70-680 Study Guide

to be used as an internal resource only

Introduction

This *free* study guide is for Microsoft's 70-680 exam, Windows 7, Configuring. This guide is intended to be supplemental to your books and other study materials. If you find any corrections or would like to suggest additions, please contact me @MrNetTek2000@yahoo.com.

Installing, Upgrading, and Migrating to Windows 7 (14 percent)

- Perform a Clean Installation
- Upgrade to Windows 7 From Previous Versions of Windows
- Migrate User Profiles

Deploying Windows 7 (13 percent)

- Capture, Prepare, and Deploy a System Image
- Configure a VHD

Configuring Hardware and Applications (14 percent)

- Configure Devices
- Configure Application Compatibility
- Configure Application Restrictions
- Configure Internet Explorer

Configuring Network Connectivity (14 percent)

- Configure IPv4 and IPv6 Network Settings
- Configure Network Settings
- Configure Windows Firewall
- Configure Remote Management

Configuring Access to Resources (13 percent)

- Configure Shared Resources
- Configure File and Folder Access
- Configure User Account Control (UAC)
- Configure Authentication and Authorization
- Configure BranchCache

Configuring Mobile Computing (10 percent)

- Configure BitLocker and BitLocker To Go
- Configure DirectAccess
- Configure Mobility Options
- Configure Remote Connections

70-680 Study Guide

to be used as an internal resource only

Monitoring and Maintaining Systems that Run Windows 7 (11 percent)

- Configure Updates to Windows 7
- Manage Disks
- Monitor Systems
- Configure Performance Settings

Configuring Backup and Recovery Options (11 percent)

- Configure Backup
- Configure System Recovery Options
- Configure File Recovery Options

70-680 Study Guide - Perform a Clean Installation

Overview:

Windows 7 is the latest release of the Windows series of operating systems by Microsoft. It can be used on a range of personal computers like desktops, laptops, and notebooks.

This guide will help you to perform a custom installation or clean installation, which means installing a new Windows 7 operating system on a computer.

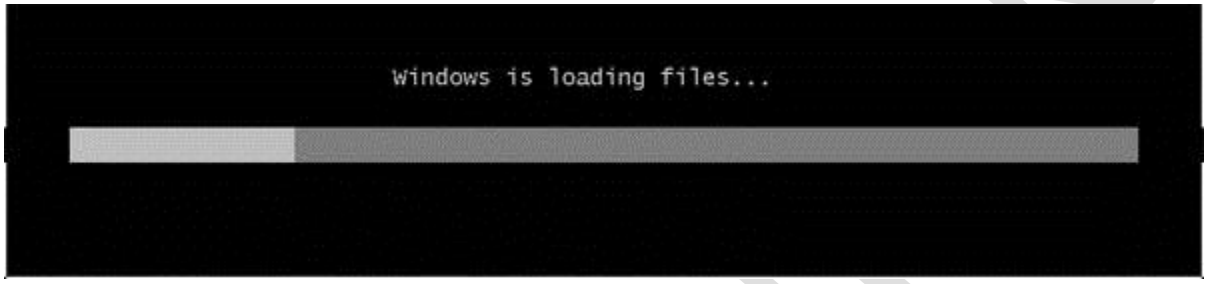
System Requirements:

Before installing Windows 7 on your computer, ensure that your computer has:

- 1 gigahertz (GHz) or faster 32-bit (x86) or 64-bit (x64) processor
- 1 gigabyte (GB) RAM (32-bit) or 2 GB RAM (64-bit)
- 16 GB available hard disk space (32-bit) or 20 GB (64-bit)
- DirectX 9 graphics device with WDDM 1.0 or higher driver

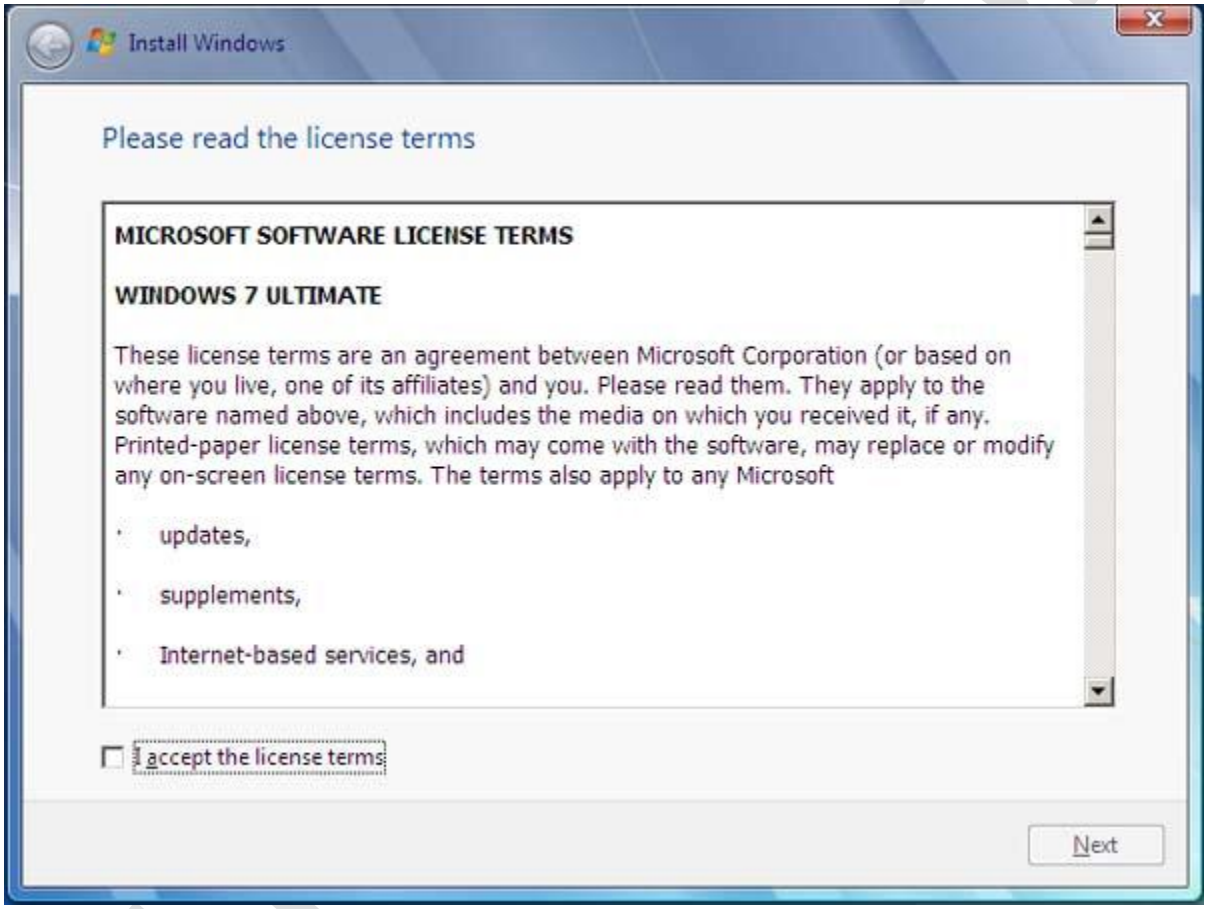
Clean Installation Instructions:

Insert the Windows 7 setup DVD into the disk drive. The Windows setup will automatically start the installation. If your computer does not start with the Windows 7 Setup DVD, then make the required changes in your BIOS and make your CD/DVD drive the primary boot device.

