opens Task Manager window in which you can select the offending program, and then click "end task". The screenshot of Task Manager window is shown below



You need to right click on the short-cut, select “properties”. Then, select short-cut tab. You can click on change icon button, to change the icon of a short-cut.

If Microsoft Windows Firewall is blocking a port that is used by a service or by a program, you can configure the Windows Firewall to create an exception. Windows Firewall may be blocking a program or a service if the following conditions are true:

- Programs do not respond to a client's request.
- Client programs do not receive data from the server.

Startup Repair tool: The Startup Repair tool is automated and used to diagnose and recover systems that do not start. It is automatically installed onto the operating system partition. After an unsuccessful start, Windows 7 automatically loads the Startup Repair tool which scans the computer for issues, automatically repairs an issue when it is possible, and then restarts the computer.

System Configuration (msconfig): msconfig is a tool that can help to identify problems that might prevent Windows from starting correctly. The following are the options that are available in System Configuration.

The command ATTRIB C:\private.txt +h +r will mark the file as hidden and read only

- General: Lists choices for startup configuration modes
- Boot: Shows configuration options for the operating system and advanced debugging settings,
- Services: Lists all of the services that start when the PC starts, along with their current status
- Startup: The Startup tab in Task Manager lists apps and services that run when the PC starts up, along with the name of their publisher, status, and startup impact.

Tools: Provides a convenient list of diagnostic tools and other advanced tools that you can run. Windows 7, Windows 8 and windows 10, uses a boot manager (bootmgr.dll) which consults with the BCD(in Boot folder) to locate the boot loader (winload.exe). “Bootmgr.dll” is a hidden system file and it is located generally in the root directory of C:\ drive By editing bootmgr.dll we may change boot configuration.

CONFIG.SYS is a text file containing DOS (Disk Operating System) commands that tell the operating system how the computer is initially set up.

Windows memory diagnostics: You can use Windows Memory Diagnostic to investigate RAM problems in Windows 7. If you're encountering application failures, operating system faults, or Stop errors, you could have defective or failing RAM. The Windows Memory Diagnostic Tool in Windows 7 can help you to test the RAM chips in your system. It is possible to use the tool without any operating system installed. You can use the optical drive to use the tool. Note that the BIOS also has the capability to test the memory, but it is very basic test. The WMD reports are very comprehensive, and tests the RAM thoroughly.

MMC(Microsoft Management Console): Windows Performance Monitor is a Microsoft Management Console (MMC) snap-in that combines the functionality of previous stand-alone tools including Performance Logs and Alerts, Server Performance Advisor, and System Monitor. It provides a graphical interface for customizing Data Collector Sets and Event Trace Sessions.

Windows Performance Monitor enables you to track the performance impact of applications and services, and to generate alerts or take action when user-defined thresholds for optimum performance are exceeded. Windows Vista includes Windows Reliability and Performance Monitor, which is a Microsoft Management Console (MMC) snap-in that combines the functionality of previous stand-alone tools. It also includes Reliability Monitor, an MMC snap-in that tracks changes to the system and compares them to changes in system stability, providing a graphical view of their relationship.

Windows Vista introduces Sync Center, which enables users to synchronize their data with other computers and devices from one common user interface. There are several ways to interact with Sync Center, one of which is as a provider of synchronization information. Synchronization information consists of a synchronization engine, and the data that it synchronizes.

In windows 7, Sync Center allows you to check the results of your recent sync activity if you've set up your computer to sync files with a network server (often called offline files). When you sync with a network server, you can access files by keeping synced copies of those files on your computer, even when the network server is unavailable. Sync Center can tell you if the files synced successfully or if there are any sync errors or warnings. To launch sync center, just open your control panel, then click sync center.

Following are the important points about MSINFO32

1. System Information (also known as msinfo32.exe) shows details about your computer's hardware configuration, computer components, and software, including drivers.

2. Open System Information by clicking the Start button. In the search box, type “msinfo” (or System Information), and then, in the list of results, click “msinfo.exe” (or System Information, if you had typed it in the search box).

3. System Information lists categories in the left pane and details about each category in the right pane.

4. System Summary displays general information about your computer and the operating system, such as the computer name and manufacturer, the type of basic input/output system (BIOS) your computer uses, and the amount of memory that's installed.

5. Hardware Resources displays advanced details about your computer's hardware, and is intended for IT professionals.

6. Components displays information about disk drives, sound devices, modems, and other components installed on your computer.

7. Software Environment displays information about drivers, network connections, and other program-related details.

8. To find a specific detail in System Information, type the information you're looking for in the Find what box at the bottom of the window. For example, to find your computer's Internet protocol (IP) address, type IP address in the Find what box, and then click Find.

Task scheduler: You may open the task scheduler as below:

1. Open the Control Panel.

2. Open the Administrative Tools window.

3. In Windows 7, look under System and Security.

4. In Windows Vista, under System and Maintenance.

5. Open the Task Scheduler icon.

6. If prompted, type the administrator's password or click Continue.

The Task Scheduler window appears , now, you can select a new task from the menu Action -> Create Task. Various tabs are as given below:

1. Triggers Tab: A trigger is an event that prompts a task to run. It can be a time of day or it can be an action, such as system startup.

2. Actions tab: An action is what a task does run a program, display a message, or make another thing happen, set a restore point, defragment the hard drive, or send an email message, for example. Yes, the action shown for setting a restore point is technical. But keep in mind that you're viewing a Windows task. The tasks you set up will not be as complex.

3. Conditions tab: The settings on the Condition tab refine when the task is run. The task doesn't run unless all the conditions are met.

4. Settings tab: The Settings tab lists further control over the task, including when to stop a task that might run amok.

5. History tab: You find on the History tab some information about when the task was last run and whether it ran successfully. That's your way to test whether your tasks are doing what you set them to do.

Features

1. Spanned volumes:

To create a spanned volume using the Windows interface

1. In Disk Management, right-click the unallocated space on one of the dynamic disks where you want to create the spanned volume.

2. Click New Spanned Volume.

3. Follow the instructions on your screen.

To create a spanned volume using a command line

1. Open a command prompt and type diskpart.

2. At the DISKPART prompt, type list disk. Make note of the number of the disk where you want to create a simple volume.

3. At the DISKPART prompt, type create volume simple [size=] [disk=].

4. At the DISKPART prompt, type list volume. Make note of the number of the simple volume you want to extend onto another disk.

5. At the DISKPART prompt, type select volume . Select the simple volume “volumenumber” you want to extend onto another disk.

6. At the DISKPART prompt, type list disk. Make note of the number of the disk you want to extend the simple volume onto.

7. At the DISKPART prompt, type extend [size=] [disk=]. Extends the selected volume onto disk “disknumber” and makes the extension size=size megabytes (MB).

2. Language settings: You can use Region and Language to support additional languages on your Windows 7 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.

3. Registry: The Registry contains the important information about the devices and applications. Any failure to backup the registry may require re-installation of the complete system.

4. 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

To connect a USB device

- 1. The OS should support USB.
- 2. The USB should be enabled in the BIOS

If both the above conditions are met, USB Controller is listed in the Device Manager. If it's not listed in the Device Manager, you can suspect that the USB was not enabled in the BIOS.

Previous Contents Next

CompTIA®A+ Core 2 Exam Notes : Important Windows Control Panel Utilities

examguides.com/Aplus-Core2/aplus-core2-5.htm

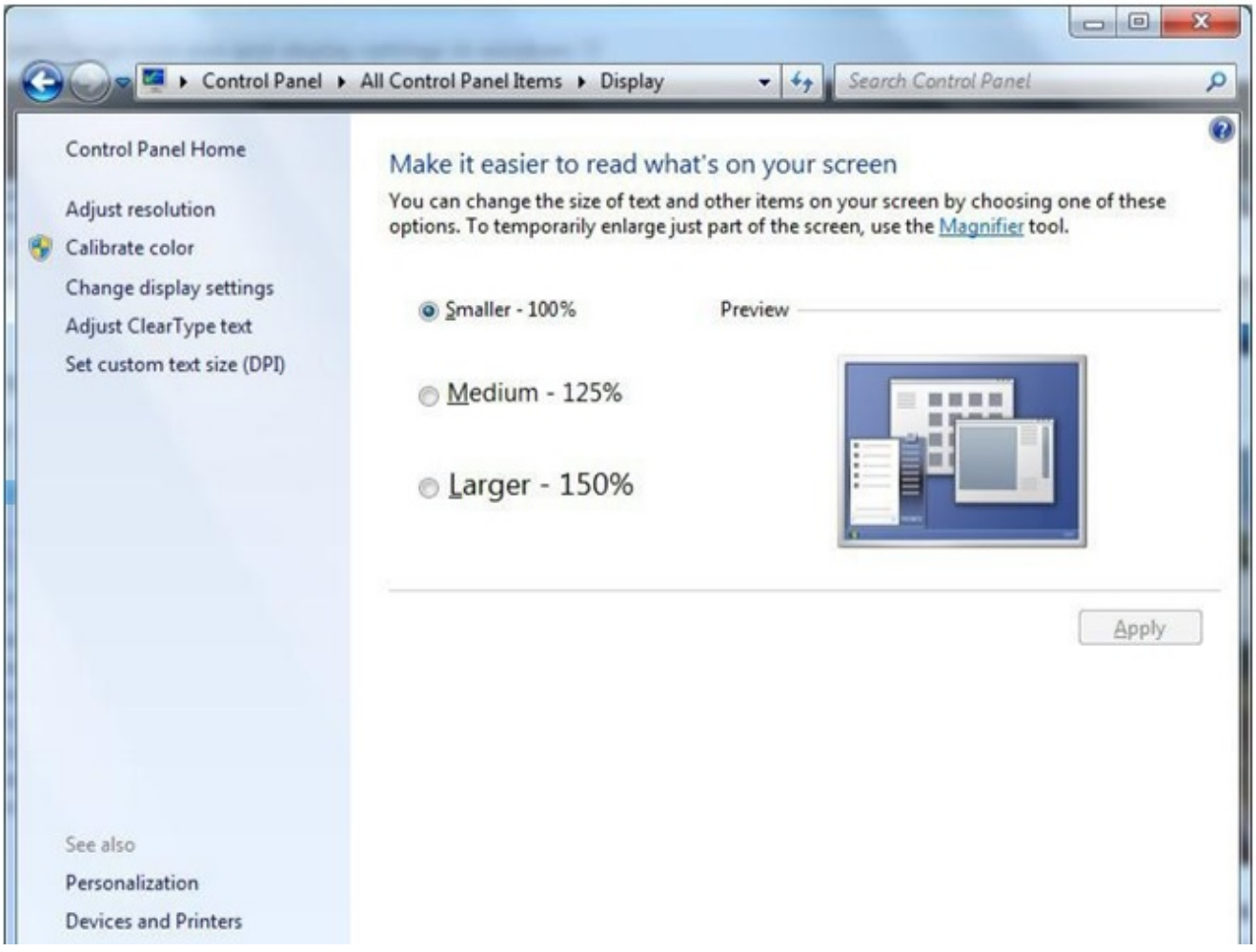
1. Windows Operating Systems

1.5 Important Windows Control Panel utilities

Display Settings: Changing the display settings in windows 7

1. In Windows, click Start, click Control Panel, then click Display.

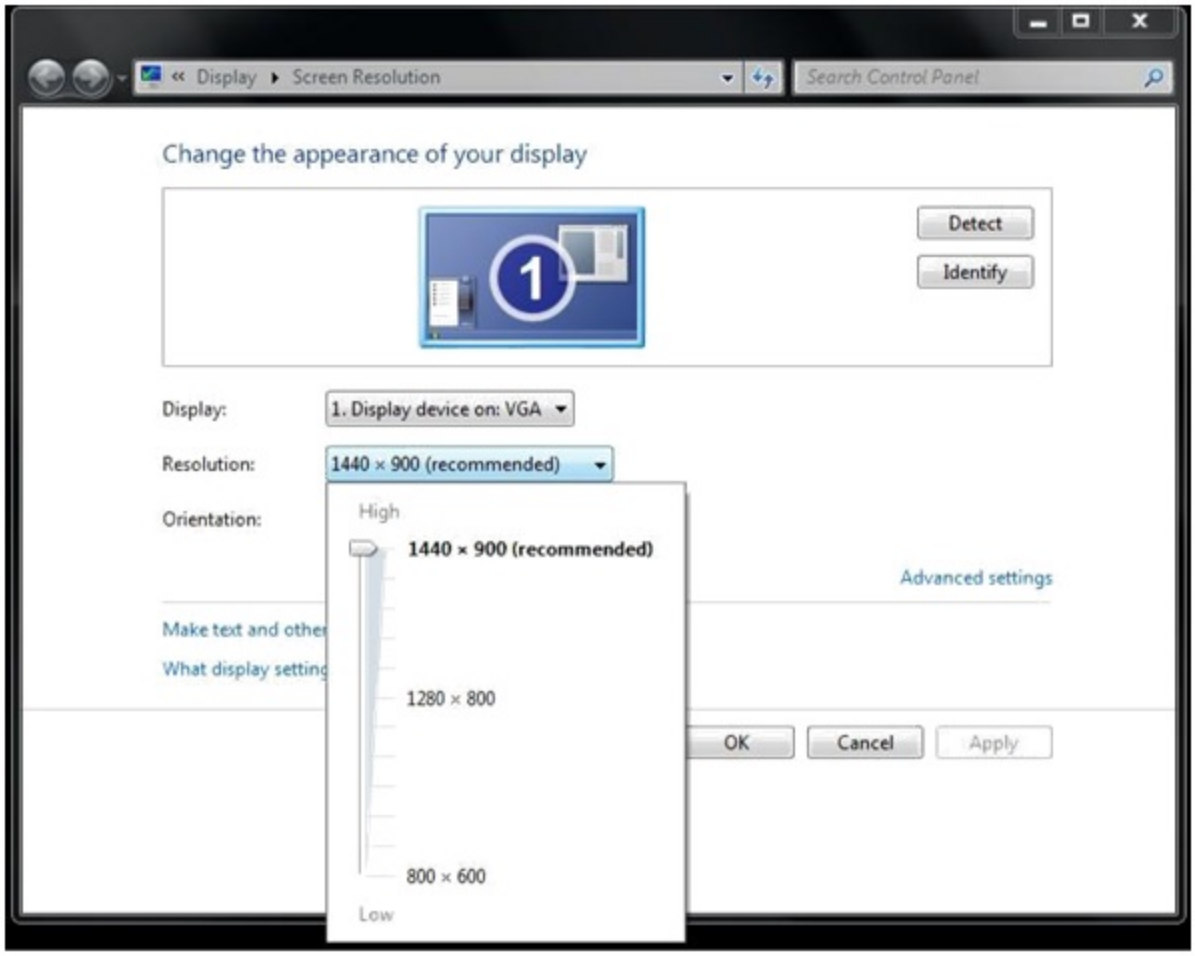
2. To change the size of text and windows, click Medium or Larger, then click Apply. The screenshot is shown below



Screen Resolution: To change screen resolution in windows 7

1. Right-click the desktop and click Screen resolution.

2. Click the image of the monitor that you want to adjust.

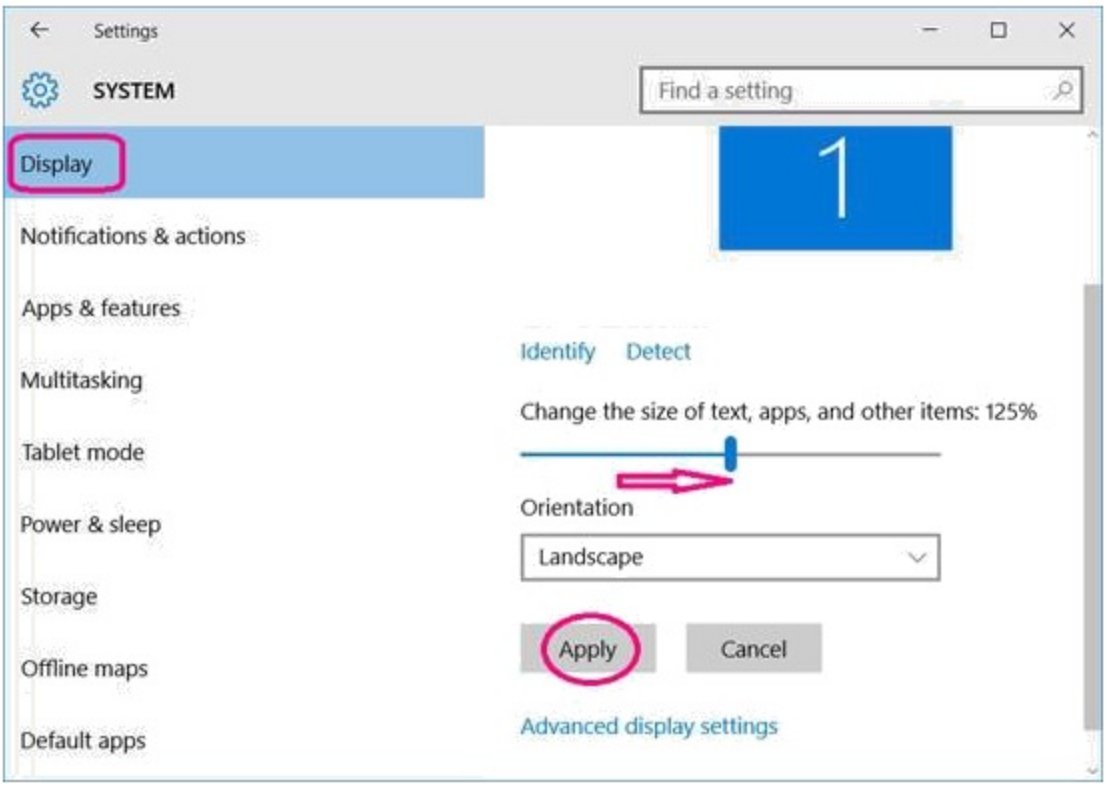


Changing the display settings in windows 10

1. Right-click on desktop screen, select "Display settings".

2. To customize your display.

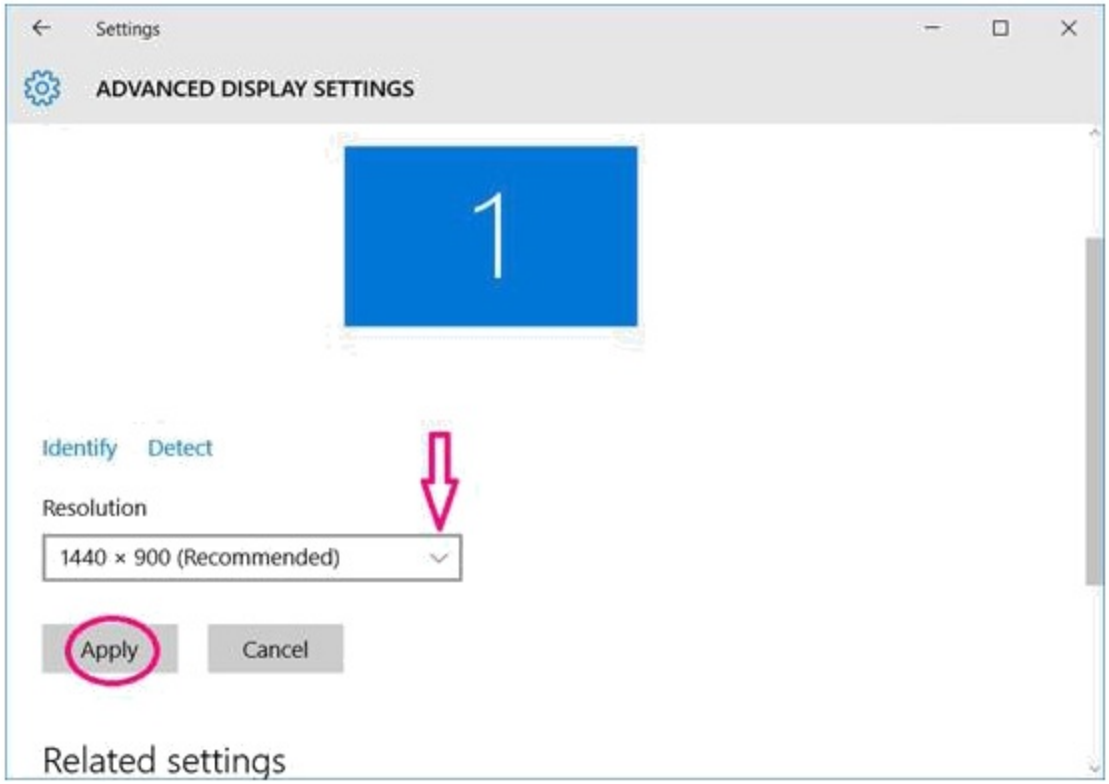
- Below "Change the size of text, apps, and other items", there is a slider.
- Move the slider to the right, the size of text, apps, and other items would be turned to larger.
- And then click on "Apply" button to apply the changes. The screenshot is shown below



Changing screen resolution in windows 10

1. Click on "Advanced display settings" on the bottom.

2. Select the appropriate resolution, and click on "Apply" to save the change. The screenshot is shown below



When the screen resolution is set to very low, then the text size becomes larger, and sometimes it may result in some portions of the text not viewable. Set the screen resolution properly using the properties window. Refresh rate results in screen flickering (if the refresh rate is too low), and nothing to do with resolution.