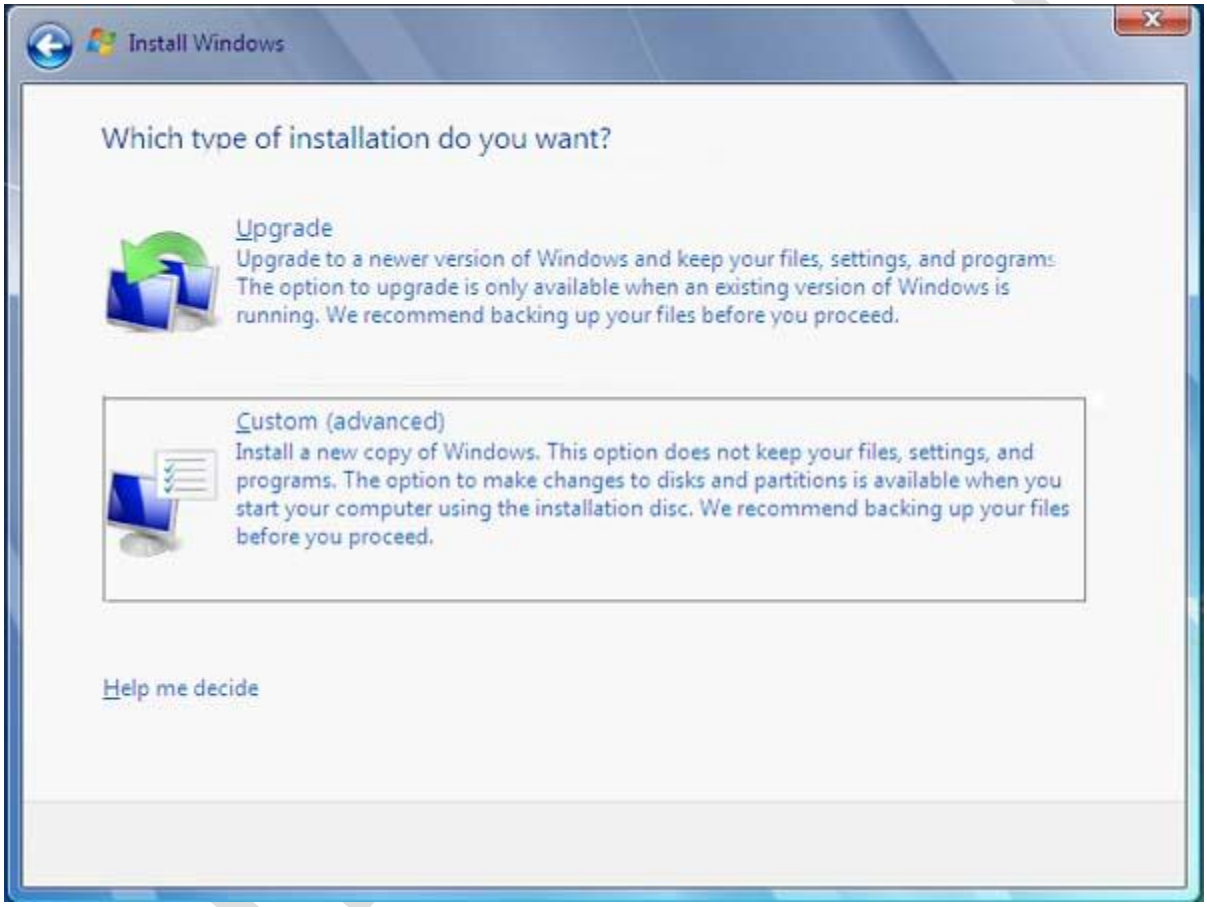


- Select the language that you want to use during the installation process.

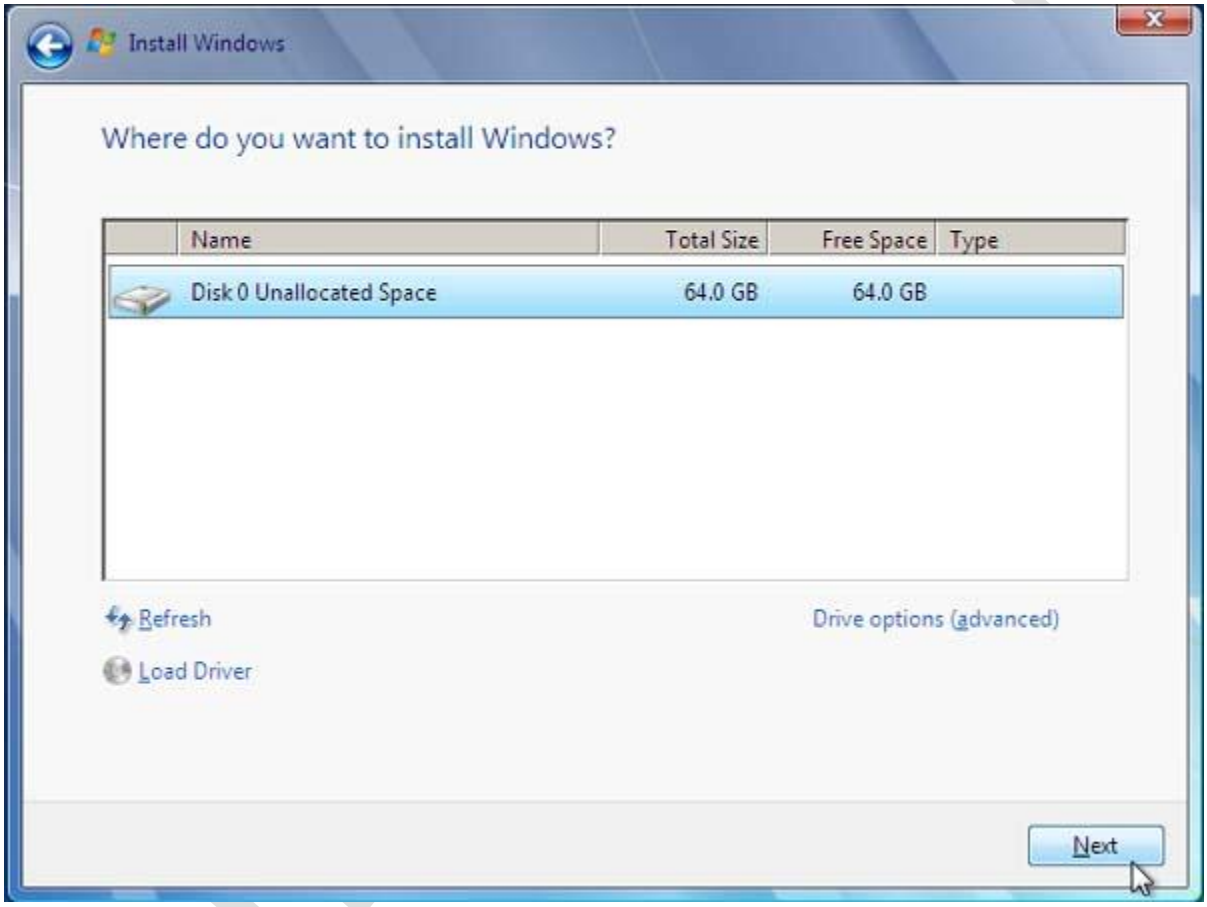
- Next, click the *Install Now* button to initiate the installation. The Setup transfers some temporary files from the DVD to your computer. The *Please read the license terms* page appears. Select the *I accept the license terms* check box.



- Select the *Custom (advanced)* install option.



- Select the hard disk drive or partition on which you want to install Windows 7.



- Setup copies the program files to your system.

- Toward the end of the installation process, your system restarts several times, and then Setup updates the registry settings. Next, Windows prompts you to perform some post-installation tasks, like selecting the user name and the computer name.

- Set the system password for your user account and enter a hint for the password.

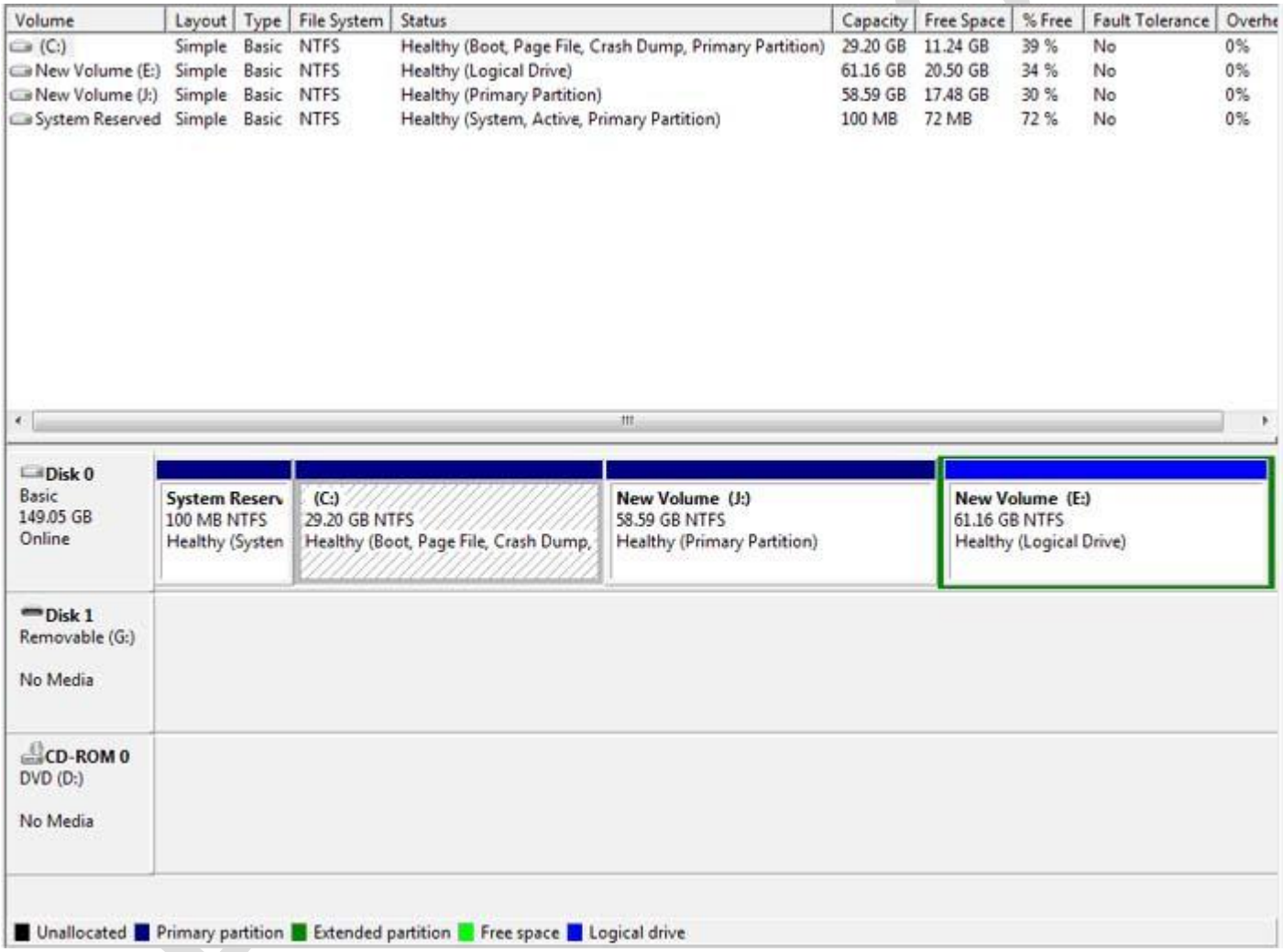
- Type the activation key.
- Set the date and time.
- Select the appropriate network settings and create a group depending on the type of Network you have chosen.
- Your Windows 7 installation is ready for use.