Configuring Multiple displays

1. To configure multiple displays on Windows 7

1. Click "Start" button -> Control Panel -> Appearance and Personalization -> Personalization ->Display Settings

2. To configure multiple displays on Windows 10 :

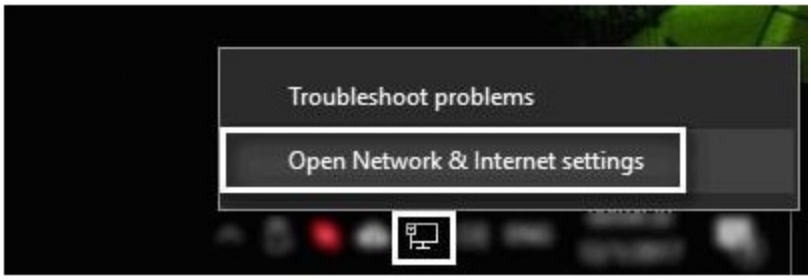
1. Right-click on desktop, click Personalize option to open Personalization section of Settings app

2. On the left-pane, click Themes to see Themes and Related settings.

3. Finally, click Classic theme settings link to open the classic Personalization window.

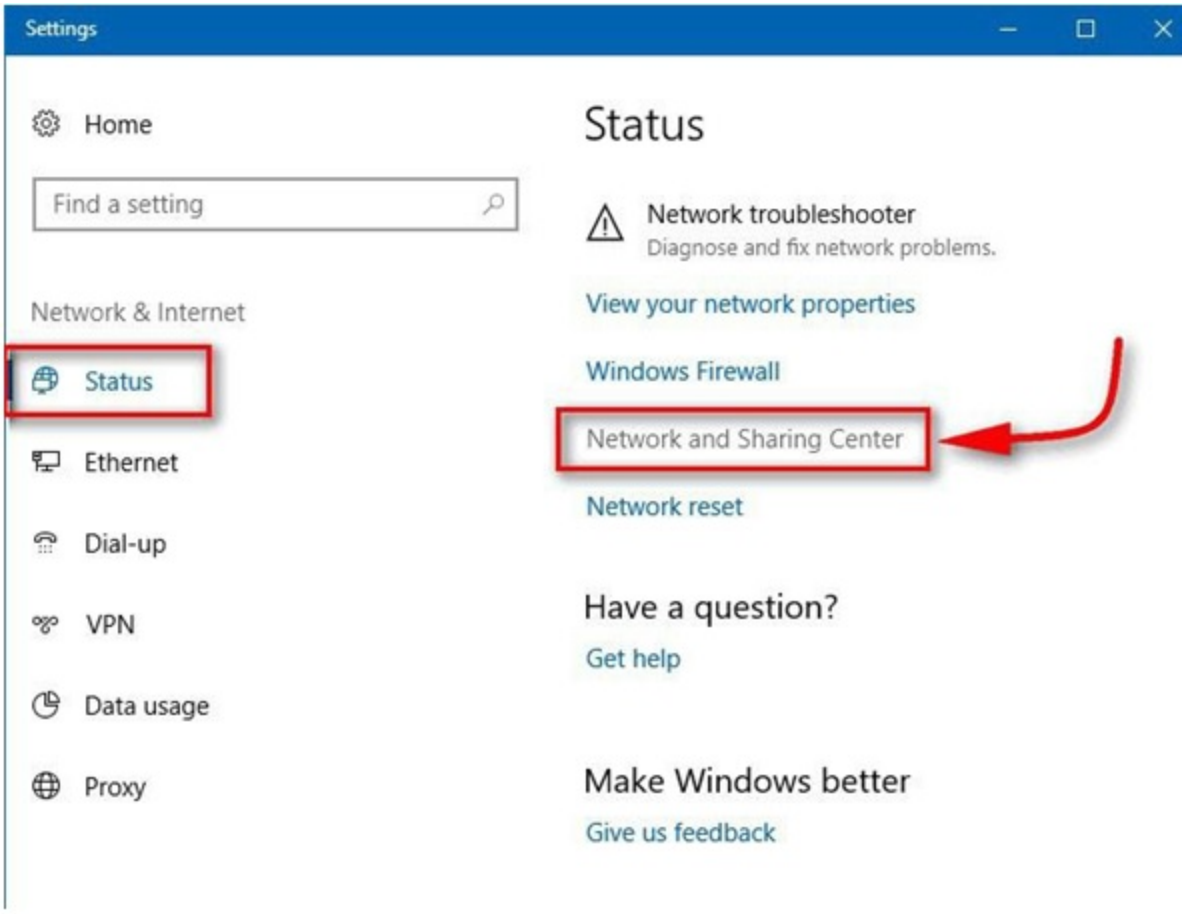
Network and Sharing Center applet: This will enable a user to configure his network connections. To open the applet perform below steps

1. Right-click the network icon in the Taskbar.



2. Select “Open Network and Internet settings”

3. Now scroll down and click on the link named “Network and Sharing Center”



Reconnect at Logon: You can select Reconnect at Logon for reconnecting to a network drive at logon.

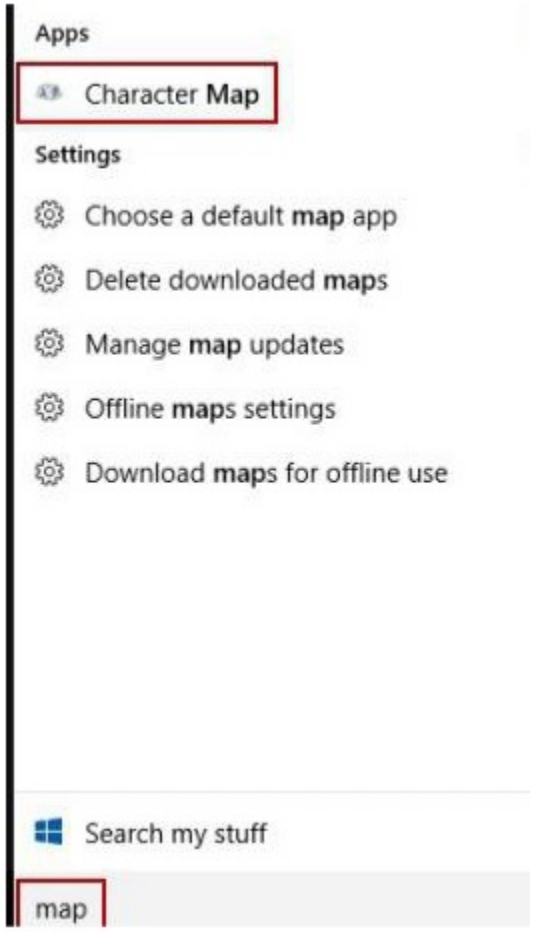
Character Map: You can use Character Map to copy and paste special characters into your documents, such as the trademark symbol, special mathematical characters, or a character from the character set of another language. To open character Map

To open character map in windows 10

Way1: Access it by searching.

1. Type map in the search box on taskbar, and choose Character Map from the result. The screenshot is shown below

Way 2: Turn it on in Start Menu.

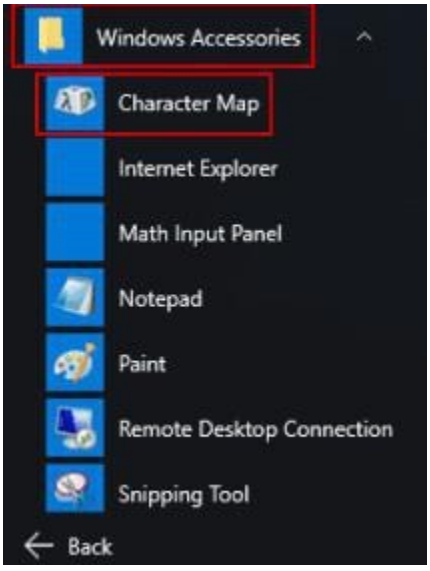


1. Open Start Menu, choose All apps, expand Windows Accessories and hit Character Map

Privacy screen or privacy guard: Privacy screen or a privacy guard protects the sensitive information on your screen while also protecting the screen itself from scratches and damage. It is useful when traveling or in public place in preventing prying eyes from seeing what's on your laptop screen. And it's thin enough that it still allows your laptop to close and latch.

To uninstall a application: You can use Programs applet in the Control Panel to add or remove a program. Programs and Features is the place to go in the Control Panel (CP) to remove an application in Windows7.

To uninstall apps in windows 10: You can uninstall both apps and traditional desktop programs directly from the Settings menu in windows 10. To do this, you need to do the following:



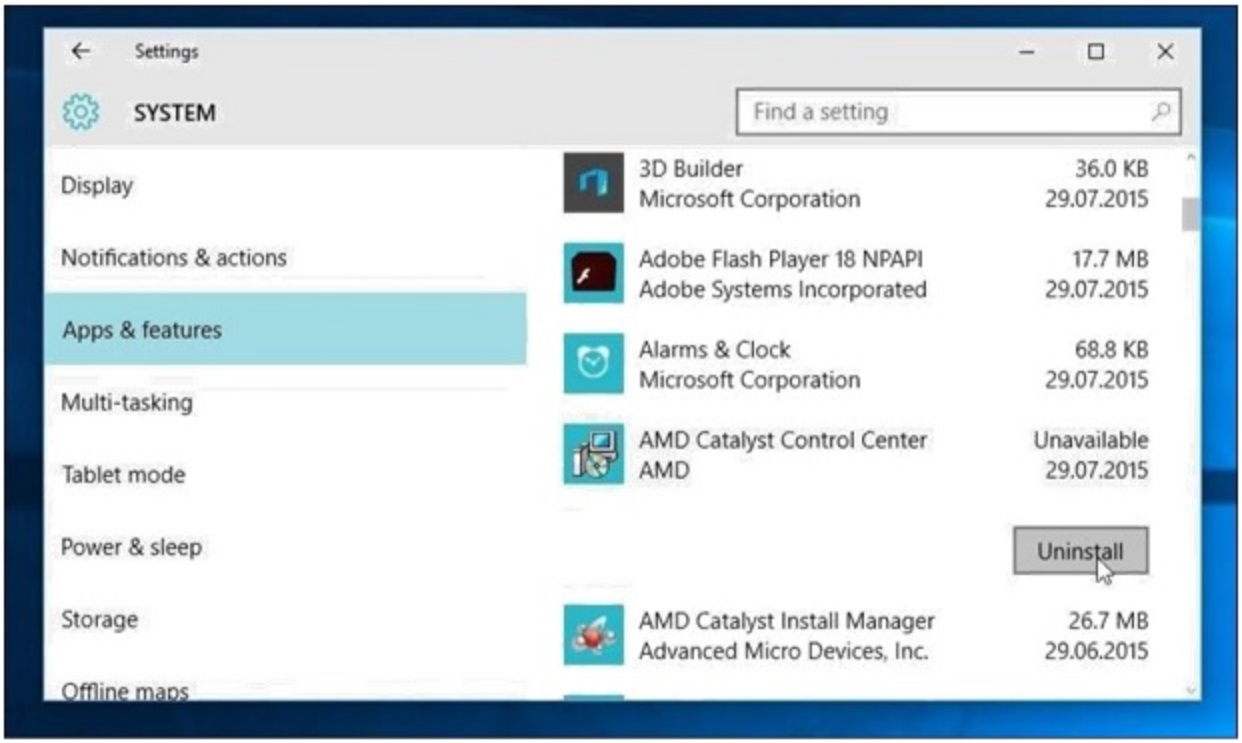
1. Open the Start menu.

2. Click Settings.

3. Click System on the Settings menu.

4. Select Apps & features from the left pane.

5. The Apps and Features display all the installed apps on your PC. These applications can also be sorted on the basis of their size. Locate the application you wish to uninstall and click on the Uninstall button. You will be prompted with a message saying "this app and its related info will be deleted", click Uninstall to delete the programs in Windows 10.



You can enable memory dump to a file when your system is about to crash due to Stop Error (such as Blue Screen)

The following types of memory dumps are available with Windows 8/8.1/10

1. Complete memory dump: A complete memory dump is the largest type of possible memory dump. This contains a copy of all the data used by Windows in physical memory.

2. Kernel memory dump: A kernel memory dump records only the kernel memory. This speeds up the process of recording information in a log when your computer stops unexpectedly. You must have a pagefile large enough to accommodate your kernel memory.

3. Small memory dump (256 KB): It contains the blue-screen information, a list of loaded drivers, process information, and a bit of kernel information. It can be helpful for identifying the error.

4. Automatic memory dump: This is the default option, and it contains the exact same information as a kernel memory dump.

You can open Windows Update in any of the following ways to check for latest help files or updated drivers:

1. Click Start | Control Panel | System and Security | Windows Update

2. Click Start | Control Panel | Windows Update

3. Type "Windows Update" on Start menu Search

4. Right-click Action Center | Open Windows Update on the notification area

5. After opening Windows Update, click "Check for updates" on the left pane

Windows 7 provides Windows Update through Control Panel > Windows Update. However, Windows 8 and Windows 8.1 provide access to Windows Update app through both Control Panel and PC Settings app. In Windows 10, to access Windows update feature, select the Start button, select Settings > Update and security > Windows Update. Ctrl+Esc will pop-up Start menu in Windows 7.

To view Hidden files in Windows 7: On your Windows 7 computer, you can use the View tab in Folder Options of Appearance and Personalization applet in the Control Panel to show / hidden files and folders that have "Hidden" attribute set. You can also use Windows Explorer -> Organize -> Folder and Search Options -> View tab.

To view Hidden files in windows 10: By default, Microsoft Windows 10 hides certain files from view when you explore them on your hard drive. This protects important files from being deleted so that the system isn't damaged. If you want to view all files all the time. Follow these steps to show hidden files.

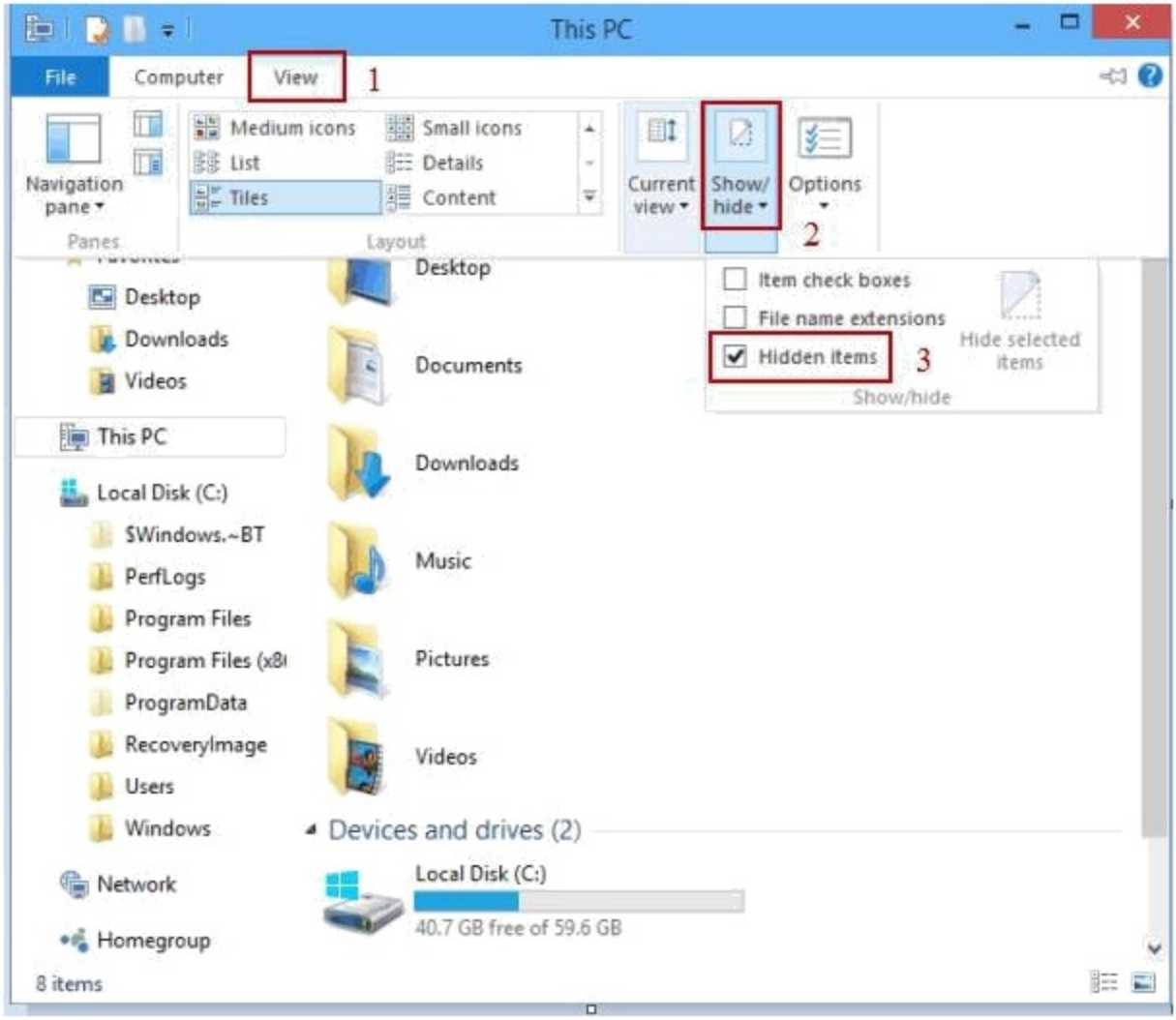
Option1: From File Explorer

1. Select the "Start" button, then choose "File Explorer".

2. Make sure the menu bar is expanded. You can toggle the menu bar by selecting the ^ at the upper right portion of the window.

3. Select the "View" tab and Check the "Hidden items" check box to view hidden items.

4. If you need more file viewing options, select "Options" > "View".



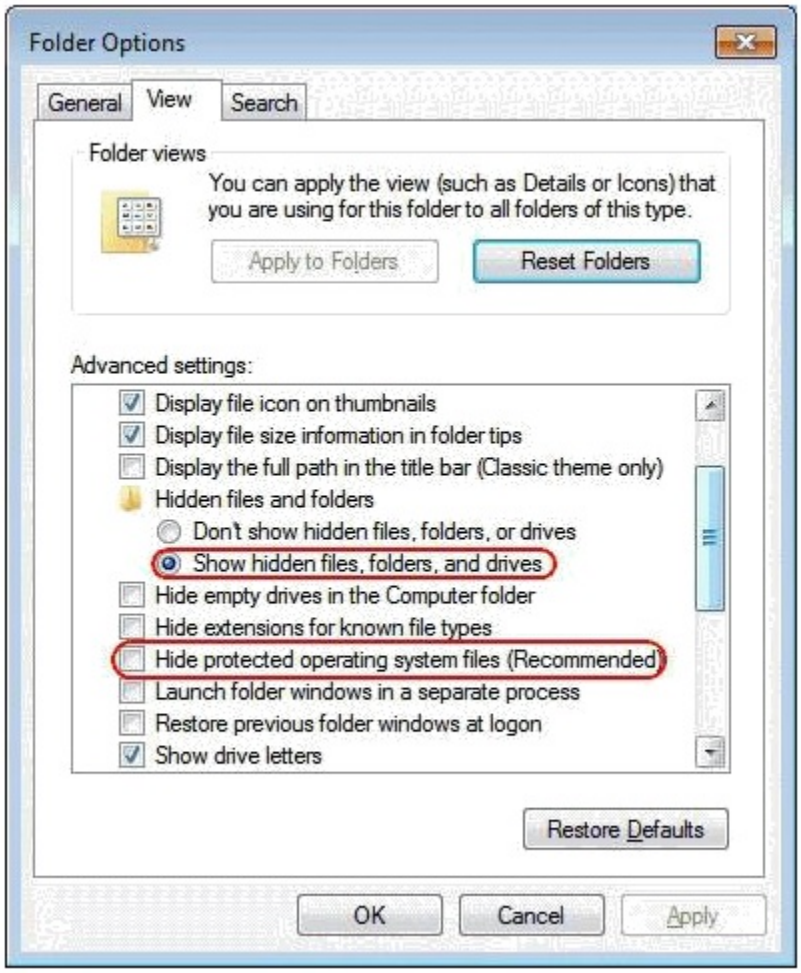
Option2: From Control Panel

1. Right-click the "Start" button, then select "Control Panel".

2. Go to "Appearance and Personalization", then select "File Explorer Options".

3. Click the "View" tab.

4. Scroll down a bit and change the "Hidden files and folders" setting to "Show hidden files, folders, and drives". Optionally, you may wish to uncheck the "Hide protected operating system files" box as well.



Power Options:

Sleep mode: It is a power-saving state that is similar to pausing a DVD movie. All actions on the computer are stopped and any open documents and applications are put in memory. You can quickly resume normal, full-power operation within a few seconds. Sleep mode is basically the same thing as “Standby” mode. The Sleep mode is useful if you want to stop working for a short period of time. The computer doesn’t use much power in Sleep mode. In Sleep mode, any open documents and applications are put in memory while the computer goes into a low -power state. The computer technically stays on, but only uses a smaller of power, and the LED screen will also be off. You can quickly resume normal, full-power operation within a few seconds. Sleep mode is basically the same thing as "Standby" mode. Sleep mode is useful if you want to stop working for a short period of time.

Hibernate mode: Saves your open documents and running applications to your hard disk and shuts down the computer, which means once your computer is in Hibernate mode, it uses zero power. Once the computer is powered back on, it will resume everything where you left off. Use this mode if you won’t be using the laptop for an extended period of time, and you don’t want to close your documents. Hibernate mode is very similar to sleep, but instead of saving your open documents and running applications to your RAM, it saves them to your hard disk. In other words, Hibernation mode stores the current session on to the hard disk,

and resumes the current session when the computer is switched on. This allows your computer to turn off entirely, thus saving power. Once the computer is powered back on, it will resume everything where you left off. This mode is useful if you don't want to close your documents when you are away for longer periods of time, and would like to continue where you had left off. Hibernate saves an image of your desktop, including all open windows and files. Then it powers down your computer just as if you had turned it off. When you turn your computer on again, your windows and files are open just as you left them.