Dual Booting Windows 7 with Windows Vista:

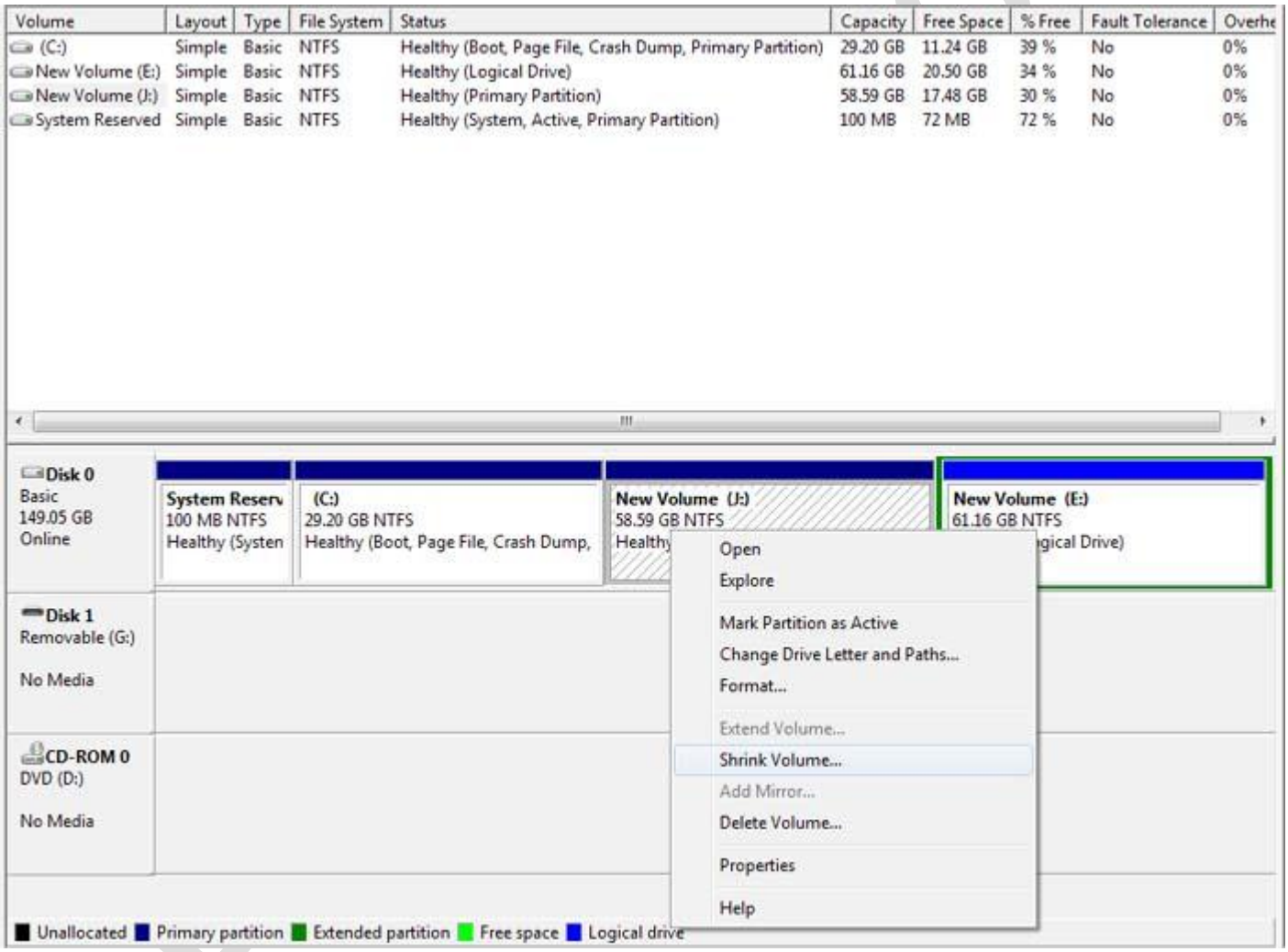
To install Windows 7 on a computer in dual boot mode, which is already running Windows Vista, follow these steps:

- If you need to create a new partition on your system's hard disk to accommodate the new operating system (Windows 7), follow these steps:

1) In Windows Vista, click *Start*, right-click *My Computer*, and click *Manage*.
2) Click *Disk Management* in the left pane. You can now view the current partitioning scheme on your system.

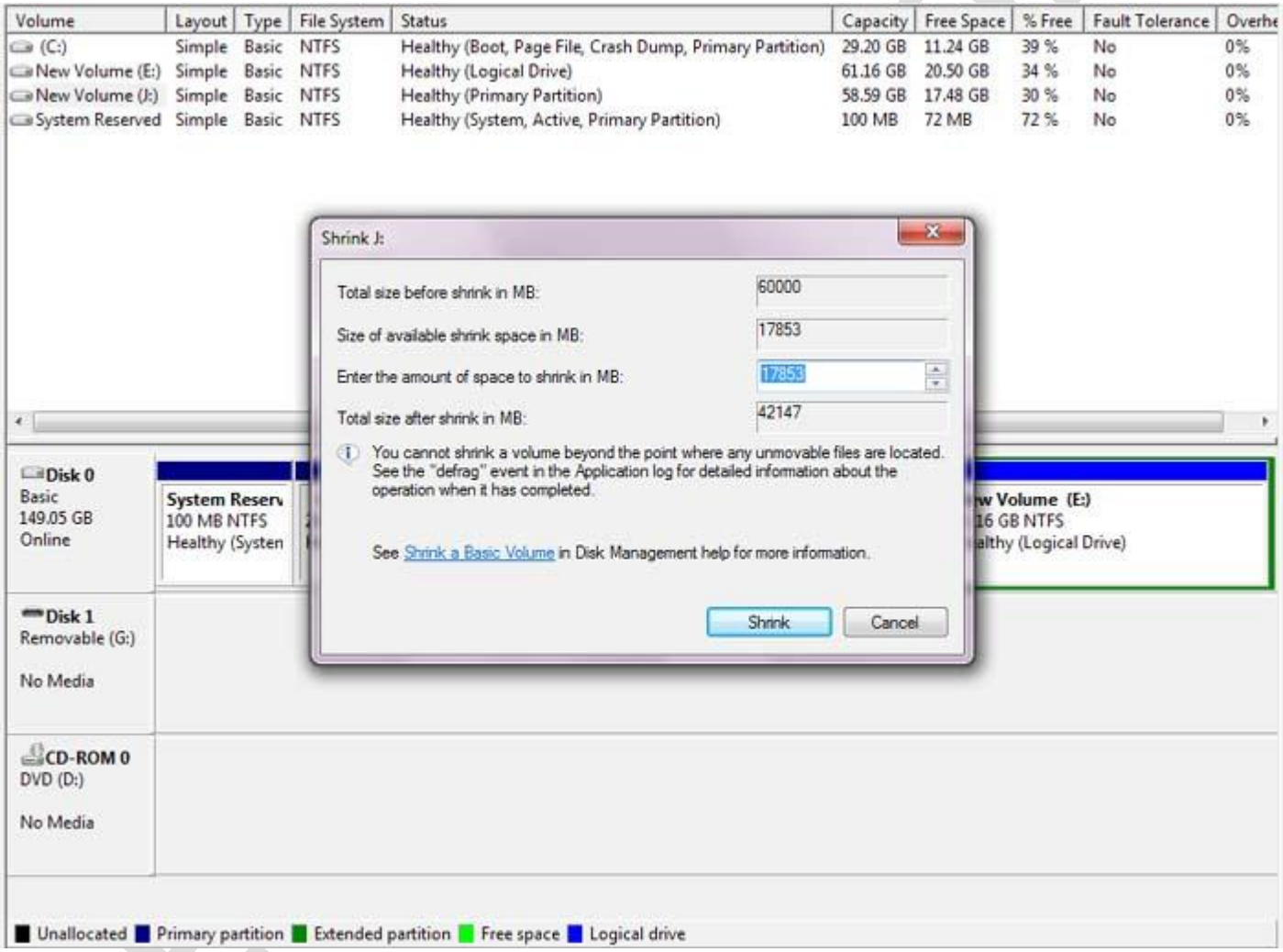


3) Right-click on the partition that you want to resize. The screen shows information on the capacity of the drive. In addition, it provides you the option to enter the amount you'd like to "shrink" your partition by. The recommended minimum partition size for Windows 7 is 16GB. Select 16GB or a larger size for your partition, and then click *Shrink Volume*.



70-680 Study Guide

to be used as an internal resource only



You can now see the unallocated space on your hard disk with the capacity you specified, situated just after your now resized original partition.

4) Right-click the unallocated volume, select New Simple Volume, and assign it a drive letter.
5) Perform Quick format of the new volume using the NTFS file system and the default allocation unit size. The volume label is optional, but you can assign it the label - Windows 7, which will help you to recognize the partition during installation process.

- After creating the partition, perform clean installation of Windows 7 by following procedure given earlier in this guide. After the installation process is complete, you'll have a new entry for Windows 7 on your boot screen when you first start-up your computer. On the boot screen, choose the Operating System with which you want to start your computer. Windows 7 can also be dual booted with Windows XP, or you can triple boot your system with Windows7, Windows XP and Windows Vista.

Installing Windows 7 From a USB Drive:

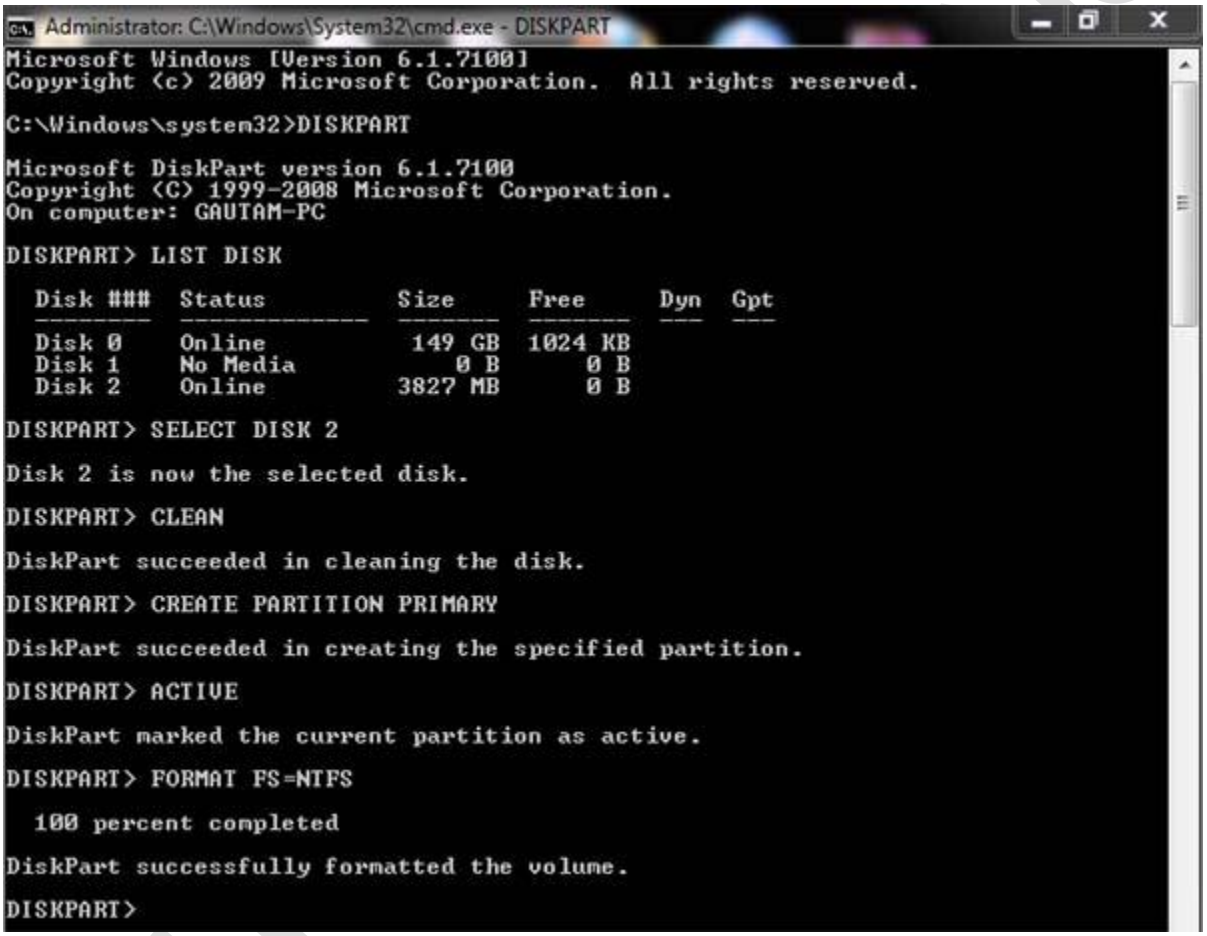
For this installation, you'll require the following:

- USB Drive (minimum 4 GB)
- Windows 7 installation files

Follow these steps to convert your USB drive into a bootable USB drive, which you can then use for Windows 7 installation:

1. Connect the USB drive. Note that the USB drive should not have any data. If it has any data, move your data to some other location.
2. Click Start, then click All Programs, and then click Accessories.
3. Right-click CMD, and select Run as administrator.
4. At the command prompt, type the following commands, as shown below:

   DISKPART
   LIST DISK (This command will list the disk numbers for all the hard disk drives and USB drives on your system.)
   SELECT DISK 2 (As system has listed the USB drive as DISK 2)
   CLEAN
   CREATE PARTITION PRIMARY
   ACTIVE
   FORMAT FS=NTFS (This process will take some time to complete)
   ASSIGN
   EXIT


Administrator: C:\Windows\System32\cmd.exe - DISKPART
Microsoft Windows [Version 6.1.7100]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Windows\system32>DISKPART
Microsoft DiskPart version 6.1.7100
Copyright (C) 1999-2008 Microsoft Corporation.
On computer: GAUTAM-PC
DISKPART> LIST DISK
Disk ### Status Size Free Dyn Gpt
Disk 0 Online 149 GB 1024 KB
Disk 1 No Media 0 B 0 B
Disk 2 Online 3827 MB 0 B
DISKPART> SELECT DISK 2
Disk 2 is now the selected disk.
DISKPART> CLEAN
DiskPart succeeded in cleaning the disk.
DISKPART> CREATE PARTITION PRIMARY
DiskPart succeeded in creating the specified partition.
DISKPART> ACTIVE
DiskPart marked the current partition as active.
DISKPART> FORMAT FS=NTFS
100 percent completed
DiskPart successfully formatted the volume.
DISKPART>

5. Insert your Windows7 DVD into the DVD drive and check the drive letter of the DVD drive. Suppose the drive letter is D. Type the following command at the command prompt:

   D: CD BOOT (where D is the drive letter for DVD)
   CD BOOT

6. Next, type the following command at the command prompt:

   BOOTSECT.EXE /NT60 F: (where F is the drive letter for the USB drive.)

7. Copy the contents of the Windows 7 installation DVD to the USB drive.

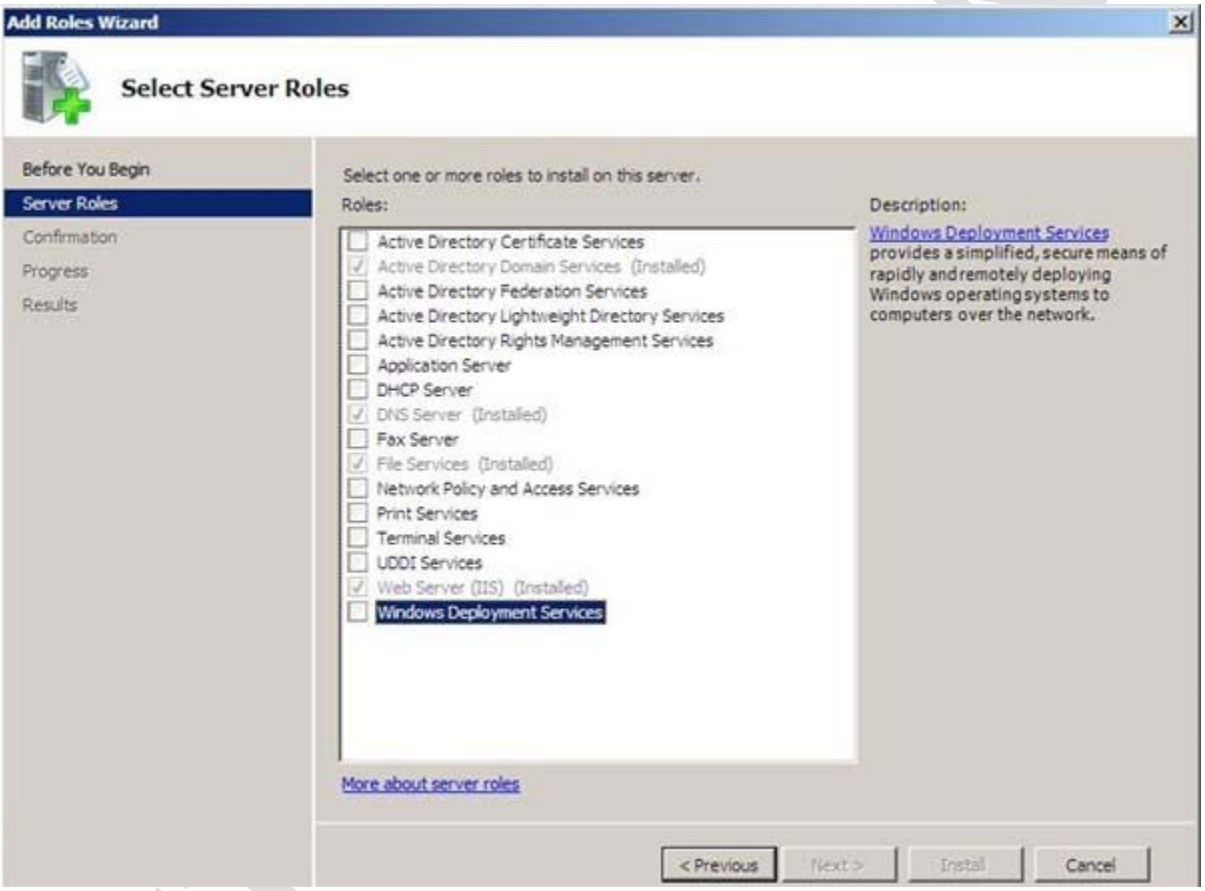
The USB drive is now ready for installation. You will need to change the BIOS to boot from the USB drive. To perform an installation using the USB drive, follow the procedure for clean installation of Windows 7 as given earlier in this guide.