Stand by: It is a mode the computer, monitor, or other device enters when idle for too long. This mode helps conserve power when a computer or computer device is not in use without having to sacrifice the time it would take to turn off and on the computer. When in Stand by, the computer or monitor has a solid or flashing amber light, indicating that there is still power but the computer is in Standby mode. When you select Standby, the power to your screen, hard drive, and peripheral devices is cut. However, the power to the computer's memory (RAM) is maintained so your open files stay open. Shutdown basically shuts down your computer completely. If you are going to be away from your computer for an extended time or overnight, putting your system into hibernate mode puts your system into an even deeper sleep than Standby mode and is essentially just short of a complete shutdown.

You can also change the amount of time before your computer goes into sleep or hibernate mode, or turn off each mode completely. To configure any of the power options, you first have to go to Start, then Control Panel, and then click on Power Options.

In the Power Options properties dialog, there are six tabs: Power Schemes, Alarms, Power Meter, Advanced, and Hibernate.

In the Advanced tab you will be able to configure the action that would take place when the laptop lid is closed.

In Windows 7, the Sleep and Hibernate options are accessed using the arrow button next to the Shut down button on the Start menu.

You can set the password policy using Local Security Policy option. Follow following steps to Open "Local Security Policy":

1. Click the Start button and type “secpol.msc” into the Search box.

2. Click secpol [Note: Administrator permission required i you are prompted for an administrator password or confirmation, type the password or provide confirmation].

3. In the Navigation pane, double-click "Account Policies".

4. Click on "Password Policy" in right pane. - F

You can also go there using Administrative Tools option in Control Panel, then clicking on Local Security Policy option.

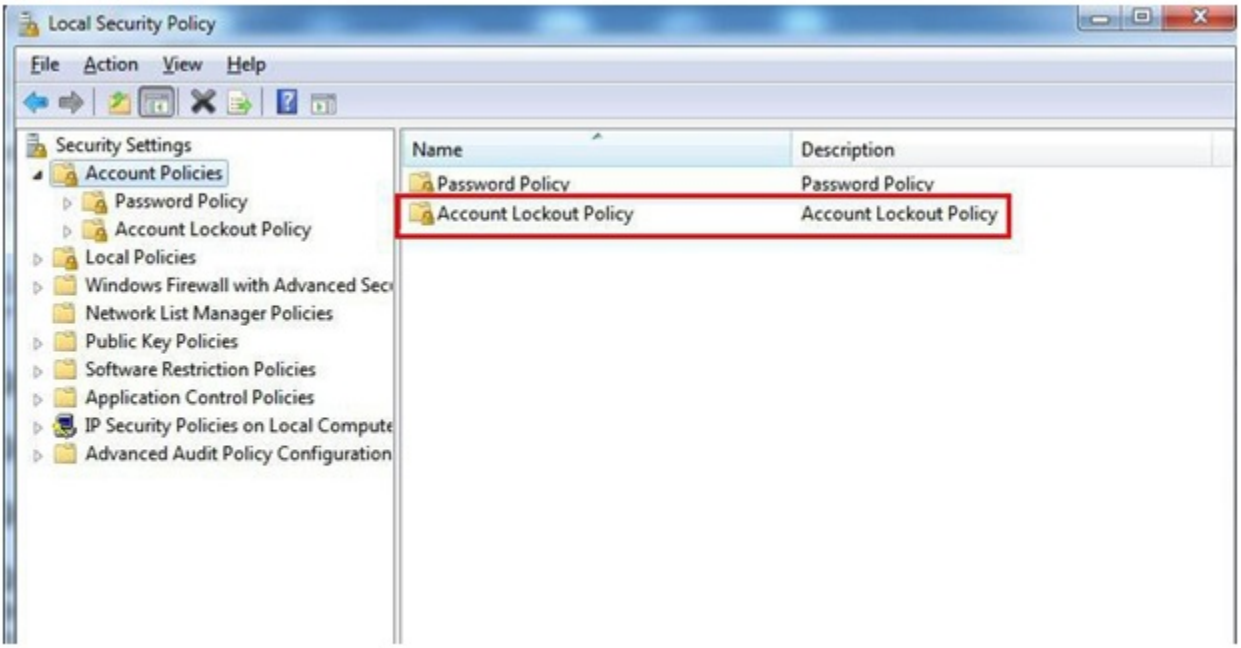
Changing account lockout policy

1. Open the Control Panel (icons view), and go to Administrative Tools.

2. In the right pane, double click on Local Security Policy to open it.

3. You can now set and manage the Local Security Policies on your computer as per your requirement.

This file is located at C:\Windows\System32\secpol.msc. (See screenshot below)



POST test card: A POST test card is a small diagnostic tool that displays error codes generated during the Power On Self Test. These errors, called POST codes, correspond directly to a test that has failed and can help determine what piece of hardware is causing an issue. Most POST test cards plug directly into expansion slots in the motherboard while a few others connect externally via a parallel or serial port. Also Known As: Power On Self Test card, POST card, POST diagnostic card, checkpoint card, port 80h card

Color Depth: Given below are some commonly used color depths and the number of bits required to store the color information per pixel:

1 bit (mono): 2 colors
2 bits: 4 colors
4 bits: 16 colors
8 bits: 256 colors
16 bits: 64K colors
24 bits: 16.7M colors

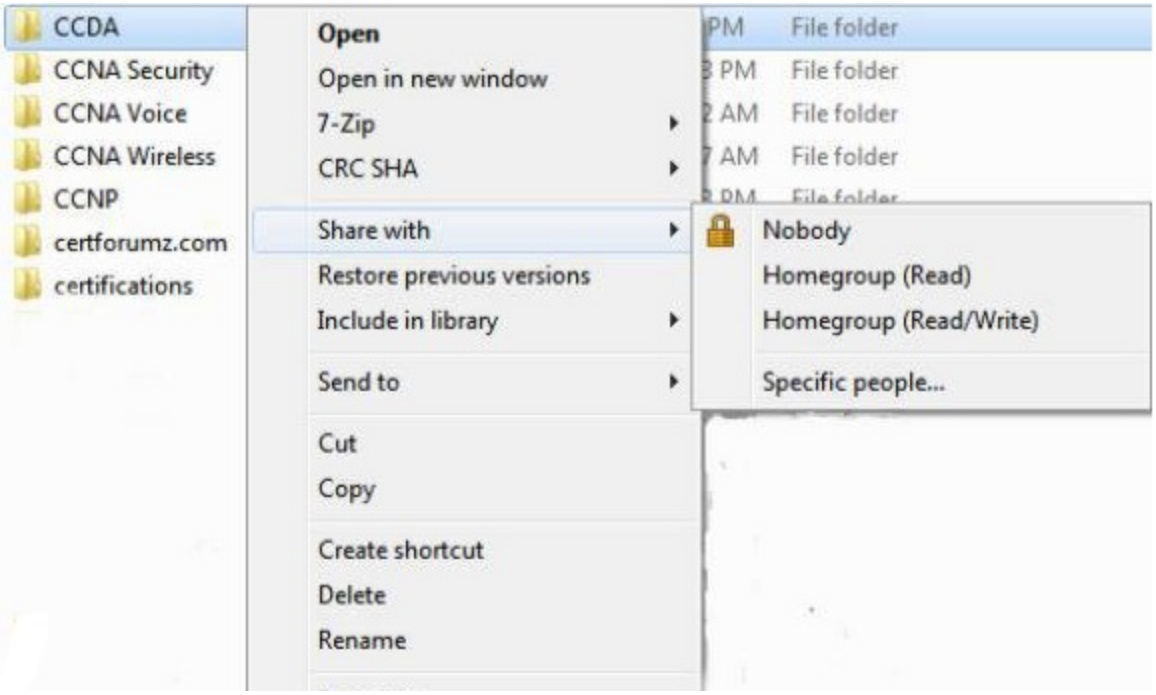
The following are the important characteristics of Windows HomeGroups:

1. HomeGroup computers connect to one another by a using a common password. You can access HomeGroup by going to Control Panel\Network and Internet\HomeGroup

2. HomeGroup computers share Windows libraries but not the Folders by default. However, you may share any folder by browsing to the specific folder. To do this, right click on the folder, and select "Share with" as shown in the figure below:

3. HomeGroups are not available in MAC OS X, Windows Vista, and Linux Distros.

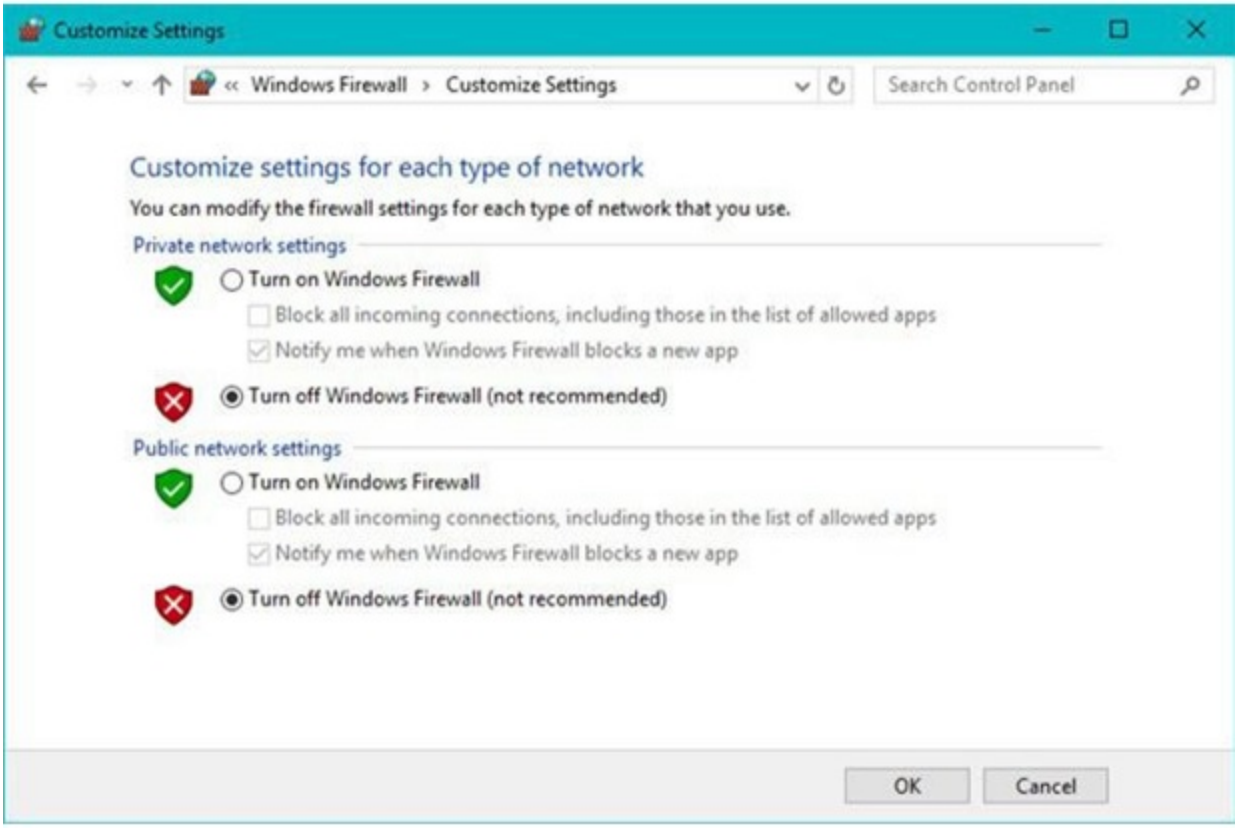
4. You can connect Windows 7 and Windows 8 computers to share HomeGroups.



Windows 10 Firewall: Microsoft Windows 10 comes pre-installed with a software firewall utility.

To enable the Windows 10 firewall:

Control panel -> System and security -> Windows Firewall -> Turn Windows Firewall on or off



Backup and Restore: Windows 10 has a backup and restore utility that can be used to backup or restore files and folders.

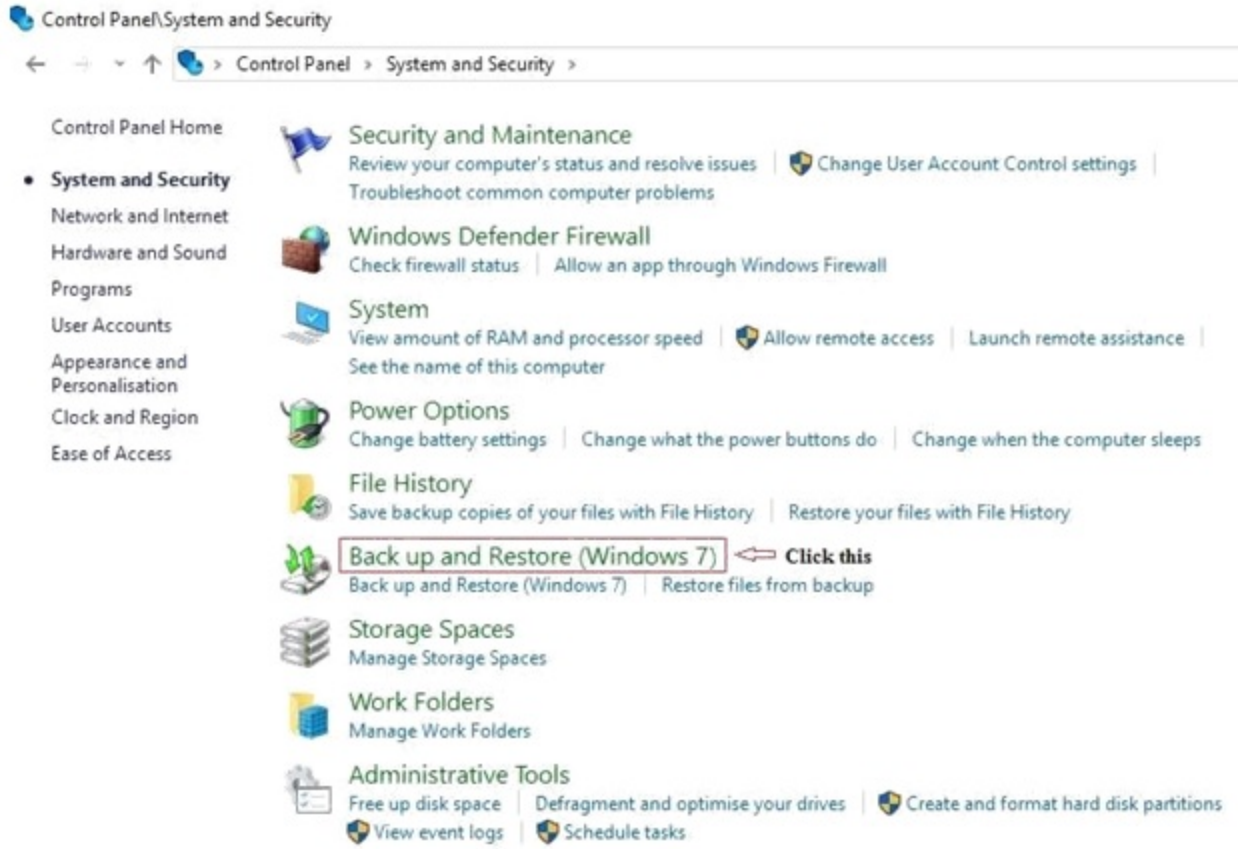
To create a System Image Backup on Windows 10

To create a full backup of your computer using the system image tool, use these steps:

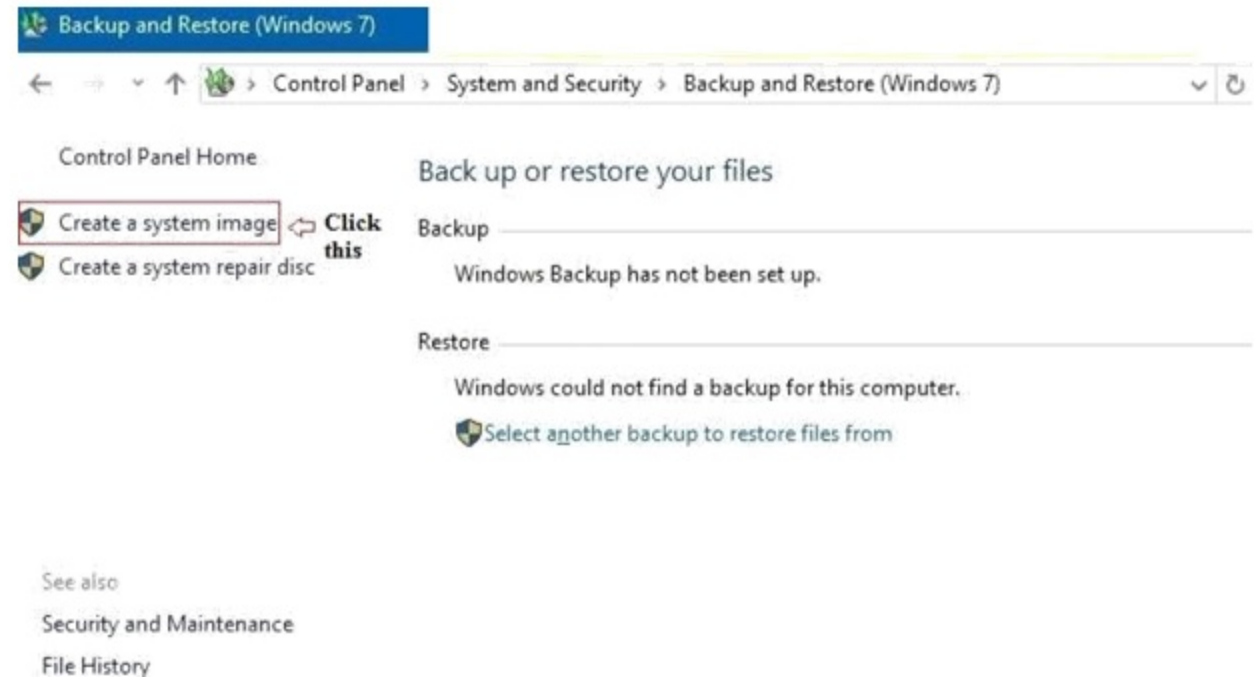
1. Open Control Panel.

2. Click on System and Security.

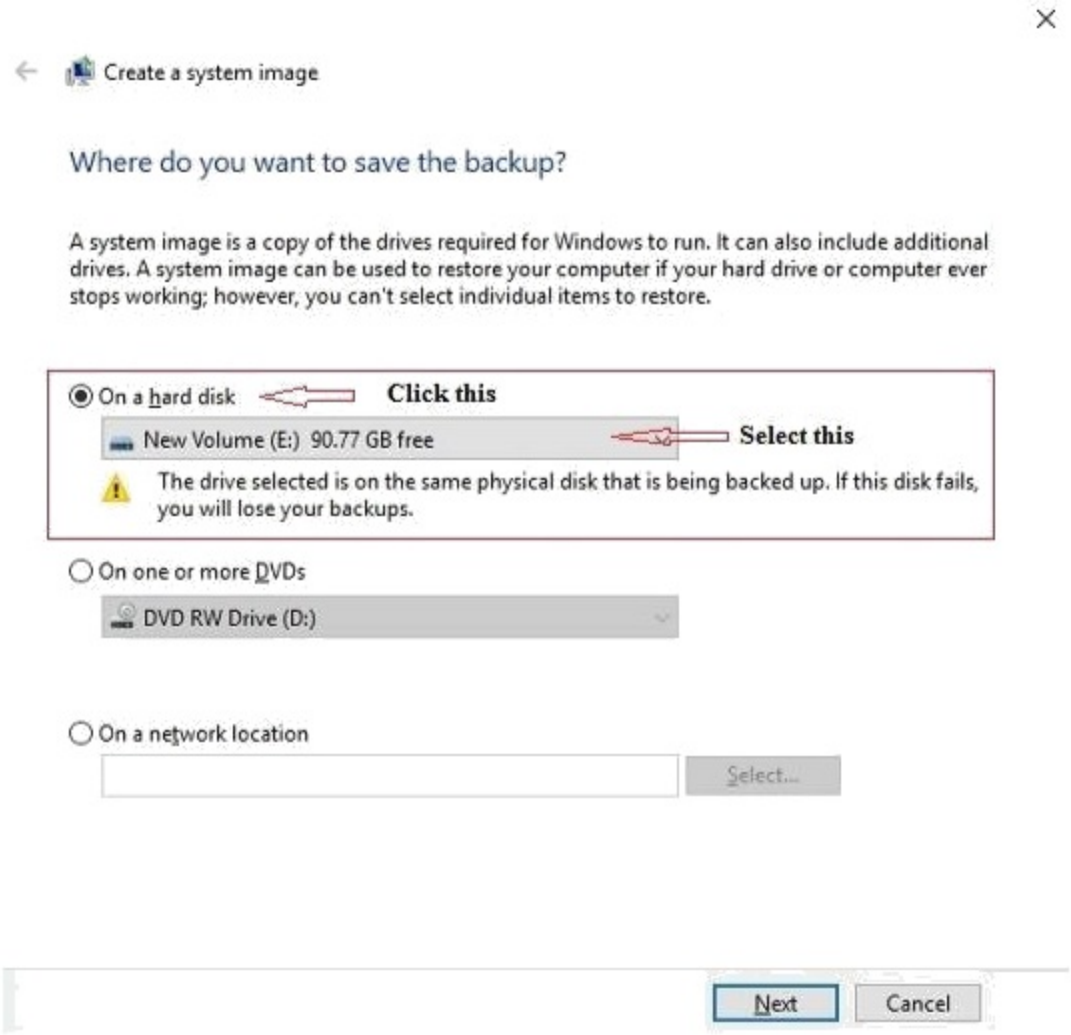
3. Click on Backup and Restore (Windows 7).



4. On the left pane, click the Create a system image link.



5. Under "Where do you want to save the backup?" select the On a hard disk option.



6.Using the "On a hard disk" drop-down menu, select the location to save the backup.