Installing Windows 7 Using Windows Deployment Services:

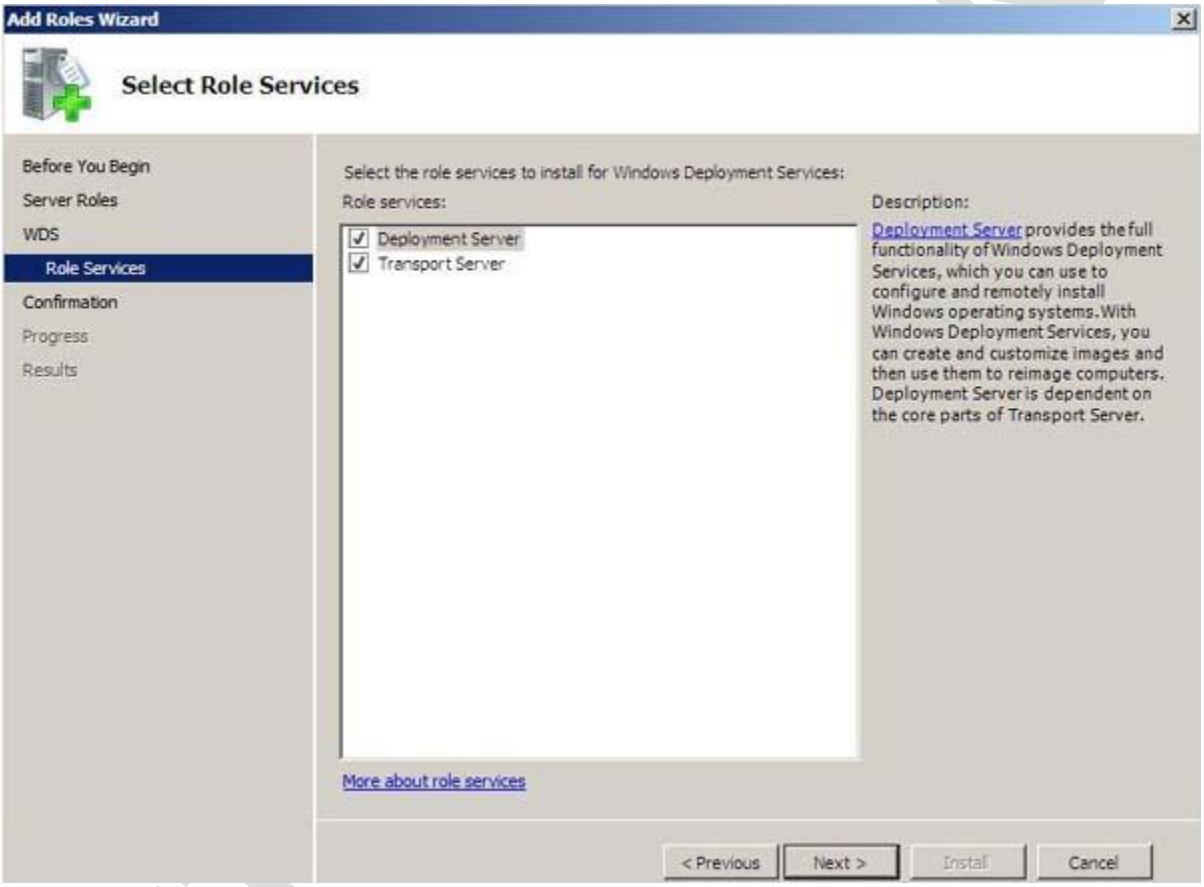
Windows Deployment Services (WDS) is the updated and redesigned version of Remote Installation Services (RIS). With WDS you can install Windows operating systems over the network. This eliminates the need to install Windows on individual computers using the local CD drive or DVD drive. WDS uses the Pre-Boot Execution environment (PXE) or Trivial File Transfer Protocol (TFTP) service on the host computer to boot from the WDS Server.

You need to install the WDS service on the computer that you want to use as a WDS Server. Here we'll install and configure this service on Windows Server 2008. On the WDS Server PXE and TFTP servers are required for network booting of the client on which installation is to be done. Follow these steps to install WDS on Windows Server 2008:

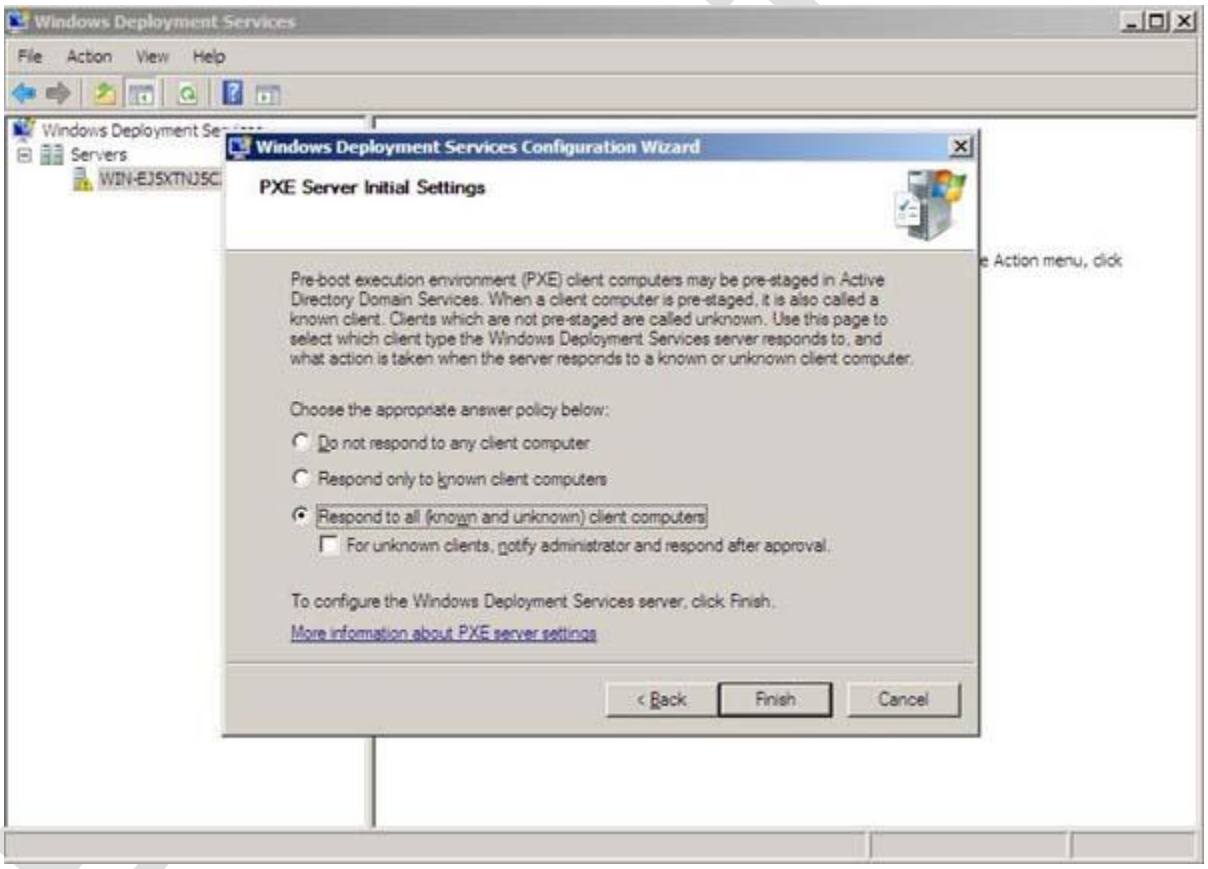
1. Open Server Manager, click *Add Roles* and then click *Next*.
2. On the Select Server Roles screen, select *Windows Deployment Services*, and then click *Next*.