7. Select any additional drives that you may want to include in the backup.

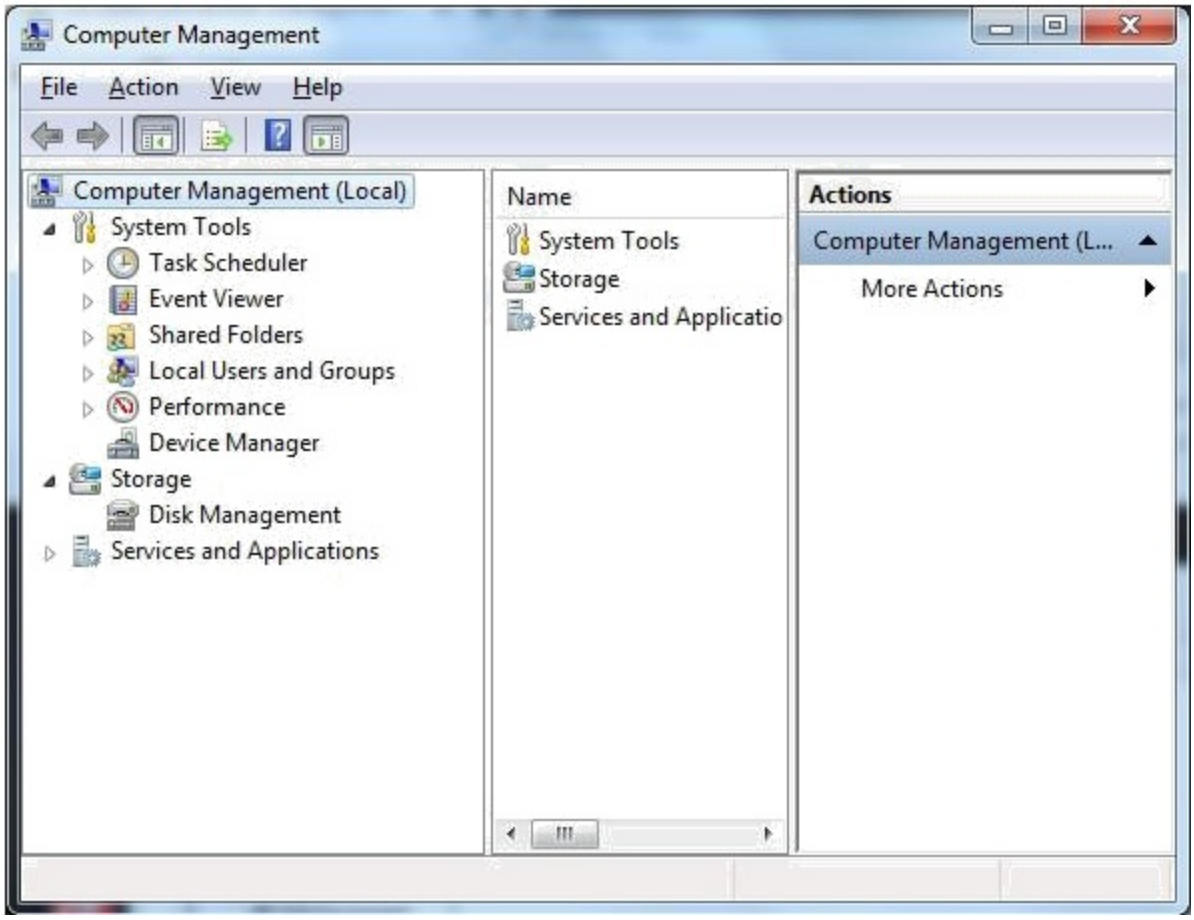
8. Click the Next button.

9. Click the Start backup button.

To open Computer Management in Windows 10:

1. Open it in the Start Menu.

Click the lower-left Start button to open the menu, type “compmgmt.msc” in the blank box and tap compmgmt.



4 ways to open Task Scheduler on Windows 10

Way 1: Open it in the Start Menu.

Click the lower-left Start button, enter “schedule” in the empty box and select Schedule tasks from the results.

Way 2: Turn on Task Scheduler via Search.

Tap the Search button on the taskbar, type schedule in the blank box and choose Schedule tasks.

Way 3: Open it in the Control Panel.

Step 1: Access Control Panel.

Step 2: System and Security > and tap Schedule tasks in Administrative tools

Way 4: Open Task Scheduler in the Computer Management.

Step 1: Open Computer Management.

Step 2: Click Task Scheduler on the left.

The Task Scheduler window appears , Now, you can select a new task from the menu Action -> Create Task.

Action Center: It is a central place to view alerts and take actions that can help keep Windows running smoothly.

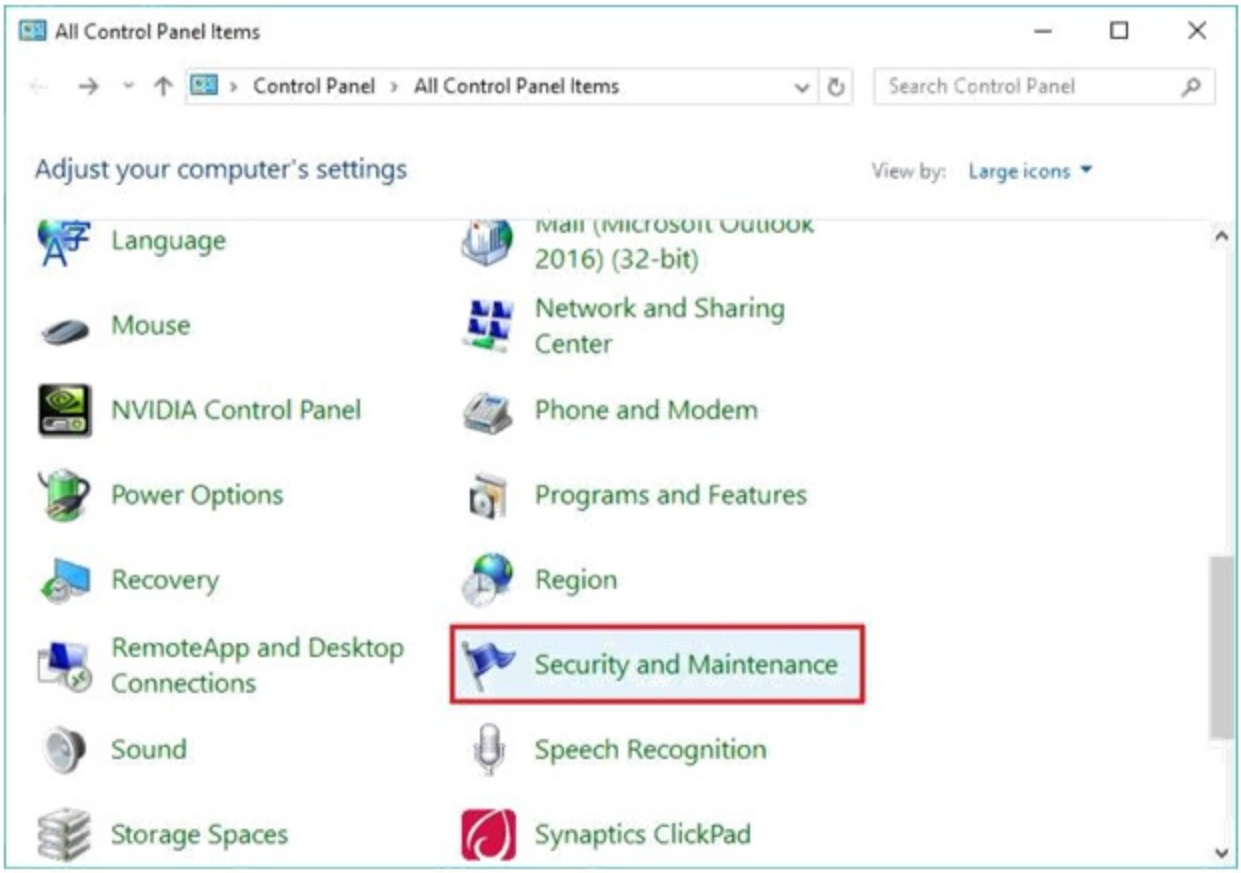
You can use either of the below ways to open Action center utility in windows 7

1. Start > run > wscui.cpl

2. Start > Control Panel > System and Security> Action Center in windows 7 system

Action center has new name in windows 10 as “Security And Maintainance” You can find it in the Control Panel app.

1. Start > Control Panel > System and Security> Security and Maintenance



Previous Contents Next

CompTIA®A+ Core 2 Exam Notes : Configure Windows Networking On A Client/desktop

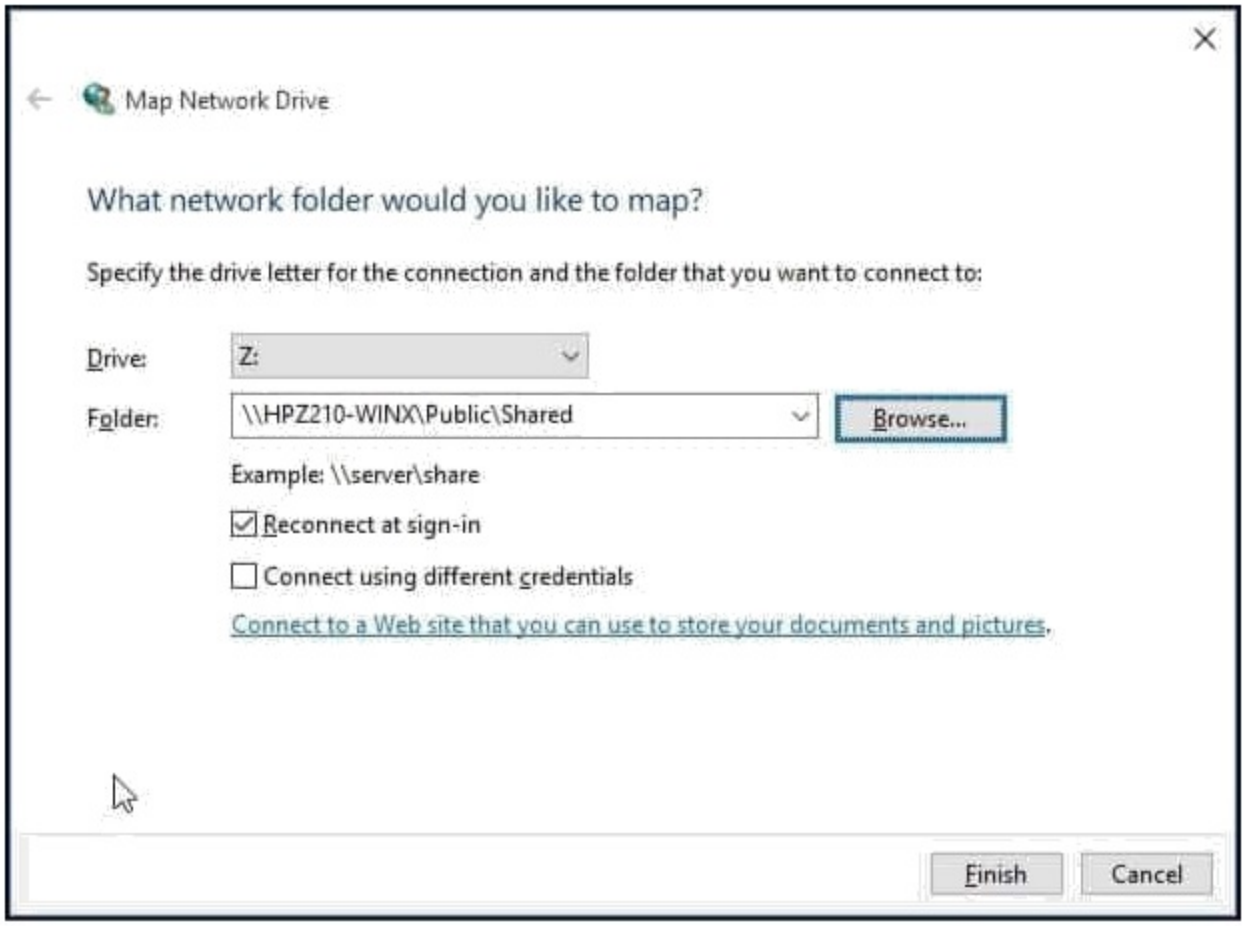
1. Windows Operating Systems

1.6 Configure Windows networking on a client/desktop

Mapping drives: To map a shared folder or a network drive to our computer, we use the Map Network drive. When we use locally connected computers in our home or office network, we may need to share our files with other computers for eliminating the requirement of manually copying the file to external storage media and after that transfer them to other computers. It will be helpful when we want to quickly access a network drive or a shared folder without remembering the complete path of the location.

To create a mapped drive

- Go to Start then right click on Computer.
- Click on Map Network Drive.
- Then enter the UNC path to the share.
- 4. When you map a drive, Windows shows the network folder as a drive in the Network Location section of Windows Explorer.



Homegroup vs Workgroup

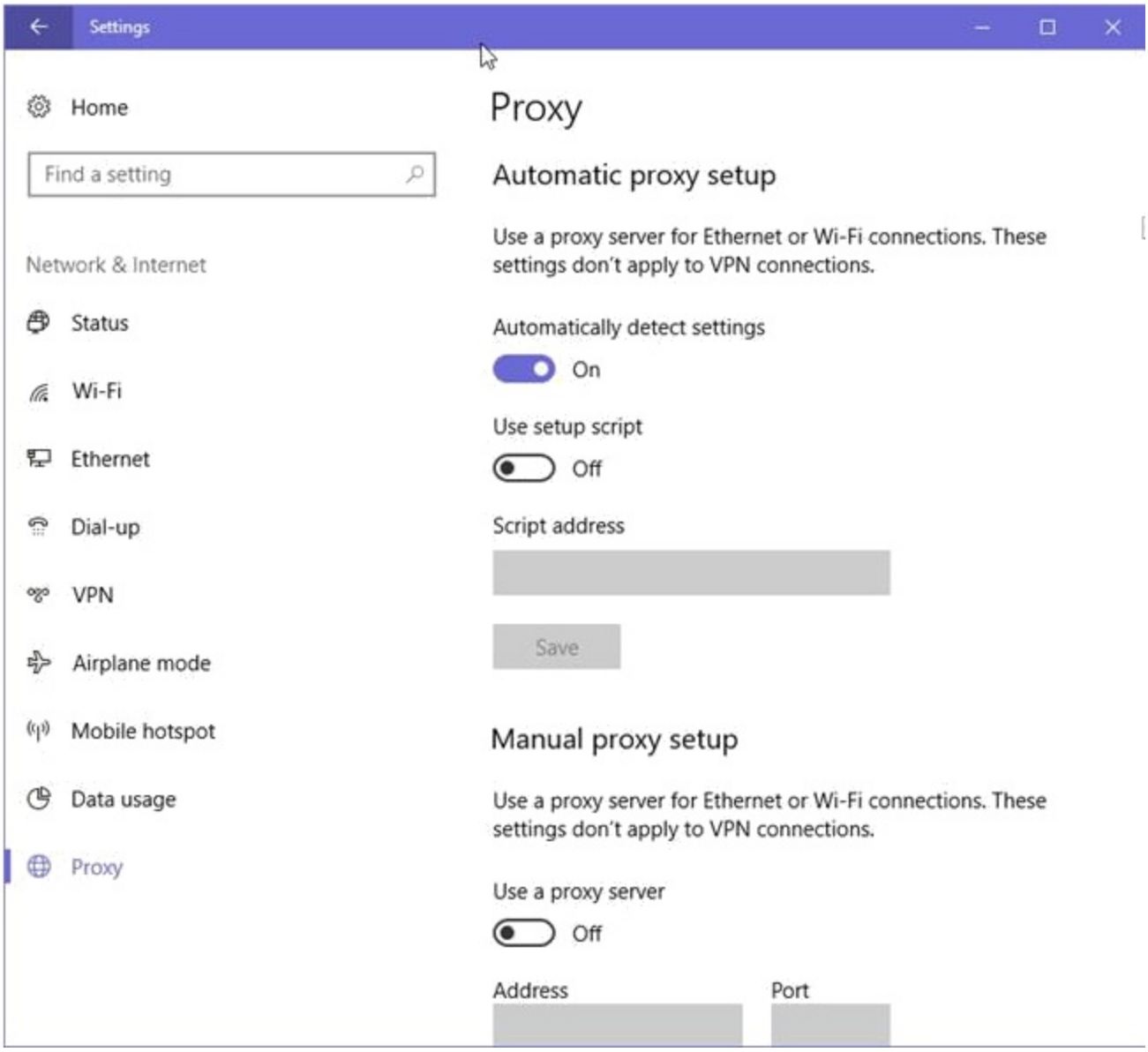
Homegroup: A homegroup is a group of PCs on a home network that can share files and printers. Using a homegroup makes sharing easier. You can share pictures, music, videos, documents, and printers with other people in your homegroup. You can help protect your homegroup with a password, which you can change at any time. Other people can't change the files that you share unless you give them permission to do so. After you create or join a homegroup, you select the libraries (for example, My Pictures or My Documents) that you want to share. You can prevent specific files or folders from being shared, and you can share additional libraries later. PCs must be running Windows 7, Windows 8, or Windows RT to participate in a homegroup. HomeGroup is available in all editions of Windows 7 and Windows8.With a HomeGroup, you can share files, printers, music, video, and pictures with other computers running Windows 7. You can also stream media to devices. The HomeGroup is protected with a password, and you will always be able to choose what you share with the group.

Workgroup: The WorkGroup describes a P2P network with no centralized authority wherein the devices on the network each control what is and is not shared on that particular device or workstation and the users or groups they want to share that resource with. In this model each workstation controls the database of users and privileges collectively referred to

as the workgroup. Each device that is part the workgroup can allow access on a user-by-user or group-by-group basis. Network usernames and passwords control access. Local Users and Groups are used to control access. If you want your computer to become a member of a domain, you need to have the network up and running, since you need to get authenticated to attach to a domain. In this case you don't have a network card and you can't attach to a domain. Therefore, it is required that you choose Workgroup, for which you don't need to have a network card.

Proxy settings: Windows 10 offers support for adding proxies inside Internet Explorer's settings. You can configure the proxy server and port to support the different protocols you use for accessing services that require a proxy within your organization.

- To configure a proxy server, you have to open the Settings app. One quick way to do that is to press Windows + I on your keyboard. In the newly opened window, click or tap the section labeled Network & Internet.
- Here, you find several subsections with settings. The last one should be named Proxy. Click or tap on it. On the right, there are two separate sections that can be configured: "Automatic proxy setup" and "Manual proxy setup."



Remote Desktop Protocol (RDP): Remote Desktop uses Remote Desktop Protocol and which in turn uses port 3389. By configuring the router to forward traffic on port 3389 to the host computer running RDP, one should be able to access the host remotely. If the host computer is on a publicly accessible IP address, there is no need for port forwarding. Remote client can access the host directly using host's public IP address. To connect to a remote computer the user account must be a member of the local group "Remote Desktop users" on the remote server in addition the user account needs the privilege to logon through RDP/Terminal Services. After performing a clean install of Windows 7 on a laptop and if you find that the Bluetooth on/off switch is not working , Instead of re-installing the OS/service pack, it is always better to install the correct driver for the device. Go to device manager, and update the Bluetooth driver.

Remote Desktop connection: Remote Desktop Connection (RDC, also called Remote Desktop, formerly known as Microsoft Terminal Services Client, or mstsc) is the client application for Remote Desktop Services. It allows a user to remotely log in to a networked

computer running the terminal services server. RDC presents the desktop interface (or application GUI) of the remote system, as if it was accessed locally. Because Windows Firewall restricts communication between your computer and the Internet, you might need to change settings for Remote Desktop Connection so that it can work properly.

- Open Windows Firewall by clicking the Start button Picture of the Start button, and then clicking Control Panel. In the search box, type firewall, and then click Windows Firewall.
- In the left pane, click Allow a program or feature through Windows Firewall.
- Click Change settings. Administrator permission required If you're prompted for an administrator password or confirmation, type the password or provide confirmation.
- Under Allowed programs and features, select the check box next to Remote Desktop, and then use the check boxes in the columns to select the network location types you want to allow communication on.
- Click OK.

You can initiate Remote Desk Top by using “mstsc” command, or by going to Start > All Programs > Accessories > Remote Desktop Connection. Please note that you will be able to connect only the Remote Desktop is already configured.

Only the Windows 7 Professional, Ultimate, and Enterprise editions can host a remote desktop connection.
Only the Windows 8/10 Pro and Enterprise editions can host a remote desktop connection.

DNS: The Internet and other IP networks rely on the Domain Name System (DNS) to help direct traffic. The DNS maintains a distributed database of network names and corresponding IP addresses. DNS uses a client/server network architecture. DNS servers store DNS database records (names and addresses), while clients include PCs, phones and other devices of end users. DNS servers also interface with each other, acting as clients to each other when needed. The DNS organizes its servers into a hierarchy. For the Internet, root name servers reside at the top of the DNS hierarchy. The Internet root name servers manage DNS server information for the Web's top-level domains (TLD) (like ".com" and ".uk"). Any organization can have its own DNS servers for private use, as long as the network uses TCP/IP protocol. However, on the public Internet, there can't any overlap of names or the IP addresses given to the individual computers or devices. Another flavor of DNS is DDNS. Unlike DNS that only works with static IP addresses, DDNS is designed to also

support dynamic IP addresses, such as those assigned by a DHCP server. That makes DDNS a good fit for home networks, which normally receive dynamic public IP addresses from their Internet provider that occasionally change.

QoS stands for quality of service. In SOHO environment, QoS is normally set at router level. If you want to enforce QoS policies in your network, make sure you use a router, which is equipped with QoS software

Previous Contents Next

CompTIA®A+ Core 2 Exam Notes : Common Preventive Maintenance Procedures Using Appropriate OS Tools

1. Windows Operating Systems

1.7 Common preventive maintenance procedures using appropriate OS tools

The following are true about backup:

Full backup: Here all files that have been chosen for backup are backed up, irrespective of wheather the archive bit is set or not set. Archive bit is set (ON) after backup.

Incremental backup: Here only the files that have been created or have changed since the previous full or incremental backup will be backed up. The archive bit is set after a file is backed up. The next Incremental backup will backup files that have changed since previous full or incremental backup.

Differential backup: Here, the files that have changed or created since the last full backup will be backed up. Note that, unlike Incremental backup, the archive bit is not set on a differential backup. The result of this is that the next differential backup will include files that were backed up during earlier Differential backups.

Previous Contents Next

CompTIA®A+ Core 2 Exam Notes : Important Features, And Functionality Of The Mac Os And Linux Operating Systems

examguides.com/Aplus-Core2/aplus-core2-8.htm

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).

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.

Preferred 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
Fat 16	2 GB	2 GB	Legacy
Fat 32	4 GB	8 TB	Legacy
NTFS	2 TB	256 TB	For Windows Compatibility
ext2	2 TB	32 TB	Legacy
ext3	2 TB	32 TB	Standard linux filesystem for many years until Ubuntu 8
ext4	16 TB	1 EiB	Modern iteration of ext3. Default file system in Ubuntu 9, 10
XFS	8 EiB	8 EiB	Created by SGI

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 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.

Previous Contents Next

CompTIA®A+ Core 2 Exam Notes : Setting Up And Use Client-side Virtualization

examguides.com/Aplus-Core2/aplus-core2-9.htm

2. Other Operating Systems & Technologies

2.2 Set up and use client-side virtualization

Purpose of virtual machines: Each Virtual Machine is like a separate platform, and the host PC is transparent to the end user. A virtual machine reduces the amount of hardware required. The hardware on the host computer is shared among several virtual machines. If a virus infects a virtual system, then it is usually limited to that specific virtual machine only.

Memory (or RAM) is the most important component when considering a host machine for virtualization. You need to have as much memory as possible onboard the host machine so that the virtual machines do not suffer from delays in performing routine tasks.

Access rights: One needs to have access rights to access network resources. Access rights is a generic term that grants permissions to a user, or to an application, to read, write and erase files in the computer. Access rights can be tied to a particular client or server, to folders within that machine or to specific programs and data files.

The following are the benefits of virtualization:

1. Virtual Machine Migration: It is easy to migrate a virtual machine to another host machine easily. It was not so when you install your operating system on a physical hardware as a stand alone OS. In the later event, you need to worry about hardware compatibilities,

and adequacy of hardware resources, and even the compatibility of the operating system with the application being used. Moving and setting up a service on a dedicated machine is also labor intensive. On the other hand, a virtual machine may be migrated to another similar host OS in matter of minutes. This has enabled moving data between data centers very fast and affordable.

2. Decoupling of infrastructure and the server platform: The OS is decoupled from the hardware in a virtual environment, thus making it easy for the application developer not to worry about the infrastructure. At the same time, it enables data center operator to concentrate on the infrastructure performance and stability.

3. Instant Capacity: Virtualization enables elastic capacity to provide systems at a moment's notice. In the physical server world, it could take weeks to procure the hardware and integrate it with the existing system.

4. Cost Benefits: With virtualization, data centers can consolidate server requirements to fewer, more powerful systems that use resources more effectively. This extends to space, power, port and cabling savings. These supporting elements of infrastructure can be very expensive, especially with respect to network and storage ports.

5. Isolating Applications: In the physical server, data centers frequently consolidated applications on servers. This was good for keeping the number of physical servers down but may lead to application incompatibilities or inappropriate allocation of resources. With virtualization, we can install applications on dedicated operating systems on a virtual server so that there are no local compatibility or resource conflicts allowing us to provision a virtual machine for required amount of memory and disk access, which are two primary resource areas in virtualization.

Virtualization Technology Examples

VMWare: ESX, and ESXi are VMware's platforms for virtualization. Though basic version is free, it costs extra money to unlock advanced management and enhancement features. XenServer on the other hand is fully open source and all advanced features are included in the single product at no cost at all. Both VMware and Citrix offer paid support for their products so you can also get help with the platforms.

Hyper-V: Hyper-v is the Microsoft product and is offered free of cost on selective platforms. Hyper-V enables running virtualized computer systems on top of a physical host. These virtualized systems can be used and managed just as if they were physical computer systems, however they exist in virtualized and isolated environment. Special software called a hypervisor manages access between the virtual systems and the physical hardware resources.

Virtualization enables quick deployment of computer systems, a way to quickly restore systems to a previously known good state, and the ability to migrate systems between physical hosts.

KVM: Kernel-based Virtual Machine (KVM) is an open source virtualization technology built into Linux. KVM lets you turn Linux into a hypervisor that allows a host machine to run multiple, isolated virtual environments called guests or virtual machines (Vms). KVM is part of Linux.

Emulator requirements:

1. Emulation involves making one system imitate another. For example, if a piece of software runs on system A and not on system B, we make system B "emulator" the working of system A. The software then runs on an emulation of system A.

2. In this same example, virtualization would involve taking system A and splitting it into two servers, B and C. Both of these "virtual" servers are independent software containers, having their own access to software based resources - CPU, RAM, storage and networking - and can be rebooted independently. They behave exactly like real hardware, and an application or another computer would not be able to tell the difference.

3. In other words, emulator is creating an environment that behaves in a hardware-like manner. This takes a toll on the processor by allocating cycles to the emulation process - cycles that would instead be utilized executing calculations. Thus, a large part of the CPU muscle is expended in creating this environment.

4. Emulation can be effectively utilized in the following scenarios:

- Running an operating system meant for other hardware (e.g., Mac software on a PC; console-based games on a computer)
- Running software meant for another operating system (running Mac-specific software on a PC and vice versa)
- Running legacy software after comparable hardware become obsolete
- While emulated environments require a software bridge to interact with the hardware, virtualization accesses hardware directly. However, despite being the overall faster option, virtualization is limited to running software that was already capable of running on the underlying hardware

1. Wide compatibility with existing x86 CPU architecture

2. Ability to appear as physical devices to all hardware and software

3. elf-contained in each instance

4. The option "Running software that is already capable of running on the underlying hardware" does not describe emulation, because there is total compatibility with the hardware.

Previous Contents Next

CompTIA®A+ Core 2 Exam Notes : Basic Cloud Concepts

examguides.com/Aplus-Core2/aplus-core2-10.htm

2. Other Operating Systems & Technologies

2.3 Basic Cloud Concepts

Different cloud models are explained below:

Private cloud: The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.

Community cloud: The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g. mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.

Public cloud: The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

Hybrid cloud: A hybrid cloud includes both the public and private options with one or more providers. By spreading things out over a hybrid cloud, you can keep good control of security and optimize costs. The downside is that you have to keep track of multiple security platforms and ensure that all aspects of your business can communicate with each other.

The primary benefits of the public cloud are:

1. Easy scalability: One of the main benefits that comes with using public cloud services is near unlimited scalability. The resources are usually offered 'on demand' so any changes in activity level can be handled easily. This in turn brings with it cost effectiveness.

2. Cost effectiveness: Since a data center houses hundreds of customer businesses, the hardware and software works out cheaper.

3. Increased reliability: The vast network of servers and the wide bandwidths with which they are inter-linked in public cloud services offers better reliability when compared with private cloud. Even if one data center was to fail entirely, the network simply redistributes the load among the remaining centers making it highly unlikely that the public cloud would ever fail. Also, data centers put lot of resources such as power backups, and backup servers available all the time to cater to any unforeseen events.

The main disadvantage of public cloud over private cloud is with respect to security. Since the public cloud is available on public Internet, it is possible that hackers may attempt to break the services. However, data center companies put several layers of security in a professionally managed data center to make it practically very difficult to bring down a service or application.

The main advantage of private cloud over public cloud is with respect to security. Since the public cloud is available on public Internet, it is possible that hackers may attempt to break the services. A private cloud uses its own server farm, and connected to others resources using private lines, such as a leased line or a VPN.

IAAS (Infrastructure as a Service) : A business may not want to invest into datacenters, servers, networking equipment and to list the current directory files and folders. Owner required to maintain all these resources. They may wish to utilize more computer resources as they grow. This is where the Infrastructure as a Service (IAAS) comes in. The vendors who provide the IAAS maintain all the hardware required so the businesses utilizing their services do not have to worry about it. IAAS allows organizations to have an unlimited storage potential of the cloud. This allows them to grow and shrink their storage as the requirements demand. The IAAS is used by companies offering disaster recovery services.

SAAS(Software as a Service): SAAS also referred to as software on demand, can be used by many people for a variety of functions. It allows users to benefit from the functionality of particular software without having to worry about storage or other issues. The software can easily be accessed by multiple users using just a web browser. Google Docs is a great example of SAAS. The software is hosted on the cloud servers and requires no installation on client computers in most cases.

PAAS (Platform as a Service): PAAS is a variant of SAAS. A client runs their own copies of the Operating System, using the cloud provider's infrastructure. Clients don't have to worry about storage spaces and maintaining servers or hard disks.

NAAS(Network as a Service): NaaS is a business model that aims at providing network services over the internet. From a client's point of view, they only require a computer that is connected to the internet - along with the access to NAAS provider's portal. This is a very cost-effective service that allows new businesses to reduce costs on their network hardware and the required personnel to maintain this hardware. The network just functions on the pay-as-you-go basis, just like water and electricity services.

A few concerns on Cloud technology:

Cloud computing systems are networked systems situated far from subscriber's premises, and are affected by traditional computer and network security issues, such as the need to provide data confidentiality, data integrity, and system availability. Since sensitive customer data resides on the cloud, and usually customers access the cloud using a browser, any browser and communication channel security breaches may directly impact the security of the cloud-based service.

Previous Contents Next

CompTIA®A+ Core 2 Exam Notes : Basic Features Of Mobile Operating Systems

examguides.com/Aplus-Core2/aplus-core2-11.htm

2. Other Operating Systems & Technologies

2.4 Basic features of mobile operating systems

1. **Advanced Configuration and Power Interface (ACPI):** specification provides an open standard for device configuration and power management by the operating system.

2. **Operating System Power Management (OSPM):** is an operating system technology for managing the power of the underlying platform and switching it between different power states. OSPM enables a platform or system to implement the most efficient power mode and is applicable across all devices and components within a platform/system. OSPM is also known as Operating System-directed configuration and Power Management.

3. **The Advanced Host Controller Interface (AHCI):** is a technical standard defined by Intel that specifies the operation of Serial ATA (SATA) host bus adapters in a non-implementation-specific manner

4. **iCloud :** is a cloud storage and cloud computing service available on iPhones and other compatible computing devices. The service allows users to store data such as music and iOS applications on remote computer servers for download to multiple devices such as iOS-based devices running iOS 5 or later, and personal computers running OS X 10.7.2 "Lion" or later, or Microsoft Windows (Windows Vista service pack 2 or later).

5. **The Global Positioning System (GPS) :** is a space-based satellite navigation system that provides location and time information in all weather conditions, anywhere on or near the Earth where there is an unobstructed line of sight to four or more GPS satellites. Most smart phones have GPS built into the software.

6.**Accelerometer:** Accelerometer measures acceleration (change of velocity) in a given direction. Mobile devices use accelerometer for screen orientation. Every modern Smartphone can change the orientation of the display based on the phone's rotation with the help of accelerometer. Traditional accelerometers use a "seismic mass" attached to a spring encased in some sort of housing. As the device moves the mass moves on the spring and the device can measure the movement. Using multiple units a device can determine which way it turned based on which masses move.

7.**Gyroscope:** A gyroscope is a device with a spinning disc or wheel mechanism that harnesses the principle of conservation of angular momentum: the tendency for the spin of a system to remain constant unless subjected to external torque. Gyroscope enables re-alignment of screen orientation as the user turns his phone.

8.**iOS, Android OS, Windows Mobile:** Google's Android, Apple's iOS, Windows Mobile are three of the most widely used operating systems in mobile devices, such as smart phones and tablets. Android, which is Linux-based and partly open source, is more PC-like than iOS, in that its interface and basic features are generally more customizable from top to bottom. However, iOS' uniform design elements are sometimes seen as being more user-friendly.

Previous Contents Next

CompTIA®A+ Core 2 Exam Notes : Configuring Basic Mobile Device Network Connectivity And Email

examguides.com/Aplus-Core2/aplus-core2-12.htm

2. Other Operating Systems & Technologies

2.5 Configure basic mobile device network connectivity and email

You can configure or view the IP address of an iOS device by going to Settings > General > Network > Wi-Fi > SSID Name > IP address

However, there is another way of finding what you need in iOS settings. This is by using the hidden "Search" option. Use this to quickly find and access settings in iOS:

1. Open the Settings app on the iPhone, iPad, or iPod touch

2. At the primary Settings app screen, tap and pull down on the settings screen to reveal the "Search" box at the top of the Settings screen

3. Type your search parameters to find the matching options in Settings app, then tap on any of the results to jump immediately to that portion of the Settings app.

Steps to configure Email on android mobile devices:

You need to know your domain name (e.g. example.com.au), email address (e.g. yourname@example.com.au) and email account password. You also need to know the POP or IMAP server name.

1. Open your device's email application

2. If you already have an email account set up, press Menu and tap Accounts. Press Menu again and tap Add account.

3. Type your Email address and Password, and click Next.

4. If you have IMAP, tap IMAP. If you're not sure, tap POP3. USE IMAP ONLY

5. Enter the settings for your incoming server, depending on the type of email you have

6. Enter the settings for your outgoing server

7. Select Require sign-in and make sure your Username (your full email address) and Password are correct Tap Next

8. Tap Next again. Name your account and enter the name you want to display on outgoing messages

9. Tap Done

Some points to remember:

- iOS 5 offers untethered updates.
- The ISP provides the information on the SMTP, and POP server addresses. You need to feed this information to the mail client while configuring to send and receive e-mail.
- You can synchronize address book and calendar between MS Exchange and iPhone.
- SIM, or Subscriber Identity Module, does have a number associated with it, called a SIM serial number (SSN). This number is also referred to as the integrated circuit card identifier (ICCID). ICCIDs are stored in the SIM cards and are also engraved or printed on the side of the card. The number can be up to 19 digits long and contains information about your operator, your location, and when it was made.

IMSI: An international mobile subscriber identity (IMSI) is a unique number, usually fifteen digits, associated with Global System for Mobile Communications (GSM) and Universal Mobile Telecommunications System (UMTS) network mobile phone users. The IMSI is a unique number identifying a GSM subscriber. Your International Mobile Station Equipment Identity (IMEI) number is different from your SSN, ICCID or IMSI. It is a unique serial number given to a device when it is manufactured that identifies a device on a mobile network, but not the subscriber. If your phone is stolen and you alert your carrier, they can blacklist the IMEI and prevent its use on all mobile networks even if a new SIM card is used.

The SSN or ICCID and IMEI information can be found under the Settings app on smartphones. On Android, go to the "About Phone" menu. On iOS devices, see "General: About" and on Windows phones, "About: More Info."

Wi-Fi tethering: Tethering is connecting one device to another. In the context of mobile phones and tablet computers, tethering allows sharing the Internet connection of the phone or tablet with other devices such as laptops. Connection of the phone or tablet with other devices can be done over wireless LAN (Wi-Fi), over Bluetooth or by physical connection using a cable, for example through USB. If tethering is done over Wi-Fi, the feature may be branded as a mobile hotspot. Mobile hotspot is a feature present in smartphones nowadays which lets you convert your smart phone into a portable router. One can setup a password protection to it easily so that no one without the password can connect to your smart phones. The Internet-connected mobile device can act as a portable wireless access point and router for devices connected to it.

Bluetooth: Bluetooth is widely used for communication between smart phones and other accessories or between PDAs and information kiosks. Various versions exist as given below:

B**luetooth 1.x:** Capabilities - Basic rate bluetooth (that would be about a theoretical maximum of 1 Mbps data rate)

Bluetooth 2.x: Capabilities - Basic rate + EDR (that would be about a theoretical maximum of
3 Mbps data rate; optional), EDR: Enhanced Data Rate.
Speed 24Mbit/s (4.0) ; 24Mbit/s (3.0+HS); 3Mbit/s(2.0)

Bluetooth 3.x: Capabilities - Basic rate + EDR (optional) + HS (optional)
Speeds up to for +HS: 24Mbit/s

Bluetooth 4.x: Capabilities - Basic rate + EDR (optional) + HS (optional) + LE (optional)
LE stands for Low Entergy.
Speed: 24Mbit/s
Bluetooth Range: Among different bluetooth specifications, there are 2 most popular classes (types) of devices:

Class 1: range up to 100 meters (in most cases 20-30 meters)
Class 2: range up to 30 meters (in most cases 5-10 meters)

Configure Screen lock: Our smart phones carry a lot of personal information. All of your text messages, emails, notes, apps, app data, music, pictures, and so much more are all on there. While it’s a very great convenience to have all of these on your phone, it’s also a major security risk if all of this data is easily accessible. The best way to prevent simple unauthorized access is by setting some sort of lock on your phone. Two popular choices, especially on Android phones, are passwords and pattern.

POP3 and IMAP Connection:

POP3: Post Office Protocol version 3 (POP3) is a standard mail protocol used to receive emails from a remote server to a local email client. POP3 allows you to download email messages on your local computer and read them even when you are offline. You can set up your mobile phone to send and receive email from your email accounts. Using POP3 (Post Office Protocol version 3), your email are retrieved and stored locally on your mobile phone and at the same time they're deleted from the server. It is therefore not possible to access your email from different devices.

IMAP: The Internet Message Access Protocol (IMAP) is a mail protocol used for accessing email on a remote web server from a local client. IMAP and POP3 are the two most commonly used Internet mail protocols for retrieving emails. Both protocols are supported by all modern email clients and web servers.

Main difference between IMAP and POP3: The POP3 protocol assumes that there is only one client connected to the mailbox. In contrast, the IMAP protocol allows simultaneous access by multiple clients. IMAP is suitable for you if your mailbox is about to be managed by multiple users."

Previous Contents Next

CompTIA®A+ Core 2 Exam Notes : Common Security Threats

examguides.com/Aplus-Core2/aplus-core2-13.htm

3. Computer 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.

Previous Contents Next

CompTIA®A+ Core 2 Exam Notes : Common Prevention Methods

examguides.com/Aplus-Core2/aplus-core2-14.htm

3. Computer Security

3.2 Common Prevention methods

Security Methods:

Anti-virus software, and Spyware software can be used to clear malicious programs from a computer. Also, note that you need to install up-to-date Service Packs, and patches.

1. It is recommended that the **backup tape** is stored at a location away from the building where the backup was taken. For most companies, backups contain important data and loosing backups may affect the continuity of one's business. If a backup is stored in the same building, it may get damaged in fire or any other natural calamities along with the computers. As a result, both the server, as well as back fail at the same time. Therefore, it is recommended to store the backup at a different location.

2. **Mantraps** are physical security devices or constructions designed to entrap a human. a man trap refers to a small space having two sets of interlocking doors, such that the first set of doors must close before the second set opens. They are also known as air locks in the security industry. Mantrap effectively prevents tailgating, in which an unauthorized person may enter a restricted premises simply following an authorized person.

3. **Remote Wipe:** Use this feature when a device is lost or stolen to erase all data on the device and reset the device. A remote wipe removes all device-based data like mail, calendar, and contacts from the device, but it may not delete data stored on the device's SD card.

4. **Disabling any unused ports** on a networking device will prevent any unauthorized persons from plugging in to the network and get sensitive data.

5. **Authentication:** CHAP uses 3-way handshaking. CHAP uses Challenge/ Response method which provides protection against the password capture while authenticating the user. One should use CHAP whenever it is possible. PAP uses 2-way handshaking. Passwords are sent in clear text across the link. Therefore, PAP is to be used only when it not possible to use CHAP.

6. Microsoft does not recommend manual removal of BHO virus or Trojans. To detect and remove this threat and other malicious software that may have been installed, run a full-system scan with an up-to-date antivirus product such as the Microsoft online scanner.

Alternative, use any trusted third party scanner for identifying and removing the threat.

Given below are the few important precautions that you may need to take to prevent infections due to malware:

- Install anti-virus/malware software. There are free as well as paid versions of software available. The Windows itself has a basic version of anti malware application by name Microsoft Security Essentials. You can enable the same at the least.
- Keep operating system up to date. You can enable automatic updates so that you don't need to worry about manually updating your OS.
- Update device drivers, and applications as necessary. Remove any unnecessary applications using add/remove programs.
- Secure your network, don't keep any open ports and use secured cabinets wherever possible.
- Do not open an email attachment from somebody that you do not know. Do not click on a link in an unsolicited email or messages.
- Use difficult to guess passwords and disable "remember password" option in the browser bar.
- Use encrypted Wi-Fi in home and office, preferably WPA2

Anti-virus update files are traditionally called as "Definitions".

MBR: Short for Master Boot Record, 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.

Even if you reinstall Windows or format your hard drive, a virus infecting the MBR will not be deleted. So, after you reinstall Windows, your computer first runs that same MBR virus code which then reinfects your new installation of Windows with viruses.

You can remove MBR virus using a Recovery CD or Vista/7 Installation DVD by following the steps below:

1. Boot using a Recovery CD or Vista/7 Installation DVD to the Recovery Environment.

2. At the System Recovery Options menu choose 'Command Prompt'

3. At the command prompt type in the command: “bootrec /fixmbr”

4. Press Enter to replace the MBR and then restart your computer.

Note that some anti-virus software are capable of detecting and removing MBR virus. However, one needs to be careful when using AV software for removing MBR virus.

Antispyware: Anti-spyware software detects spyware through rules-based methods or based on downloaded definition files that identify common spyware programs. Anti- spy ware software can be used to find and remove spy ware that has already been installed on the user's computer, or it can act much like an anti-virus program by providing real-time protection and preventing spyware from being downloaded in the first place.