3. On the Role Services screen, select *Deployment Server and Transport Server*, then click *Next* and then click *Install*.



4. Next, configure the PXE Server settings. Select *Respond to all (known and unknown) client computers* and then click *Finish*. Once a computer is linked to a computer account object in AD DS, the computer is considered "prestaged" or "known". For security reasons, you may opt to select PXE to only respond to known computers, or if you make the selection used in our instructions, you may want to click the *For unknown clients, notify administrator and respond after approval* checkbox.

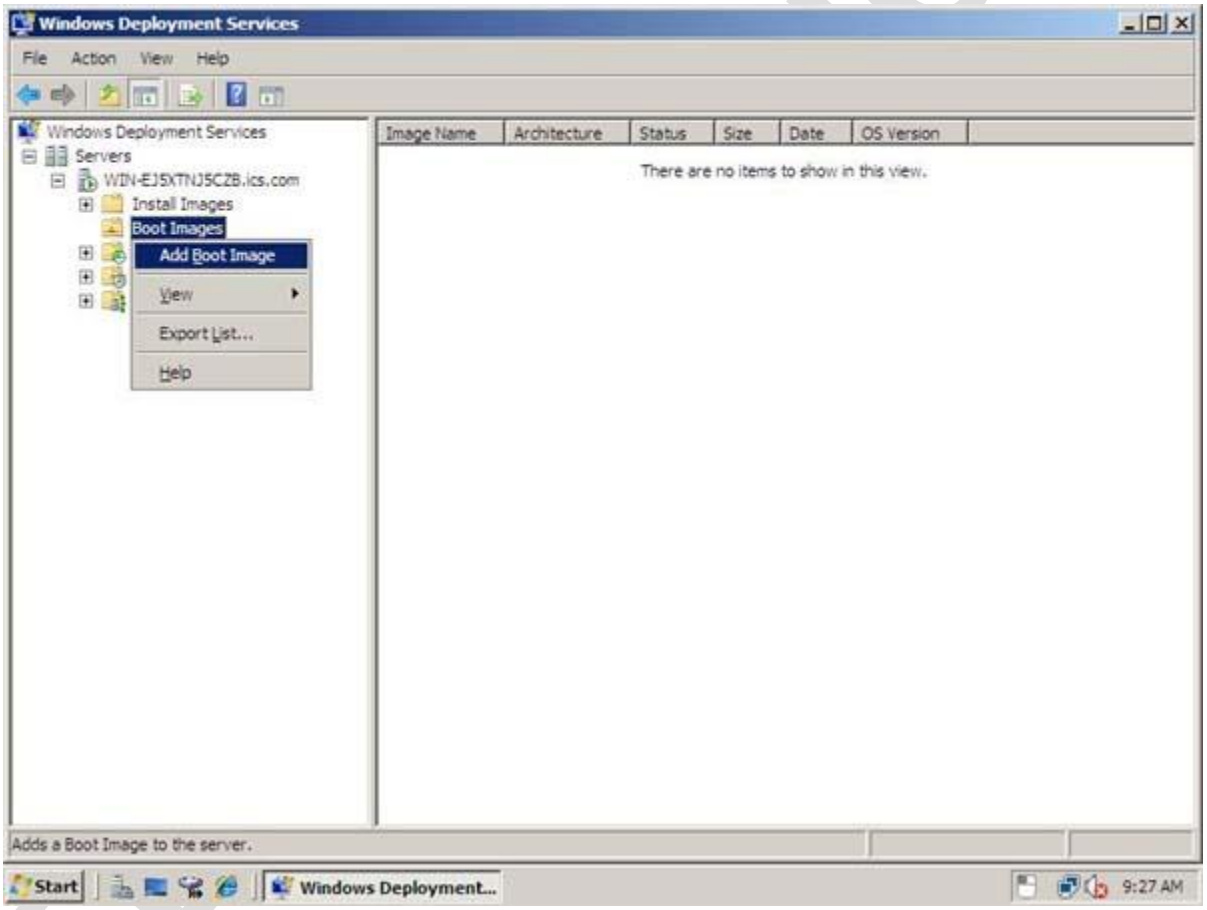


Adding a Boot image on the WDS Server:

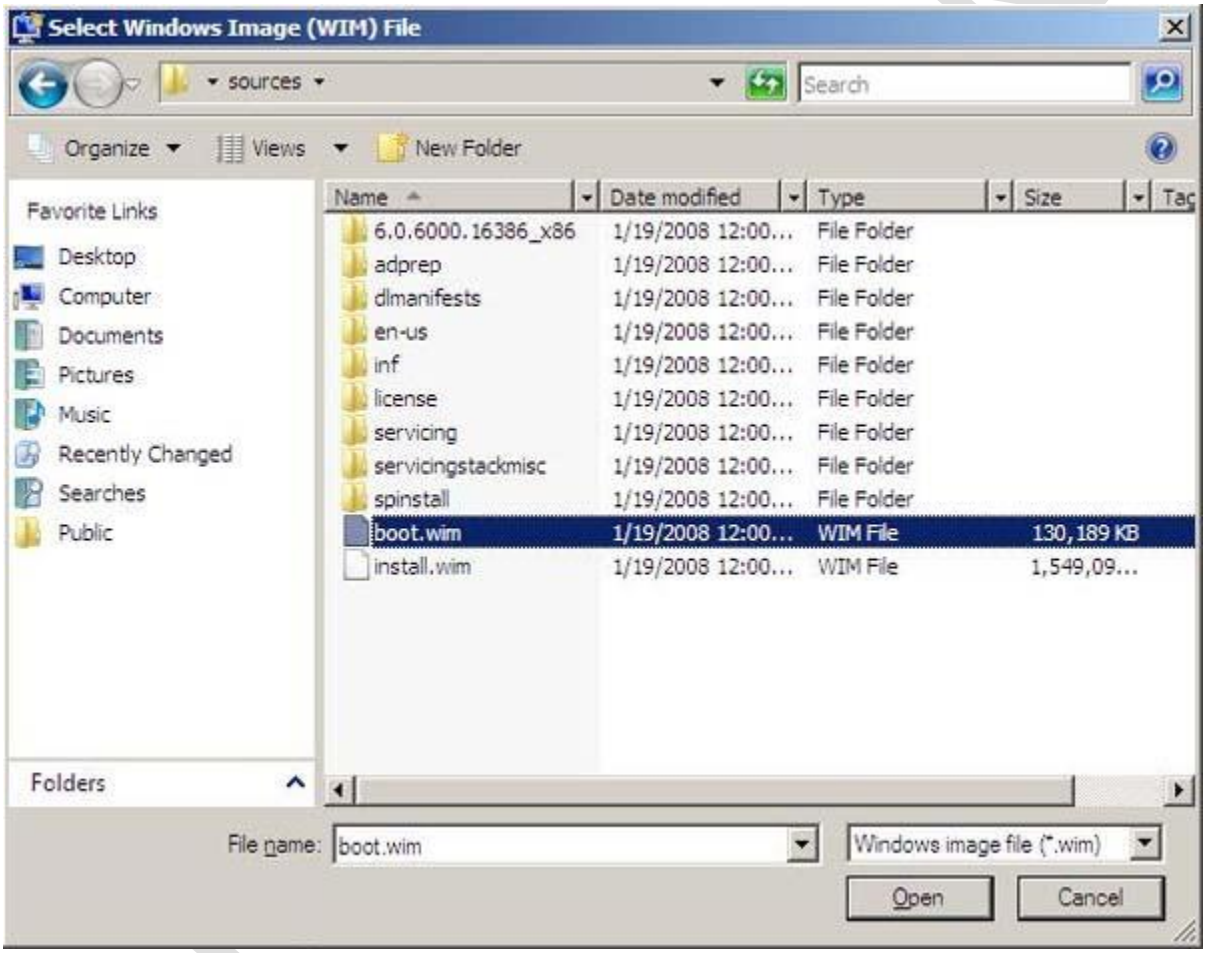
Boot images are Windows images that are used to boot a client computer, and install an operating system on the computer. To add a boot image on the WDS Server, perform these steps:

1. Click *Start*, then click *Administrative Tools*, and then click *Windows Deployment Services*.
2. Open the Windows Deployment Services management console.