User authentication: Authentication begins when a user tries to access information. First, the user must prove his access rights and identity. When logging into a computer, users commonly enter usernames and passwords for authentication purposes. This login combination, which must be assigned to each user, authenticates access. However, this type of authentication can be circumvented by hackers. A better form of authentication, bio metrics, depends on the user’s presence and biological makeup (i.e., retina or fingerprints). This technology makes it more difficult for hackers to break into computer systems.

Key fobs: A key fob is a small electronic security device with built-in authentication protocols or mechanisms to allow whoever possesses it to enter a secured network or location in order to access data or services. A key fob is designed to be small so that it can be carried around inconspicuously just like a key chain, hence the name key fob.

Previous Contents Next

CompTIA®A+ Core 2 Exam Notes : Basic Windows Os Security Settings

examguides.com/Aplus-Core2/aplus-core2-15.htm

3. Computer Security

3.3 Basic Windows OS security settings

BitLocker To Go: Encryption is a key component in any operating system security plan. With the help of the newly improved BitLocker, Windows 7 users can have more control over the encryption of their hard drives. Microsoft's BitLocker even automatically encrypts new data while it's running. It's a hands-off tool that should improve security in Windows 7.

- BitLocker To Go is new to Windows 7. Rather than encrypting just the desktop
- BitLocker To Go allows users to encrypt portable hardware, like external hard drives and USB keys.
- It's probably one of the best new security features in Windows 7.
- More users than ever are going mobile. Data is at risk whenever that happens.
- BitLocker To Go helps to limit the spread of sensitive data to malicious hands.
- BitLocker Drive Encryption is a full disk encryption feature included with the Ultimate and Enterprise editions of Microsoft's Windows Vista and Windows 7 desktop operating systems.
- It is designed to protect data by providing encryption for entire volumes.
- The algo loads before the OS, and protects the entire volume. OS files can't be put in a volume that uses BitLocker.

- To make all files in the directory myfiles to be read only, the command is "ATTRIB C:\MYFILES +r"

If you encrypt a folder on an NTFS volume, all files and subfolder created in the encrypted folder are not automatically encrypted. However, you will be prompted whether you want to encrypt all the subfolders and their content. If you choose YES, they will also be encrypted.

Also note that you can't encrypt a file or folder that is compressed. If you want to encrypt a file or folder that is compressed, you need to first decompress the file or folder and then encrypt. Only NTFS volumes support file or folder encryption.

You can set the following attributes using ATTRB command:

1. System

2. Hidden

3. Read-only

4. Archive

'+' sets and attribute
'-' clears an attribute

Correct syntax is : ATTRIB [+R -R] [+A -A] [+S -S] [+H -H] [PATH] [FILESPEC] [/S] /s Processes files in all directories in the specified path.

Encrypting File System(EFS) keeps your documents safe from intruders who might gain unauthorized physical access to your sensitive stored data by stealing your laptop or Zip disk, or by other means.

Windows 7 BitLocker and the Encrypting File System (EFS) are two robust security features designed to protect the system and user data. When comparing BitLocker and EFS

1. BitLocker encrypts volumes, whereas EFS only encrypts files.

2. BitLocker does not require user certificates, but EFS does.

3. BitLocker protects the operating system from modification, whereas EFS does not.

Windows Security Center: By using latest Windows update, it is possible to secure the operating system from any known bugs. Windows Security Center also shows the status of software designed to protect against spyware, In addition to it's own software, Windows Security Center can monitor security products from multiple companies and show you which are enabled and up to date.

For local administrators, only the built-in administrator account can be used to perform a remote install. Since this account is disabled by default, use the "net user administrator /active:yes" command from the command console. This will enable this account to install applications remotely.

Login time restrictions: Even if the login and password are available, the user may be ignorant of the same. You need to take the login information from the user directly before proceeding with any work.

BIOS Password: In the BIOS the supervisor password will prevent someone from re-configuring the BIOS settings without the proper password. The BIOS password is stored in CMOS memory that is maintained while the PC is powered off by a small battery, which is attached to the motherboard. Refer to the motherboard manual to find the jumper that clears the BIOS password. Alternatively, if you remove this battery, all CMOS information (including the BIOS password) will be lost. The company policy requires that the password be changed every month. It is highly recommended that the password be remembered. It is a bad practice to alternate between two known passwords.

Account Management: On a stand-alone computer or a computer that is a member of a workgroup, a user account establishes the privileges assigned to each user. The three user accounts available are: Administrator, Limited, and Guest. The important features of these accounts are as given below:

Administrator account:

- Can create and delete user accounts on the computer.
- Can change other users' account names, passwords, and account types.

Standard account:

- A standard user account lets a person use most of the capabilities of the computer, but permission from an administrator is required if you want to make changes that affect other users or the security of the computer.
- When you use a standard account, you can use most programs that are installed on the computer, but you can't install or uninstall software and hardware, delete files that are required for the computer to work, or change settings on the computer that affect other users.

Guest account:

- Cannot install software or hardware, but can access applications that have already been installed on the computer.
- Cannot change the guest account type.
- You should disable any guest accounts on your system as they can provide information to hackers and increase your security risk.

User level security gives better control of resource on user to user basis. Share level security assign passwords to the resources rather than the users and is less secure. Create a group, and give privileges to group members to make required changes to workstations. Add the user accounts to this group. You could go to Task Manager and click on "users" tab. All currently logged in users will be listed.

Previous Contents Next

CompTIA®A+ Core 2 Exam Notes : Securing Wireless And Wired Network

examguides.com/Aplus-Core2/aplus-core2-16.htm

3. Computer Security

3.4 Securing wireless and wired network

MAC Filtering (or layer 2 address filtering): MAC filtering refers to a security access control method whereby the 48-bit address (also called MAC address) assigned to each network card is used to determine access to the network. MAC addresses are uniquely assigned to each card, so using MAC filtering on a network permits and denies network access to specific devices through the use of blacklists and whitelists. To limit the number of computers to a known few, configuring MAC filtering is a very good option. This is configured on the wireless router and not on the client computers. Any wireless network, SSID needs to be configured on the wireless router. Note that if the router broadcasts SSID, then the clients will automatically learn about the wireless network. If the SSID broadcast is disabled on the router, you need to configure the clients with proper SSID (same as that of the router SSID).

Enable MAC Filtering: MAC limiting the MAC addresses that can access the wireless network, you can prevent unauthorized computers from accessing your wireless network. Note that each MAC address is unique, and hence MAC address filtering can effectively prevent unauthorized computer access. By using MAC filtering, you can allow or disallow certain MAC addresses only. Note that even if the SSID broadcast is turned off, it is possible to access the wireless network if the intruder some how knows the network name.

Changing default SSID: SSID, short for service set identifier, a unique identifier attached to the header of packets sent over a WLAN. The SSID differentiates one WLAN from another, so all access points and all devices attempting to connect to a specific WLAN must use the same SSID. You can hide the SSID so that it is not broadcast over the wireless network. For encryption, enable WPA2 (or the older versions like WPA). This would provide basic protection for the wireless network. Remember to use difficult to guess password for WPA2.

Installing an authentication server or an external Firewall incurs additional costs, and not a best solution. By default, SSID is broadcast by a wireless access point. By disabling SSID broadcast, the wireless network existence may be hidden. However, if SSID broadcast is disabled, one needs to pre-configure the SSID on a client workstation manually.

Otherwise, it wouldn't be possible to communicate in the wireless network. Enabling SSID broadcast will only announce the network to neighborhood devices, thus lessening the security of the network.

Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) are two security protocols and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks. It is possible that several networks are operating at the same frequencies. It is recommended that you change the WI-FI channel and see if it solves the problem.

WPA: WPA, short for Wi-Fi Protected Access, is a Wi-Fi standard that was designed to improve upon the security features of WEP (Wired Equivalent Privacy). The technology is designed to work with existing Wi-Fi products that have been enabled with WEP.

WPA2: WPA2 is an encryption standard, and client workstations will still be able to see SSID even if the WPA2 and Mac filtering are enabled. MAC filtering is another security precaution, which enables (or disables) listed MAC addresses in the internal MAC filter table of WAP. You need to manually enter the MAC addresses for this purpose. SSID needs to be configured on the laptop for connecting to the Access Point. The DHCP server typically supplies IP address, DNS server information, and subnet mask. To secure the wireless router for home use from unauthorized access you need to change the default login/password on a router soon after the router is installed. Secondly, ensure to set encryption such as WPA2 so that only authorized users will be able to access the wireless network.

Note that for WPA encryption, you need to configure it on the wireless router and on all the workstations. To enable MAC filtering, you need to gather the MAC addresses of all client computers, and feed it into the wireless router

The specifications for various 802.11 standards is as given in table 1:

TABLE 1: IEEE 802.11 PHY STANDARDS						
Release date	Standard	Band (GHz)	Bandwidth (MHz)	Modulation	Advanced antenna technologies	Maximum data rate
1997	802.11	2.4	20	DSSS, FHSS	N/A	2 Mbits/s
1999	802.11b	2.4	20	DSSS	N/A	11 Mbits/s
1999	802.11a	5	20	OFDM	N/A	54 Mbits/s
2003	802.11g	2.4	20	DSSS, OFDM	N/A	54 Mbits/s
2009	802.11n	2.4, 5	20, 40	OFDM	MIMO, up to four spatial streams	600 Mbits/s
2012	802.11ad	60	2160	SC, OFDM	Beamforming	6.76 Gbits/s
2013	802.11ac	5	40, 80, 160	OFDM	MIMO, MU-MIMO, up to eight spatial streams	6.93 Gbits/s

As can be seen in the table, 802.11ac works at 5 GHz, and supports bandwidth up to 6.93Gbits/sec.

Note: MIMO (multiple input, multiple output) is an antenna technology for wireless communications in which multiple antennas are used at both the source (transmitter) and the destination (receiver). The antennas at each end of the communications circuit are combined to minimize errors and optimize data speed. MIMO is one of several forms of smart antenna technology, the others being MISO (multiple input, single output) and SIMO (single input, multiple output).

Parental Control: The parental controls built into Windows 7/8/10 help parents determine which games their children can play, which programs they can use, and which websites they can visit, and when. Parents can restrict computer use to specific times and trust that Windows OS will enforce those restrictions, even when they're away from home.

Content filtering: To set the content filtering on the Android phone , go to apps > menu key. Choose 'Settings' and then “Parental Controls” then choose appropriately from 'Set Content Restrictions'. You can now choose which apps are allowed on your phone.

Port Forwarding: The computers on the network have been configured to use DHCP and private IP addresses. Therefore, you need to set up port forwarding to access the host computer running RDP. Remember, RDP uses port 3389 by default.

Locking Android phone: Locking your Android smartphone with a password, PIN or unlock pattern is your first defense against those who would use it for malicious purposes like stealing your info or sending joke texts to your friends and family. To setup, go to Settings/Security/ Set up screen lock, and choose to enter a pattern, or a password or a PIN. If you are looking for fast and easy way to unlock your smart phone, choose "Pattern".

Common wireless security protocols

Features of RADIUS server:

- 1. Open standard, and widely supported. Note that TACACS+ is a Cisco proprietary standard, but well supported too.
- 2. Use UDP port
- 3. Provides extensive accounting capability when compared with TACACS+ server
- 4. Only the password is encrypted in packets transiting between the RADIUS server and the client (any device acting as client, such as a router or a switch or a host computer).
- 5. There is a new upgrade expected, named Diameter.

Features of TACACS+ server

- Granular control: TACACS+ uses the AAA (AAA refers to Authentication, Authorization and Accounting) architecture, which separates AAA. This allows separate solutions that can still use TACACS+ for be used for authentication, authorization and accounting. For example, with TACACS+, it is possible to use Kerberos authentication and TACACS+ authorization and accounting. TACACS+ is very commonly used for device administration.
- TACACS+ encrypts the entire body of the packet but leaves a standard TACACS+ header.
- TACACS+ is a Cisco proprietary protocol (later became an Open standard), and very widely supported by various vendors offering AAA servers. Note that RADIUS is an Open Standard and widely supported too.
- TACACS+ uses TCP port (port #49) to communicate between the server and the client.
- TACACS+ provides complete encryption for communication between the TACACS+ server and the client.

Previous Contents Next

CompTIA®A+ Core 2 Exam Notes : Implementing methods for securing mobile devices

examguides.com/Aplus-Core2/aplus-core2-17.htm

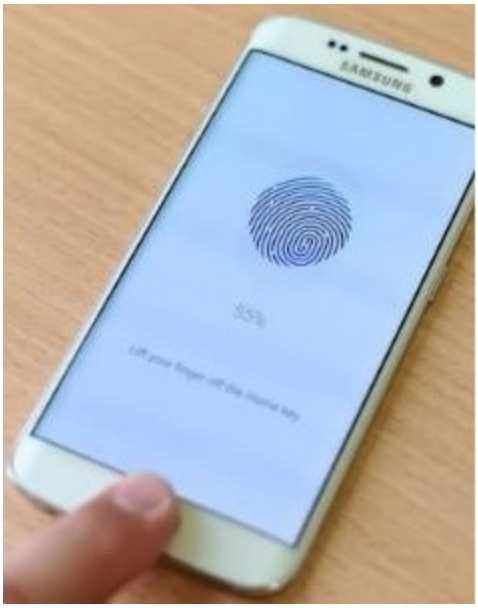
3. Security

3.5 Implementing methods for securing mobile devices

Screen Locks: Apple and Android mobile devices include a requisite locking mechanism, which is off by default. The user can enable these locks. The following are types of locks that you can implement to secure your device.

Fingerprint lock: A fingerprint lock has a built-in fingerprint reader that is used to access the device. It is a biometric-type of lock that uses your fingerprint to unlock the device. This works by placing your finger on a touchpad sensor on the device.

Face lock: Face lock uses the built-in camera to identify the users face to allow access. There are a high number of false positives that makes the face lock less secure than the fingerprint lock. This means that presumably someone that looks like you could unlock your phone.



Swipe lock: Swipe lock has a predefined pattern that users outline with their finger to allow access. The swipe lock works by displaying nine dots in a matrix of 3x3. You then swipe with your finger with the registered pattern to unlock the phone. The swipe lock is the least secure of any locking methods. A grease trail from your fingers can allow someone to derive the swipe pattern.

Passcode lock: Passcode lock uses a personal identification number (PIN) to access the device. It is a 4-6 digit numeric passcode or a alphanumeric depending on the device. Passcode locks suffer from the same problems that password are prone to: People can shoulder surf or learn your passcode over time.

Remote wipes: In the event of a lost or stolen your mobile device the capability to remotely delete all of the data on the device is extremely important to the device security. In most cases the security measures given above will be sufficient to secure your data. When you are

sure the device cannot be recovered or you think the security measures will not withstand a breach, you have no choice but to clear all personal data from the device. This operation will return the device to its factory settings. Remote wipe program may or may not have the capability to clear data from SD cards that may be installed on the device. Some apps are capable of this feature and if there is a risk you should select your remote software accordingly.

Locator applications: If you have misplaced a device, all mobile operating systems support a degree of interactive device location. The Android Device Manager for the Android OS uses Google Maps and the location information last reported by the device to provide the last known location. In some cases this may be sufficient to find the device by simply activating the ringer. This application allows you to Ring the device, lock it or remotely wipe your personal data returning the device to its out of the box configuration. However, note that either the remote wipe or the locator apps will not work if the service is powered off or has its SIM card removed.

Remote backup applications: Each mobile operating system supports backups to the cloud. This is in the form of iTunes and iCloud of Apple devices, OneDrive for Microsoft and Google Drive on Android. Access to these storage locations are controlled for the most part by email specific logins. For example you would create User@domain.com for a Microsoft account, User@gmail.com on Android and your personal apple ID to access Apple services like iTunes and iCloud Drive, other free backup and storage locations include Dropbox and others. You will find that all free backup services have either feature or size limitations or both. iCloud is geared toward storage, while iTunes handles backups and synchronization.

Failed login attempts restrictions: Primarily the mobile devices can be configured to lock after a specified number of login attempts. This is usually a temporary condition providing you with the time necessary to remember your password. In the conventional PC environment it is common to see login restrictions like the number of failed attempts that are allowed before the account locks. The number of attempts allowed can be reset, but it is important to know that on an iPhone for example, after an excessive number of attempts the

device will permanently lock and erase all data. In most cases the access can be restored by using the primary account and password data. Providing, of course, that the device has not been erased.

Patching/OS updates: A patch modifies the existing software to add security features or operational improvements also known as bug fixes. Critical patches are known as hotfixes. A Service Pack refers to a group of patches and hot fixes compiled into a single download and install as a cumulative update. In the mobile environment the programming on the device is being constantly tested for vulnerabilities. As important as it is to keep your device virus and malware protection up to date, it is equally important to allow your mobile OS to patch and update its software. A widely used technique to trick you into installing malware employs a fake download site loaded with malware infected drivers.

Biometric authentication: One approach is biometric authentication, a system that relies on the unique biological characteristics (such as retina, voice, fingerprint, signature) of individuals to verify identity for secure access to electronic systems. The benefits of using biometrics for user authentication are evident. Whether it is a retina scan, a fingerprint or using your voice, the user always has their "password" with them and it is never forgotten. For the most part, it is easy to use because it is on someone's person and all they need to do is "show up." If your employees already have devices equipped with the appropriate biometric readers, it may be an affordable approach. However, as with any technology, there are some downsides to using biometrics for authentication. One of those challenges is that you are introducing a high level of dependencies in your organization. Implementing biometric authentication can prove expensive and inconvenient, as initial provisioning of users requires a tamper-proof process to link identity and biometric data. Additionally, workers may no longer be able to login from devices other than their company-issued computer as their private tablet or PC may not have the necessary biometric scanner.

Full device encryption: Encryption is a highly effective security measure for files, folders even volumes. Encrypted content is digital junk without the decryption key. This enhanced security comes with a system performance penalty. The solution to this performance impact is whole device encryption which encrypts everything decreasing any internal operational performance lag.

Multifactor authentication: The combination of more than one authentication method is called multifactor authentication. Smartphones or other mobile devices can play an integral part in this process. Multifactor methods are frequently used by financial institutions to prevent unauthorized access and intrusion. Some multifactor authentication implementations use an email /password combination to initiate a callback or text back passphrase delivery. This will be in the form of a one-time passphrase (OTP) delivered to the mobile device then used as the second element of authentication. Also where the mobile device connectivity cannot be assured the multifactor method can have an email/password combined with facial recognition to provide the necessary security level.

Authenticator applications: An authenticator app works with mobile devices to generate security codes that can keep accounts secure by requiring 2 factor authentication. Once this is setup, your account will require a code from the app in addition to your account password. An account is usually added to the authenticator applications by entering a secret key or scanning a QR barcode, this creates the account in the authenticator applications.

Trusted sources vs. untrusted sources: Software drivers and other apps can easily be corrupted to allow malware to operate. You should study any system errors and verify the source of all errors and warnings. Once you are satisfied, always start with the manufacturer's recommended website when updating any elements of your system. This is Google Play for Android and Apple's App Store for iOS and the Microsoft Store for Windows based devices. Use the device settings where possible to block or restrict unknown or untrusted sites. It is necessary to examine the actual sources of everything you install on your machine. Given the possibility of misdirected web traffic look at the URLs carefully. It's essential to understand the importance of using trusted sites to obtain your software. Also know the consequences of installing untrusted content up to and including identity theft and complete device failures.

Firewalls: The firewall system is set up to block any unauthorized access to the mobile communications system. On a mobile device some features of the firewall are configured during individual app installations. Each app requests specific permissions to install. Review these permissions for their relationship to the app operation and whether or not you wish to grant it. A mobile device firewall app will allow you to monitor both the inbound and outbound communications on your mobile device.

Policies and procedures: With this explosive growth of mobile devices in the workplace, there are many different policies and procedures that may be required for organization to minimize data loss.

BYOD vs. corporate owned: The term BYOD (Bring your Own Device) describes a corporate policy that allows an employee to use their own device in the corporate environment. This includes evaluation by the company IT department to be sure the device meets the corporate security requirements regarding software, patches, anti-malware, firewall, VPN, login requirements and encryption. Any software installation needed to meet the BYOD policy are referred to as on-boarding. Corporate owned devices are configured to meet these same requirements.

Profile security requirements: This policy will be clearly outlined and enforced. The policy will also include provisions for wiping the data from lost/stolen devices or employees that have been dismissed.

Previous Contents Next

CompTIA®A+ Core 2 Exam Notes : Troubleshoot PC operating system problems with appropriate tools

examguides.com/Aplus-Core2/aplus-core2-18.htm

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 a blank screen:

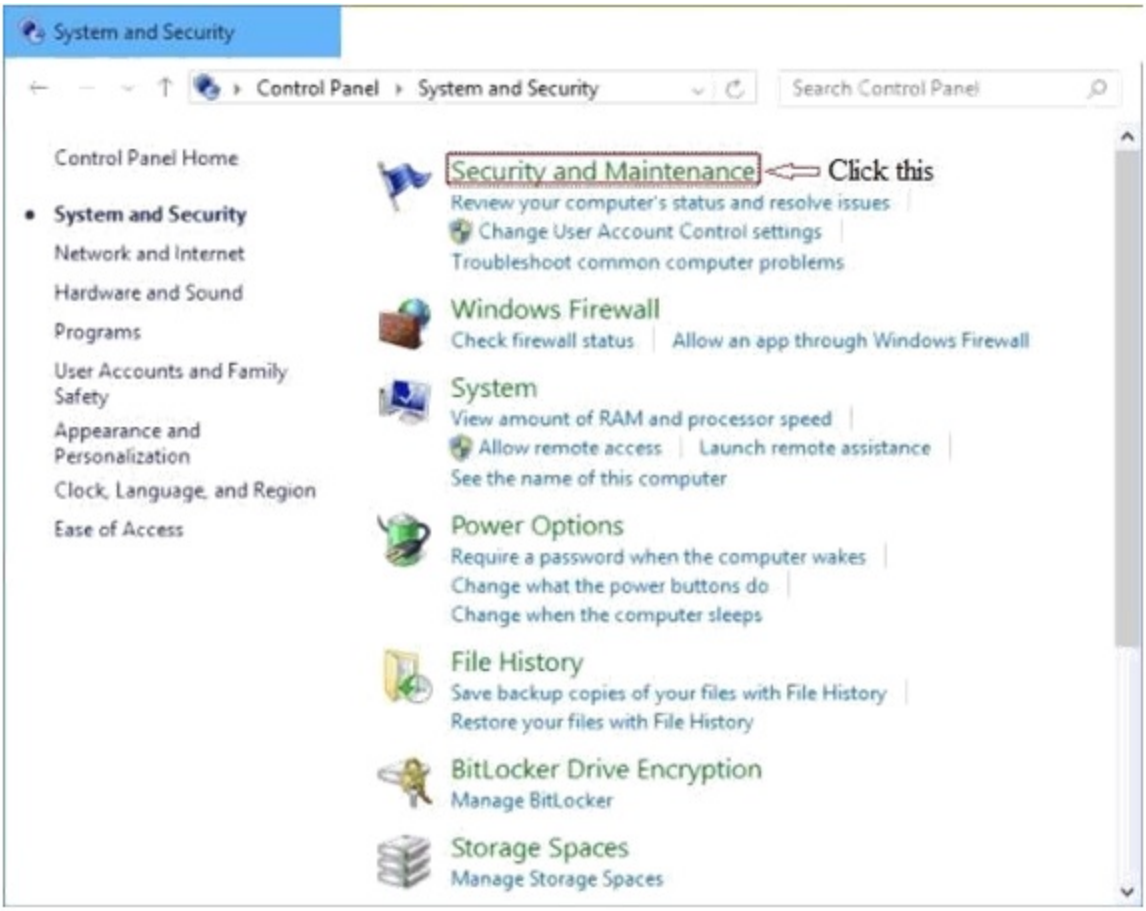
- Hold down the Windows logo key (normally between CTRL + ALT on your keyboard) at the same time as pressing Ctrl, Shift + B. If you're running Windows 10 on a tablet, you'll need to press the increase volume and decrease volume buttons together three times within a twosecond period.
- You should see 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.

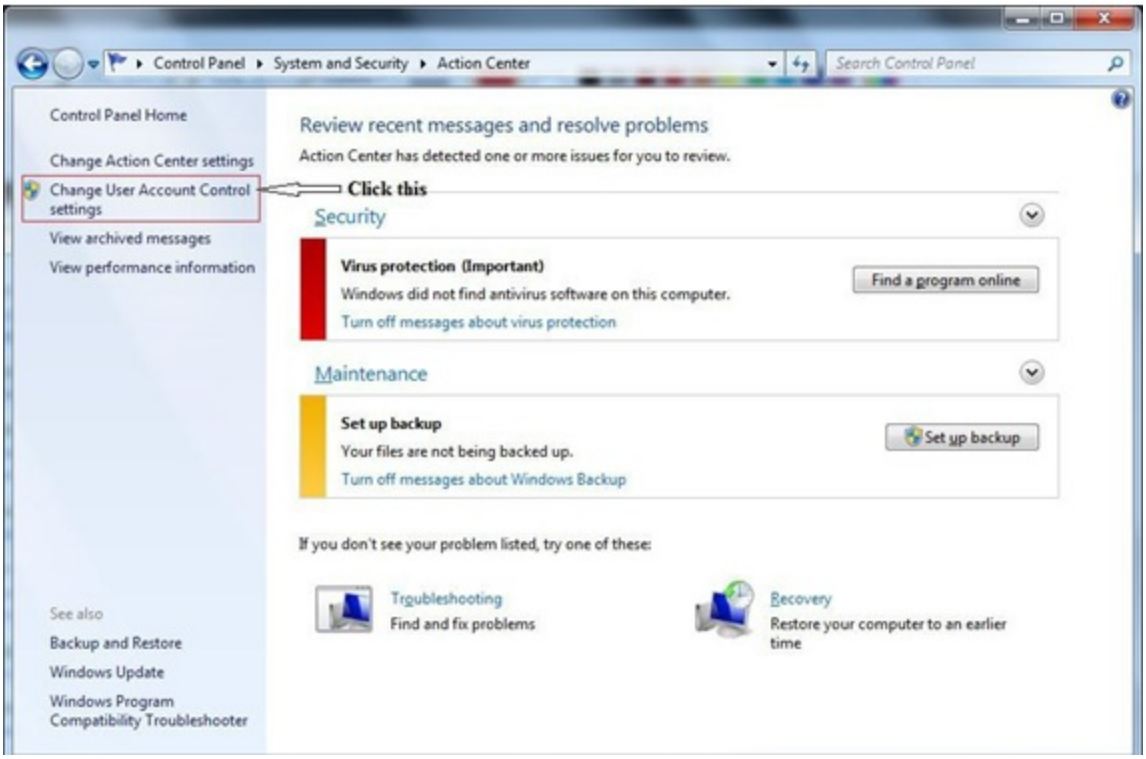
How to change UAC settings in Windows 7

Open the Windows Control Panel, and then click System and Security.

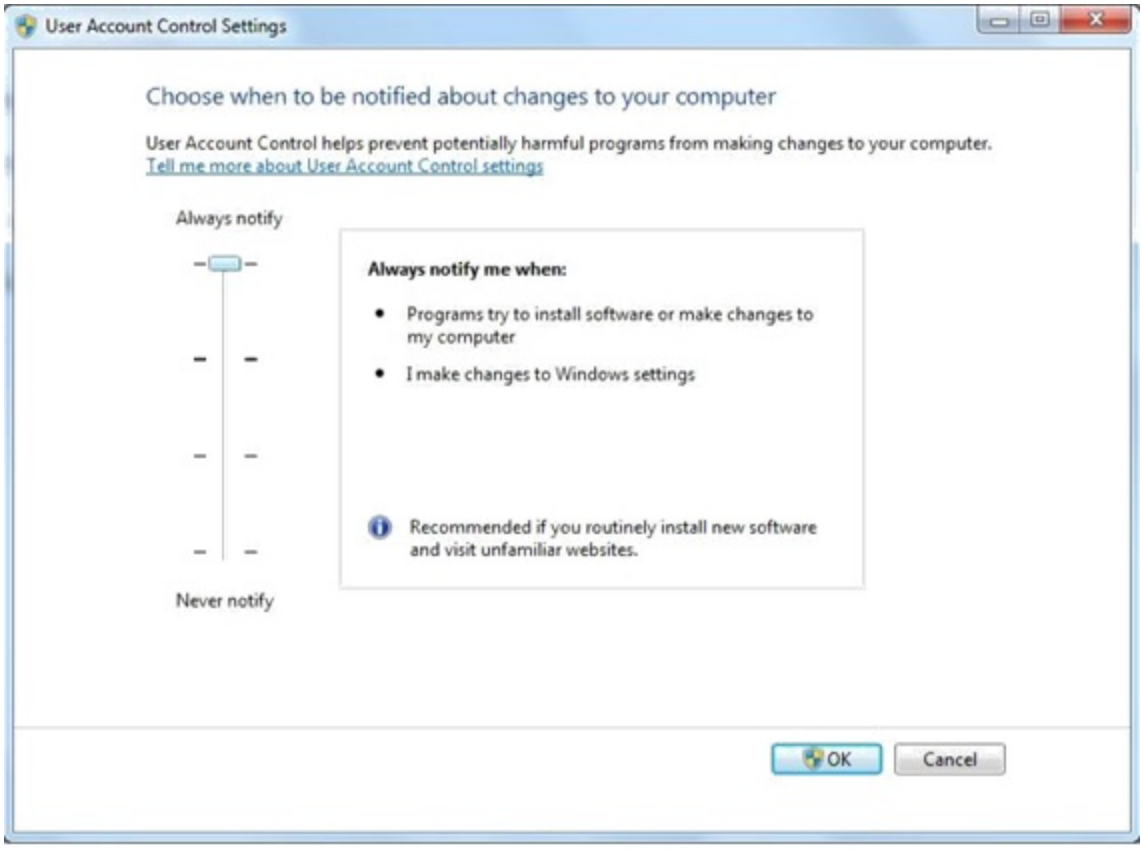
2. The System and Security window appears. Click Action Center



3. The Action Center window appears. In the left pane, click Change User Account Control



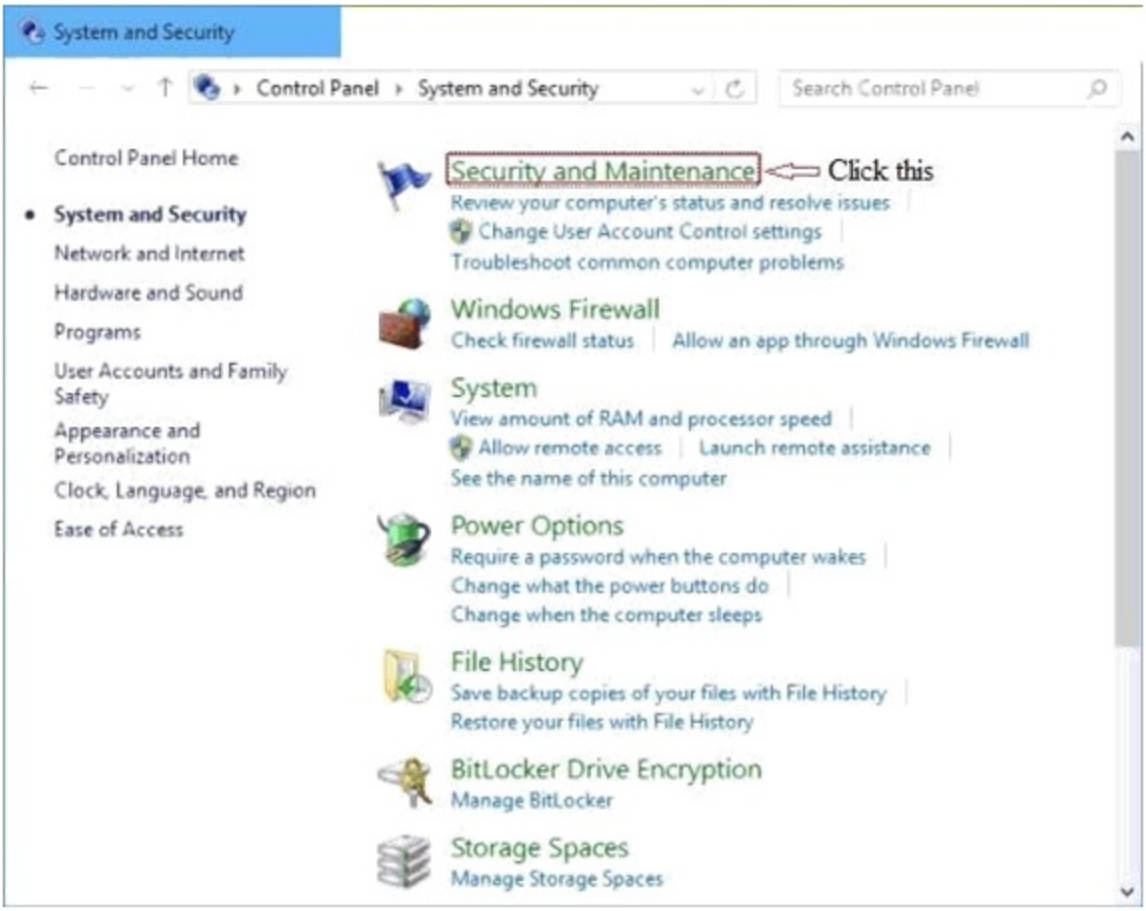
The User Account Control Settings dialog box appears, as shown in the figure below. Slide the vertical bar (on the left side) to your desired setting and click OK.



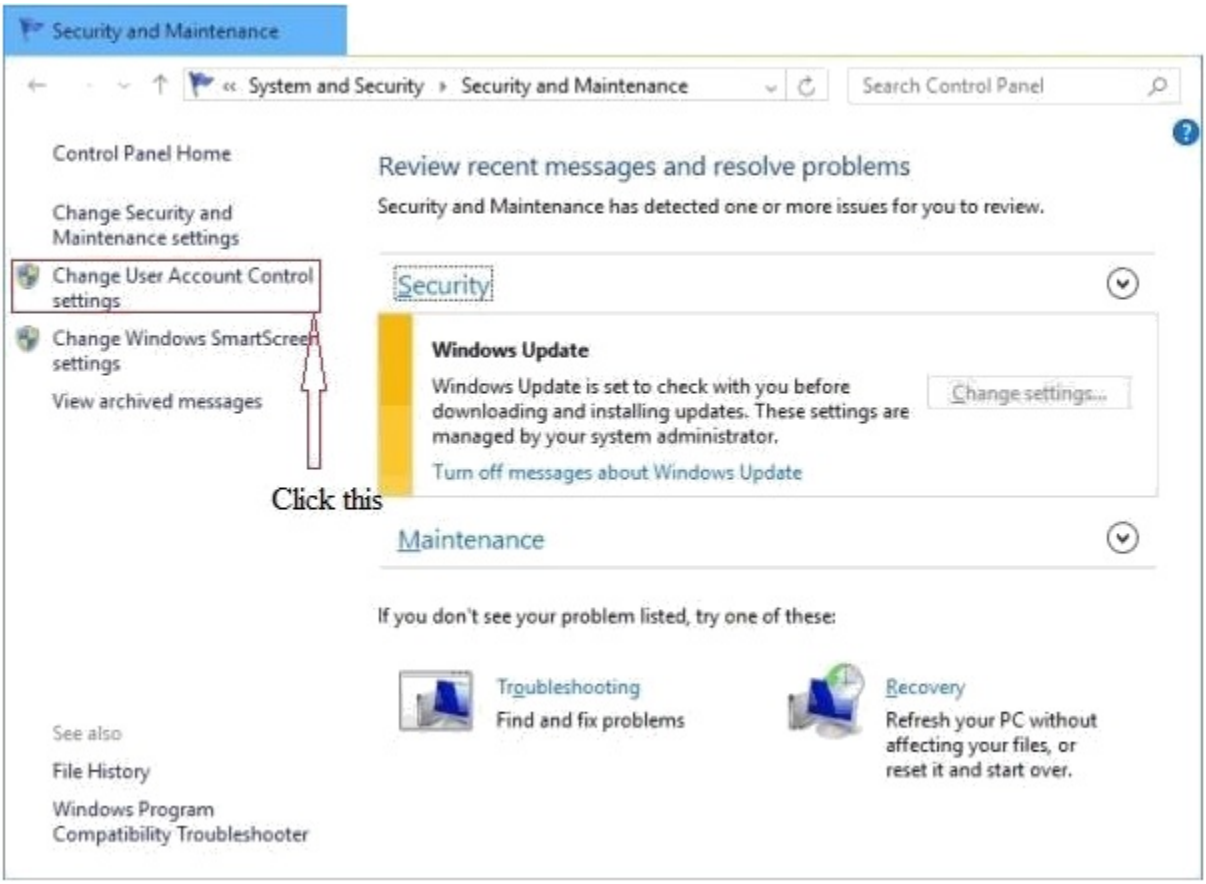
To change UAC settings in windows 10

1. In the control panel window click “System and Security”

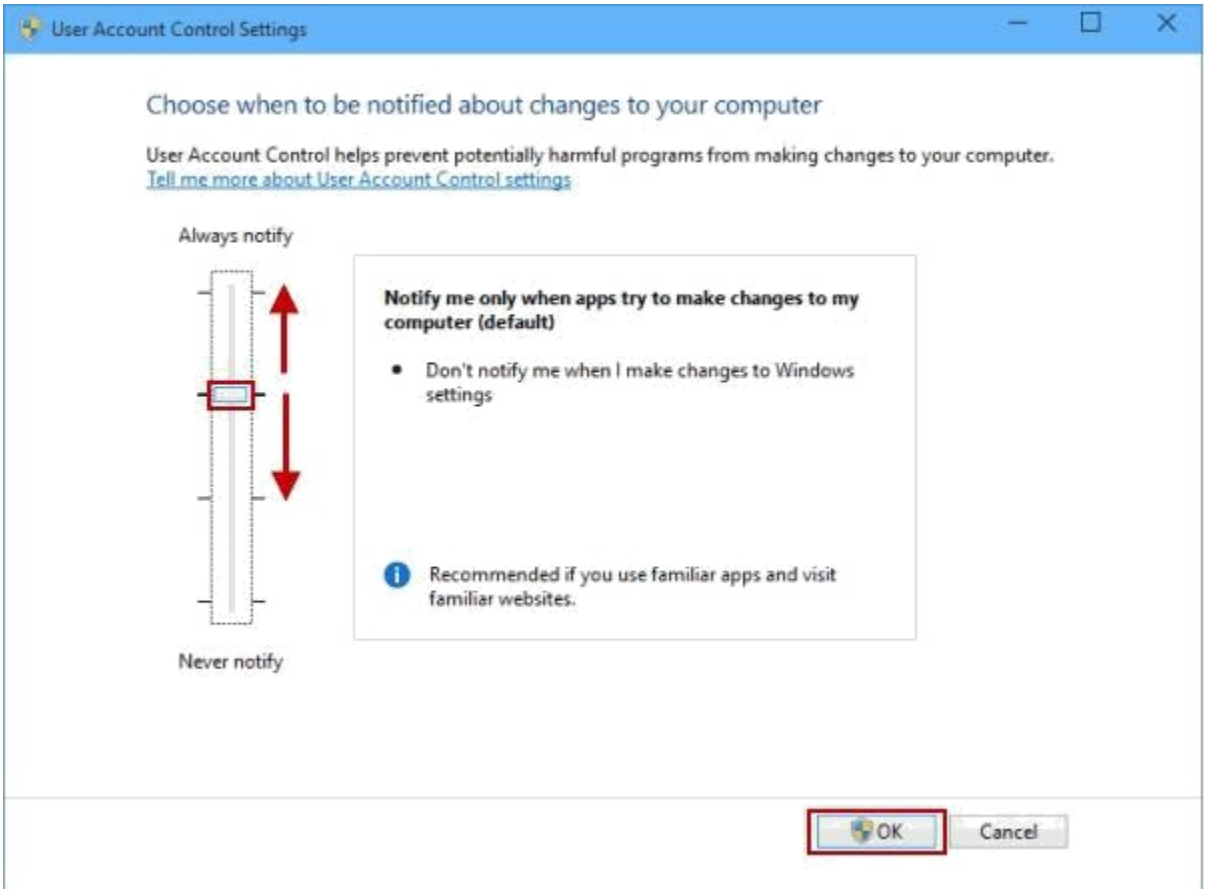
2. To change UAC settings in windows 10.



3. To change UAC settings in windows 10.



4. To change UAC settings in windows 10



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.

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 wouldeliminate 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.

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

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

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:

- Fixing boot-level startup problems (Startup Repair)
- Returning your system to a previous configuration (System Restore)
- Recovering your computer with a previously-created system image (System Image Recovery)
- Checking for defective memory (Windows Memory Diagnostic)
- 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:

1. Running Driver Verifier could cause the computer to crash.

2. You should only run Driver Verifier on computers that you are using for testing and debugging.

4. You must be in the Administrators group on the computer to use Driver Verifier.

5. Driver Verifier is not included in Windows 10 S, so we recommend testing driver

6. 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.

Previous Contents Next

CompTIA®A+ Core 2 Exam Notes : Troubleshooting mobile OS and application issues

examguides.com/Aplus-Core2/aplus-core2-19.htm

4. Software troubleshooting

4.2 Troubleshooting mobile OS and application issues

Common symptoms: Many mobile device problems have simple solutions that are really easy to diagnose and the repair is just as simple. When you encounter display problem on a mobile device diagnosis is usually simple the repair is another matter.

Dim display: In smartphones you should check the brightness settings to ensure that they have not been inadvertently changed. Many android devices allows to choose between manual settings of brightness and auto brightness.

Intermittent wireless: Almost all mobile devices include an internal wireless card. This is convenient, but it can be susceptible to interference between the device and the access point or cell tower. You can reduce the number of items blocking the signal between the two devices.

No wireless connectivity: When there is no wireless connectivity, it is usually because of one of two things.

- The wireless capability is disabled, it is easy to disable inadvertently. There can also be a hardware switch on the side, front, or back of the case.
- The wireless antenna is bad or the cable needs to be replaced.

When troubleshooting lack of wireless (Wi-Fi) connectivity, use the following steps:

- Power cycle the AP or wireless router
- Power cycle the device.
- On a smartphone check the wireless settings to ensure that WiFi is on. Also make sure that Airplane mode is off.
- Disconnect and reconnect
- Verify that the wireless device is using the correct password.

No Bluetooth connectivity: Bluetooth is also enabled and disabled with a key combination and can be disabled easily. In a smartphones and laptops problem may occur after an upgrade or update of some sort. This may due to some driver is missing from the upgrade or corrupted or overwritten during the upgrade process. Following are the things you can try on a smartphone.

1. Power cycle the device.
2. Remove the battery and put it back in.
3. Clear the Bluetooth cache.

Turn on Bluetooth from Quick Settings, in Android (all versions)

This method works same in all versions of Android, and it involves using Quick Settings.

1. To access them, flick downwards on the top side of the screen of your Android device. You should see several quick settings displayed.

If one of them has the Bluetooth symbol, tap on it. If you do not see the Bluetooth icon, you need to expand the list of quick settings. To do that, flick downwards one more time, on the top side of the screen or press the Expand icon on the bottom of your quick settings.