3. Right-click the Boot Images node and then click *Add Boot Image*.

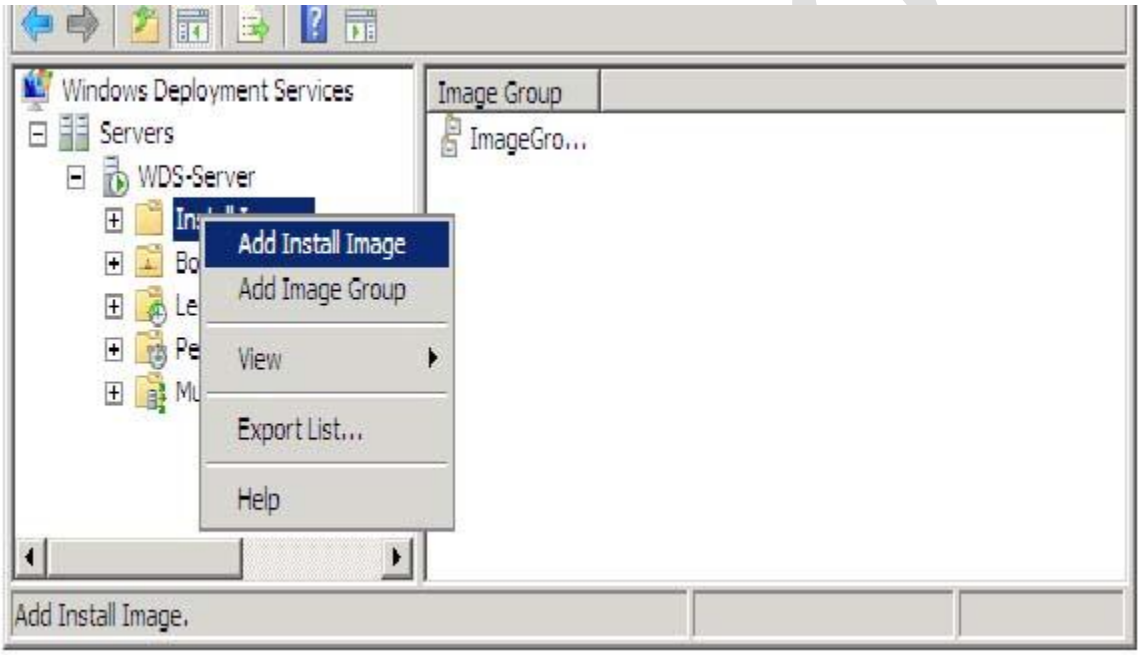


4. Click *Browse* to locate the boot image you want to add. Select *Boot.wim* from the /sources folder on the Windows 7 installation DVD.

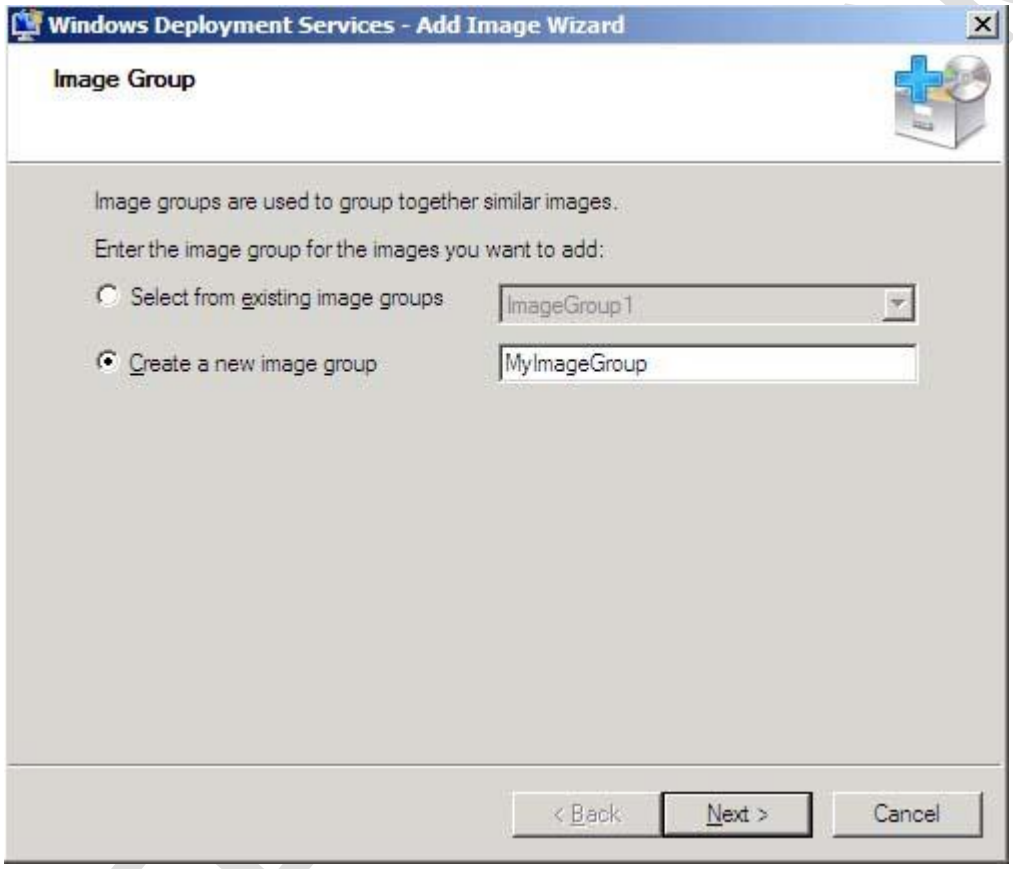


Adding an Install Image on the WDS Server:

1. Click *Start*, then click *Administrative Tools*, and then click *Windows Deployment Services*.
2. Open the Windows Deployment Services management console.
3. Right-click the *Install Images* node and then click *Add Install Image*.



4. Specify a name for the image group and then click *Next*.



5. Click Browse to locate the default install image (Install.wim), which is located in the \Sources folder of the product DVD, and then click *Open*.
6. Enter a name and click *Save*.
7. Next select *Upload image to WDS Server*.
8. Repeat the process if you want to add more than one Install Image to your WDS Server. You must add at least one boot image and one install image before you will be able to boot to the Windows Deployment Services server and install an image.

Installing From an Install Image:

After you have at least one boot and one install image on the server, you can deploy an install image assuming you meet the following requirements:

- The client computer must be capable of performing a PXE boot.
- Your user account must be a member of the Domain Users group.
- The client computer must have at least 512 MB of RAM, which is the minimum amount of RAM for using Windows PE.

- The client must meet the system requirements for the operating system of the install image.

To perform a PXE boot on a computer to install an image, use the following procedure.

1. Configure the BIOS of the computer to enable PXE booting, and set the boot order so that it is booting from the network first.
2. Restart the computer, and when prompted, press *F12* to start the network boot.
3. Select the appropriate boot image from the boot menu. (This boot image selection menu will be available only if you have two or more boot images on the server.)
4. Follow the instructions in the Windows Deployment Services user interface.
5. When the installation is completed, the computer will restart and Setup will continue as it would in a regular clean installation.

70-680 Study Guide - Upgrade to Windows 7 from previous versions of Windows

Upgrading Windows Vista to Windows 7:

Upgrades to Windows 7 from windows Vista are only supported by Vista Service Pack1 and Service Pack 2 editions. All the Windows Vista device drivers are compatible with Windows 7. Following type of upgrades are supported from Windows Vista to Windows 7:

- Windows Vista Home Basic (SP1, SP2) 32-bit (x86) and 64-bit (x64) can be upgraded to Windows 7 Home Basic, Home Premium and Ultimate 32-bit (x86) and 64-bit (x64).
- Windows Vista Home Premium (SP1, SP2) 32-bit (x86) and 64-bit (x64) can be upgraded to Windows 7 Home Premium and Ultimate 32-bit (x86) and 64-bit (x64).
- Windows Vista Business (SP1, SP2) 32-bit (x86) and 64-bit (x64) can be upgraded to Windows 7 Professional, Enterprise and Ultimate 32-bit (x86) and 64-bit (x64).
- Windows Vista Enterprise (SP1, SP2) 32-bit (x86) and 64-bit (x64) can be upgraded to Windows 7 Enterprise 32-bit (x86) and 64-bit (x64).
- Windows Vista Ultimate (SP1, SP2) 32-bit (x86) and 64-bit (x64).

Following types of upgrades are not possible from windows Vista to Windows 7:

- Cross-architecture in place upgrades (for example, x86 to x64) are not supported from Vista to windows 7.

- Cross-language in place upgrades (for example, en-us to de-de) are not supported.
- Cross-media type in-place upgrades (for example, from Staged to Unstaged or from Unstaged to Staged) are also not supported.

Follow these steps to upgrade Windows 7 from Windows Vista:

1. Insert the Windows 7 DVD. The DVD does not have an auto run option on the Windows Vista. Open the DVD drive in My Computer and double click setup.exe. (If you are performing an upgrade, the Windows installation process will not delete the old version. It will rename the Windows Root folder.) You can also use other media for installation like a USB drive or the downloaded Windows 7 setup. Click setup.exe file from the media that you are using for installation, to start the installation process.
2. Click *Install now* on the Install Windows screen begin the installation. You can also check the compatibility of your computer with Windows 7 operating system, by clicking *Check Compatibility Online*.
3. By selecting *Go online to get the latest updates for installation*, you can get the latest updates to help ensure a successful installation, and to help protect your computer against security threats. Your computer will need to be connected to the Internet during Windows 7 installation to get these updates.
4. On the Please read the license terms page, click *I accept the license terms*, and then click *Next*.
5. On the Which type of installation do you want page, click *Upgrade*. This will present you with compatibility report. This is used to help you determine what may not work properly after the upgrade.
6. Setup starts installing Windows 7 on your computer by copying the program files to your system. It will prompt you for a Windows login password, and password hint.
7. Type the activation key and Set the date and time.
8. Select the appropriate network settings and create a group depending on the type of Network you have chosen.