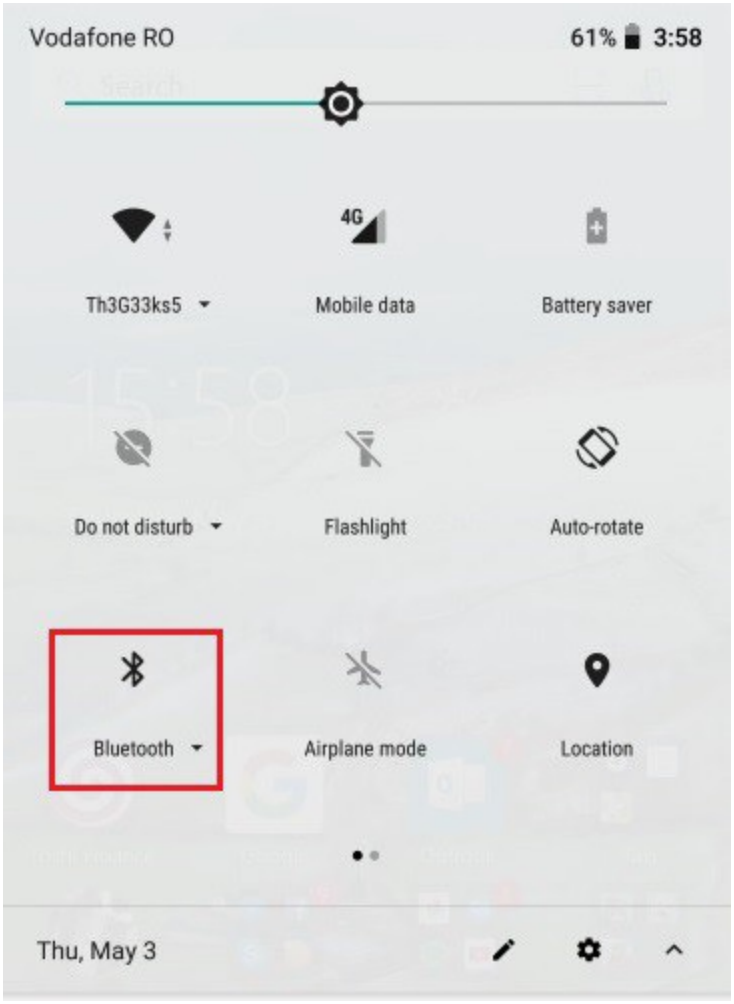
It looks like an arrow pointing downward. Then, tap the Bluetooth symbol to turn Bluetooth on. The Bluetooth symbol changes its color to signal that Bluetooth is now turned on.

Slow performance: Extremely short battery life and overheating – This condition is related to heat and also having too many apps open. Start your evaluation by feeling the temperature of the device in areas not related to the battery. Consult your documentation for specific heat related remedies. This could be a combination of too many apps exhausting your resources and generating unwanted heat. Shut the device down and let it cool. Restart it and use your application manager to see exactly what gets loaded at startup. Make adjustments to the apps for resource usage and monitor the device for a recurrence of the heat issue. And if the steps above don't work, you can always refresh the device back to its factory settings using the key combination from the manufacturer.

Unable to decrypt email: Most problems of this type are caused by a corrupted public key. You create your public key and share it with people you need to receive encrypted email from. If you can't decrypt email at all the focus of the problem would be on your machine. It appears your public key is corrupt. You should recreate your public key and share it with your confidential contacts.

Frozen system: In this case a system may lockup or freeze and it cannot be recovered. The only option is to do a soft reboot. Each manufacturer has a different method for rebooting from a lockup. Follow the manufacturer's instructions for doing this.

No sound from speakers: Occasionally, a device can be unknowingly put into silend mode, which will keep sound from being sent out of the speakers, headphones or other connected devices. You can usually raise the volume simply by clicking the up volume button. There are several different volume controls for sound. Below fig. Shows a typical android interface for sound controls. You can see that the Media sound is completely off, whereas all the other volume controls are set to allow audio volume.



You can check the volume controls on an android device by tapping Setitngs > Sounds and Vibration > Volume.

Touchscreen non-responsive: A non-responsive touch screen can have a variety of causes, to get back in.

1. If you have the screen protector remove it.
2. Turn the device off, and then clean the screen and your hands thoroughly.
3. Don’t reinstall the screen protector until it can be ruled out as a problem,
4. Restart the device and recalibrate the screen.

Apps not loading: When an app will not load on a mobile device, the first item to check is that the app is the right version for the device. Not all apps work on all devices. When an app has been working and now won't open or load when you access it, try the following items.

1. Check whether there is an update for the app.
2. Force the app to quit.
3. Before downloading the app make sure that you have enough space for the app.

4. If the app is resource intensive, ensure that your device has the resources to run the app.

Previous Contents Next

CompTIA®A+ Core 2 Exam Notes : Troubleshooting mobile OS and application security issues

examguides.com/Aplus-Core2/aplus-core2-20.htm

4. Software troubleshooting

4.3 Troubleshooting mobile OS and application security issues

Mobile security aims to protect personal and business information that is stored on, or transmitted to and from, mobile devices. It relates to all aspects of security, from malware threats to mitigating risk and securing mobile data in case of unauthorized access, theft or accidental loss of a mobile device.

Tools used to troubleshoot mobile OS security issues

1. Antimalware: An essential software for defense against all virus, malware and exploits is a good antimalware program. The mobile platform requires smaller more efficient apps than the desktop versions. Apps like Malwarebytes, Pegasus, and Lookout have both Android and iOS versions. These programs detect malicious programs by comparing it to known malware called signatures. Each particular malware has a specific digital footprint. As the malware evolves it will alter itself and change its footprint to avoid detection. The antimalware signatures need to be updated as frequently as possible to keep up with the evolution of the threats. Also, these applications are able to detect the slight changes that malware makes to itself and have the capability to detect malicious behavior.

2. App scanner: App scanners check the apps on your device for security vulnerabilities. This is another area where the need for real-time detection is clear. In addition to checking installed apps, it is important to have the ability to scan apps before they are installed.

3. Factory reset/Clean install: There are a number of reasons why you might need to factory reset your Android phone. Maybe your phone is overloaded with apps and running slow, or you've downloaded a recent update and it's causing problems with your phone's functionality.

Or maybe you want to reset to the factory settings because you're selling your phone. A factory reset is the ultimate cleansing of your Android device. When you perform a factory reset you're essentially wiping out everything you've ever done to the phone or tablet and restoring it back to the basic manufacturer software. It wipe out any core application updates you've downloaded or installed after buying the phone. Or put it another way, factory reset your phone to the state when you bought it.

It's highly recommended that you do some precautions before doing the factory reset.

1. Back up any important files to your PC or external storage.
2. Make sure your contacts are synced with your Gmail account.
3. Write down a list of apps you may want to reinstall.

Following are the steps to Factory Reset Android phone

1. Open the Settings menu on your device.
2. Under the Personal category, select "Backup & Reset."
3. At the bottom, you will see "Factory data reset."
Once you select to factory wipe your device, all info will be wiped including contacts (unless they're synced to your Google account), pictures, documents, and everything else. It returns the device to as it was when you just bought it.
4. After selecting Factory data reset, click "Reset phone" to confirm the reset.

Once hit, the device boots into recovery and wipes it clean. After it is done, it will reboot and your device will act as if it is brand new with all of its content gone.

4. Uninstall/reinstall apps: When you encounter an unusual behavior in an app, try stopping and restarting the app. If that does not work try restarting the device. If the problem is still unresolved, you need to remove the app by uninstalling it. Then obtain a fresh install file from the play store or App Store and install. The online store retains a record of all previously installed apps to help you choose your new installation files.

5. WiFi analyzer: WiFi analyzer can help you to identify Wi-Fi problems, find the best channel or the best place for your router/access-point by turning your PC/laptop, tablet or mobile device into an analyzer for your wireless network. WiFi analyzers can provide signal

strength metrics and quality information. It also addresses security vulnerabilities including the location and activity of unauthorized devices. Traditionally WiFi analyzers were dedicated devices. The mobile device are capable of supporting a WiFi analyzer app making wireless network analysis and threat detection more accessible as opposed to the expensive dedicated instruments.

6. Force stop: Sometimes during app troubleshooting, you will attempt to uninstall an app only to fail. An app that is reported as in use will not uninstall. Use Settings > Apps to force a running app to stop. This will usually facilitate the uninstallation.

7. Cell tower analyzer: A cell tower analyzer can be used by technicians to measure the signal strength across a network and assist in device placement to provide uniform coverage.

8. Backup/Restore: Apple devices have flexibility in the backup and restore process. Itunes can be used to backup, sync mobile content with your MAC or PC. Then it can be used to restore content from the computer to the mobile device. The size of the backup is only limited by the available space on the Mac/PC. Encrypted backups can be selected but encryption is off by default. Apple Configurator can be used to manage profiles, apps and backup settings including wiping the device and selectively create an instance with the iOS and individual apps to be deployed. The configurator can work with the iCloud and is scalable to configure multiple devices. It does not perform backup and sync, it configures the device to perform these functions.

9. Google sync: Google sync has been replaced by GoogleDrive to synchronize mail, contacts, photos and other selected content for the personal user. Google Sync is only available to G Suite, Drive for Work, Government, and Education customers. The Google Drive provides up to 15GB free storage with a Gmail account. Download Google Drive and a Google Drive folder will be created and you can select files in the Cloud to be synchronized with your mobile device. Desktop/laptop GoogleDrive folders begin synching immediately.

10. OneDrive: Microsoft's OneDrive is available to Windows, Android and iOS devices. It offers 5GB of free storage which can be increased to 1TB with an Office 365 subscription.

11. Itunes: Itunes is a media player and media library application developed by Apple Inc. It is used to play, download, and organize digital audio and video on personal computers running the OS X operating system and the iOS-based iPod, iPhone, and iPad devices, with editions also released for Microsoft.

12. iCloud: iCloud is a cloud storage and cloud computing service from Apple Inc. The service allows users to store data such as music and iOS applications on remote computer servers for download to multiple devices such as iOS-based devices running iOS 5 or later, and personal computers running OS X 10.7.2 "Lion" or later, or Microsoft Windows

(Windows Vista service pack 2 or later). iCloud is Apple's cloud-storage subscription service. iCloud Drive is like an external hard disk in the sky. Available for iOS devices, Macs, and Windows PCs. You can access all of your files and data from any device.

Steps to Sync Contacts from iPhone 4s/5/5s/6/6s to Mac via iCloud:

1. On your iPhone, tap Settings > iCloud > Sign in with your Apple ID > Find Contacts option here and toggle it to ON.
2. On your Mac, if you haven't enabled your iCloud on Mac, you should set it up first. Go to System Preferences > Find and open iCloud > Sign in with your Apple ID > Select Contacts to enable it. After that, all your iPhone contacts are synced to your Mac via iCloud.

Note: OSX Mavericks v.10.9 or later, your contacts, calendars, and other info are updated on your computers and iOS devices via iCloud.

When installing a third party application such as iTunes on your PC, ensure that the following recommendations are fulfilled:

1. You have administrative rights to the computer
2. Get latest Windows updates.
3. Disable any conflicting software; you can use MSCONFIG utility to troubleshoot the problem in Windows 7/8/8.1/10
4. Make sure your folder names don't contain strange characters
5. Additionally, if you are installing unsigned software, you will be prompted whether you are willing to go ahead with the installation. You must accept to the risks to complete the installation.

Example: The problem is that Jason was not able to update contacts and getting an error "Unable to Connect to the Server". The problem may be solved by:

1. Checking the health of the iCloud server. If the iCloud server is down, usually, it will be fixed by the company in a few minutes.
2. Verifying his login credentials. Sometimes, if you are not able to connect to the iCloud, it might be due to verification failure. Just login to iCloud from both your iPhone and the desktop and verify login credentials. In most cases, this will solve the problem. You may need to restart your devices before doing this and close any other applications before verifying your credentials.

Pairing: Establishing a connection between two Bluetooth devices is called pairing. For example, to pair a headset with a phone, the phone is configured to "Discoverable" mode and the headset is setup to pair by pressing one or more keys for some number of seconds. The headset finds the phone and establishes a connection using an assigned passkey (if any).

Previous Contents Next

CompTIA®A+ Core 2 Exam Notes : Given a scenario use appropriate safety procedures

examguides.com/Aplus-Core2/aplus-core2-21.htm

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\ .
- 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.

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.

Previous Contents Next

CompTIA®A+ Core 2 Exam Notes : Demonstrate proper communication techniques and professionalism

5. Operational Procedure

5.2 Demonstrate proper communication techniques and professionalism

- You have informed a customer that you would attend to his work at 10 AM sharp. However, due to some exigency, you are going to be late by a few hours. In such a case The customer would be expecting you at the specified time. It is appropriate to call the customer over phone, and inform him that you would be late. Sending an email may not be the best option, since the customer may not see his/her email often. Your colleague may not convey the message to your customer appropriately.
- If the customer complains that scanner is not working , you need to gather information regarding the problem. For example, knowing that the scanner was working previously, would make troubleshooting much easier.
- While doing any hardware up gradation on a laptop (such as adding more memory, etc), remember to remove the battery in addition to unplugging of AC mains.
- A junior technician is replacing a memory card on a PC, but does not have his grounding strap. Having an anti-static work station is the most appropriate solution when working with sensitive components. However, under emergencies, it may not always be possible to wear a wrist strap or have an anti static work station.
- Chain of custody: Chain of custody (CoC) refers to the chronological documentation or paper trail, showing the seizure, custody, control, transfer, analysis, and disposition of physical or electronic evidence. Chain of custody ensures that the evidence is not tampered with when presented in a court.

The following are the best practices that a computer technician should exercise:

a. Maintain a positive attitude
b. Listen and do not interrupt the customer
c. Be culturally sensitive
d. Be on time (if late contact the customer)
e. Avoid distractions like personal calls, taking co-workers, etc.
f. Avoid arguing with customers and/or being defensive
g. Follow-up with the customer about any installation or repair activity
h. Properly document any activity

A user's PC has been confiscated for prohibited use. So before giving the PC to another department technician needs to document change of custody before giving the PC to another department.

When you are attending to the maintenance of a clients computers from time to time. On one occasion, you notice that one of the systems have a lot of inappropriate content. In such case you need to report the matter using proper channel first.

If technician finds a prohibited content in a computer located in a common area that is used by several employees, in such a case any inappropriate material should be reported to the management for necessary action. The reporting structure needs to be maintained in an organization.

A customer calls you, because a solution that was earlier suggested by another technician did not appear to have solved the problem. Ask the customer to explain the problem. It is possible that you would be able to resolve the same without escalation. Decide if you need to escalate the issue after carefully reviewing the problem.

CompTIA®A+ Core 2 Exam Notes : Processes for addressing prohibited content/activity, and privacy, licensing, and policy concepts

examguides.com/Aplus-Core2/aplus-core2-23.htm

5. Operational Procedure

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

Incident Response: In some cases violations may be innocent transgressions attributed the employee's misinterpretation of the rules and in others, they may be flagrant violations with legal implications. In either case, regardless of how you become aware of the violation, it is important that you adhere to the policies that relate to your handling of the situation. You may be tempted to err on the side of leniency in some matters. This is NOT your decision to make. In the worst case, failure to report incidents could make you an accomplice. Every company has slight terminology variations as to what is and is not acceptable use. The fundamental principles will be the same. For example, every company will have an Acceptable Use Policy (AUP) that is part of the employment agreement and is also freely available for employee review. Read it completely and follow it to the letter.

Open source vs. commercial license: Software can be generally classified two ways. Open source (freeware) where the source code is freely available and can be modified by subsequent developers providing that any derivative works remain freely available and there are no fees for its use. This software is developed by and for a community that values the betterment of the product over financial reward.

Types of Licenses

1. Personal License

2. Enterprise licenses

1. Personal License: Licenses are purchased by the company and can be used by any single person within this organization. A Personal license is an option for private individuals who purchase a license with their own funds, and solely for their own use. Personal licenses are not to be purchased, refunded or in any way financed by companies.

2. Enterprise licenses: Enterprise License means a non-exclusive, non-transferable license to install and operate the Software Products, on any applicable media, without quantity or limitation.

Personal license vs. enterprise licenses: When using commercial software the licensing is purchased based on the intended use. Personal use is defined a single user installing the product on the personal devices in his home (domicile). In the corporate environment, products are usually covered under an enterprise site license that grants use to all employees. If the software is particularly expensive or use is confined to a small group or department, a per-seat license may be more cost effective. This license limits the installations to a predetermined number of users.

Regulated data

PII (Personally identifiable information): PII is any piece of information about a user that can be used alone or in combination with other pieces of information to identify an individual user. While it is the responsibility of all organizations to protect PII that they may possess, it is especially important in certain regulated industries such as healthcare and finance.

PCI(Payment Card Industry): PCI encourages and enhances cardholder data security and facilitates broad adoption of consistent data security measures globally.

GDPR (General Data Protection Regulation): The GDPR applies to EU-based organizations that collect or process the personal data of EU residents and to organizations outside the EU that monitor behavior or offer goods and services to EU residents.

PHI(Protected Health Information): PHI, also referred to as electronic protected health information (EPHI or ePHI), is any individually identifiable health information, provides guidelines for implementing the Health Insurance Portability and Accountability Act Security Rule.

Digital Rights Management(DRM): Explains what rights a user has to use a document or media. DRM protection is built into publicly sold media such as DVDs, and also downloaded content such as from the iTunes store.

European User License Agreement(EULA): EULA is a legally binding contract stating that you abide by the terms of use of the software you are about to install. You can only have one active copy on a PC you own, so you cannot run multiple copies at the same time.

An acceptable use policy(AUP): AUP is a document that outlines a set of rules to be followed by users or customers of a set of computing resources, which could be a computer network, website or large computer system. An AUP clearly states what the user is and is not allowed to do with these resources.

An original equipment manufacturer(OEM): Traditionally is defined as a company whose goods are used as components in the products of another company, which then sells the finished item to users.

Utilizing proper power devices is part of a good preventative maintenance plan and helps to protect a computer. You need to protect against several things:

- Surges
- Spikes
- Sags
- Brownouts
- Blackouts

A **surge** in an electrical power means that there is an unexpected increase in the amount of voltage provided. This can be a small increase or a larger increase known as a spike. A spike is a short transient in voltage that can be due to a short circuit, tripped circuit breaker, power outage, or lightning strike.

A **sag** is an unexpected decrease in the amount of voltage provided. Typically, sags are limited in time and in the decrease in voltage. However, when voltage reduces further, a brownout could ensue. During a brownout the voltage drops to such an extent that it typically causes the lights to dim and causes computers to shut off.

A **blackout** is when a total loss of power for a prolonged period occurs. Another problem associated with blackouts is the spike that can occur when power is restored. In the New York area, it is common to have an increased amount of tech support calls during July; this is attributed to lightning storms. Quite often this is due to improper protection.

Some devices have specific purposes, and others can protect against more than one of these electrical issues. Few of these devices are

Material Safety Data Sheet (MSDS): Each type of equipment that has a potential environmental risk associated with it has a MSDS. It provides information on hazardous chemicals present in various materials. The topics include composition of ingredients, handling and storage methods, lethal dose information, and toxicology and ecology. The aim of MSDS is to inform people about the adverse effects of various chemicals and how to properly handle these chemicals. You can obtain this sheet from the manufacturer or from the EPA. The Web site is www.epa.gov.

MSTSC: The Microsoft Terminal Services Client, currently known as Remote Desktop Services, is a component of Microsoft Windows that allows users to take control of a virtual machine or remote computer over a network connection.

Previous Contents Next

CompTIA®A+ Core 2 Exam Notes : Windows7 Upgrade & Other features

examguides.com/Aplus-Core2/aplus-core2-24.htm

6. Appendix

6.1 Windows7 Upgrade & Other features

The following reserved characters can't be used in Windows file names

- < (less than)
- > (greater than)
- : (colon)
- " (double quote)
- / (forward slash)
- \ (backslash)
- | (vertical bar or pipe)
- ? (question mark)
- *(asterisk)

The default spool folder is located at: %SystemRoot%\SYSTEM32\SPOOL\PRINTERS. For example, if the OS is residing on C drive, the default location will be

C:\Windows\System32\spool\PRINTERS

The following editions of windows support the Aero Feature:

Windows 7 Home Premium,
Windows 7 Professional,
Windows 7 Ultimate, and
Windows 7 Enterprise

32-bit vs. 64-bit: If you want to move from a 32-bit version of Windows to a 64-bit version of Windows 7 or vice versa, you'll need to back up your files and choose the Custom option during Windows 7 installation. Then, you'll need to restore your files and reinstall your programs. 32-bit Operating systems (especially, workstation Operating Systems such as Win 7 32-bit) usually support only up to 4GB of memory due to address bus limitation. It is recommended to go for 64-bit operating system if you want to use more than 4 GB of memory.

Windows XP Mode for Windows 7 makes it easy to install and run your applications for 32-bit Windows XP directly from your Windows 7 32-bit or 64-bit based PC. It utilizes virtualization technology such as Windows Virtual PC to provide a Virtual Windows XP environment for Windows 7. Windows XP Mode provides only Windows 7 Professional, Ultimate, or Enterprise users the flexibility to run many older productivity applications in a virtual Windows XP environment on a Windows 7-based PC.

Windows Upgrade:

Upgrades to Windows 7 from the following operating systems are not supported:

Windows 95, Windows 98, Windows Millennium Edition, Windows XP, Windows Vista RTM, Windows Vista Starter, Windows 7 M3, Windows 7 Beta, Windows 7 RC, or Windows 7 IDS Windows NT Server 4.0, Windows 2000 Server, Windows Server 2003, Windows Server 2008, or Windows Server 2008 R2 Cross-architecture in-place upgrades (for example, x86 to x64) are not supported.