Upgrading Windows XP to Windows 7:

Windows 7 does not provide direct in-place upgrade for Windows 7 from Windows XP that will retain user's applications programs, settings, customizations, personalization and data during the upgrade process. If you try to upgrade to Windows 7 from a system which is using Windows XP, you will be shown this error report which informs you that direct upgrade from Windows XP to Windows 7 is not available.

You can perform an upgrade to Windows 7 from windows XP, by using Windows Easy Transfer wizard, that allows you to save Selected User Accounts, Files and folders, Windows settings, Program data files and settings from Windows XP computer and later on restore them on upgraded windows 7.

Follow these steps to upgrade XP to Windows 7:

1. On your Windows XP computer insert Windows 7 DVD.
2. Navigate to Support folder and open migwiz (migration wizard) folder and run migwiz.exe. It opens Windows easy Transfer window which initiates the process of File transfer.
3. It asks you for the media you wish to use to transfer your settings. Select the appropriate media from the options presented by the wizard.
4. It ask whether this is the New computer (in which you wish to copy the settings) or the old computer (from you wish to copy the settings) select old computer. The wizard will now start scanning system for your files.
5. Once scanning is complete it shows the list of user profiles and you can select the files and settings in each profile which needs to be transferred to Windows 7.
6. It asks you to provide a password for the data file. Provide a password for data security. Then press *Save*. Once the data is saved, Easy transfer tells you the location where the files are stored.

7. Close the Easy Transfer and open the Windows 7 Setup by browsing to the root folder of the DVD, and then double clicking *setup.exe*.
8. Click *Install now* on the Install Windows screen begin the installation.
9. By selecting *Go online to get the latest updates for installation*, you can get the latest updates to help ensure a successful installation, and to help protect your computer against security threats. Your computer will need to be connected to the Internet during Windows 7 installation to get these updates. If you don't want to check for updates during Setup, click *Do not get the latest updates*.
10. On the Please read the license terms page, click *I accept the license terms*, and then click *Next*.
11. On the Which type of installation do you want page, click *Custom (advanced)* to perform an upgrade to your existing Windows.
12. In the next step, select the partition where you want to install Windows 7. If you chose to install Windows 7 on a partition where your current Windows XP is installed, it will overwrite and if you have chosen to install on another drive, you can dual boot with XP.
13. Setup copies the program files to your system. Toward the end of the installation process, your system restarts several times, and then Setup updates the registry settings.
14. Windows prompts you to perform some post-installation tasks, like selecting the user name and the computer name.
15. Set the system password for your user account and enter a hint for the password.
16. Type the activation key. Set the date and time.
17. Select the appropriate network settings and create a group depending on the type of Network you have chosen.
18. Once your Windows 7 installation is complete, you can transfer the files that you copied from Windows XP. Boot your new Windows 7. Insert the USB or the external hard disk where you saved the transferred files.
19. Click *Start*, then click *All Programs* and then click *Accessories*.
20. Click *System Tools*, and then click *Windows Easy Transfer*. Once Easy transfer opens up, click the *next* button and select *An external hard disk or USB flash drive* from the options.
21. Select *This is my New computer*.
22. It asks you to browse the file which you created while copying data from old computer.
23. Click *Transfer* to transfer all files and settings. Once you select the file and click *open*, Easy Transfer will again scan for the user profiles available in the saved data. You can chose which files need to be migrated for which all users you have saved. You can customize the migration using the customize button below each profile.
24. When the transfer is complete click *Close*. Now all your files and settings which you saved from your XP installation will be available in Windows 7.

70-680 Study Guide - Migrate User Profiles

About User Profiles:

A Microsoft Windows user profile describes the Windows configuration for a specific user, including the user's

environment and preference settings. The user profile contains the settings and configuration options specific to the user, such as installed applications, desktop icons, and color options. The user profile contains:

- Desktop settings - screen colors, wallpaper, screen saver.
- Persistent network and printer connections.
- Mouse settings and cursor settings.
- Recently edited documents.
- Start-up programs, shortcuts, and personal groups.
- Settings for Windows applications - Notepad, Paint, Windows Explorer, Calculator, Clock, and more.
- Start menu settings - Programs that can be selected from the start menu.

The user profile settings are saved on disk and are loaded when the user logs on. User profiles in Microsoft Windows are of two types – Local and Roaming user profiles. Local profiles are only stored on the computer to which you log in. Roaming profiles are profiles that have been placed on a central server. When the user logs onto the domain, the roaming profile is copied to the local computer the user logged on from. If the user makes changes to the profile, they are saved to the local computer and the central server. When the user logs on from another computer the most recent of the local or server stored profile is used. Since Roaming profiles are downloaded when a user logs on, and uploaded when the user logs off, large user profiles degrade system performance. Using local profiles, and limiting the profile size shortens the time required to log on and off and improve system performance for all users.

User State Migration Tool (USMT):

The User State Migration Tool (USMT) 4.0, part of the Windows Automated Installation Kit (Windows AIK), is a command line-scriptable tool for migrating user state from one computer or operating system to another. It is designed for large-scale migrations whereas Windows Easy Transfer is for small-scale and individual transfers. USMT migrates files and settings between Microsoft Windows versions 2000, XP, Vista and Windows 7, and is useful in migrating user settings and files during OS upgrades. Migrations from 32-bit to 64-bit are supported, but from 64-bit to 32-bit are not supported by USMT. USMT can transfer:

- Selected User Accounts.
- Files and folders.
- E-mail messages, settings, and contacts.
- Photos, music, and videos.
- Windows settings.
- Program data files and settings.
- Internet settings.

A migration can be side-by-side or wipe-and-load. Side-by-side, sometimes called PC Replacement, migrates data from one computer to another via central storage such as a server. Wipe-and-load, sometimes referred to as PC Refresh, moves data to central storage and then back to the same PC.

For more information, read Common Migration Scenarios

USMT uses ScanState command to collect the files and settings from the source computer and LoadState to restore the user state onto the destination computer.

ScanState scans the source computer, collects the files and settings and creates a store. ScanState does not

modify the source computer. By default, ScanState compresses the files and stores them as an image file (USMT3.MIG).

LoadState migrates the files and settings from the store to the destination computer. LoadState migrates each file (one by one) from the store to a temporary location on the destination computer — the files are decompressed (and decrypted if necessary) during this process. Next, LoadState transfers the file to the correct location, deletes the temporary copy, and begins migrating the next file.

Migrating All User Accounts and User Settings Using USMT:

1. Log on to the source computer as an administrator, and at a command prompt type:
   scanstate \\fileserver\migration\mystore /i:miguser.xml /i:migapp.xml /o
2. Log on to the destination computer as an administrator.
3. Enter either of the two strings at a command prompt depending on your requirements:

   If you are migrating domain accounts, type:
   loadstate \\fileserver\migration\mystore /i:miguser.xml /i:migapp.xml

   If you are migrating local accounts along with domain accounts, type:
   loadstate \\fileserver\migration\mystore /i:miguser.xml /i:migapp.xml /lac /lae

Migrating 2 Domain Accounts (User1 and User2):

1. Log on to the source computer as an administrator, and specify:
   *scanstate \\fileserver\migration\mystore /ue:** /ui:domain1\user1 /ui:domain2\user2 /i:miguser.xml /i:migapp.xml /o*
2. Log on to the destination computer as an administrator.
3. Specify the following:
   loadstate \\fileserver\migration\mystore /i:miguser.xml /i:migapp.xml

Migrating 2 domain accounts (User1 and User2) - Move User1 From the NewYork to the Portland Domain:

1. Log on to the source computer as an administrator, and type the following at the command-line prompt:
   *scanstate \\fileserver\migration\mystore /ue:** /ui:NewYork\user1 /ui:NewYork\user2 /i:miguser.xml /i:migapp.xml /o*
2. Log on to the destination computer as an administrator.
3. Specify the following:
   loadstate \\fileserver\migration\mystore /mu:NewYork\user1:Portland\user2 /i:miguser.xml /i:migapp.xml

ScanState Syntax
LoadState Syntax

USMT Hard-Link Migration:

USMT 4.0 hard-link migration is a new feature that you can use to perform an in-place migration much faster

than by using traditional file copy mechanisms. Hard-link migration in USMT scans the computer for user files and settings and then creates a directory of hard links to those files. The hard links are remapped into the appropriate locations in the new operating system. The entire process typically takes a few minutes to run, does not duplicate files on the local disk, and can save several hours when upgrading to Windows 7. You can use USMT hard-link migration both online and offline.

Follow these steps to perform user profile migration:

1. Boot in to Windows XP. Insert Windows 7 DVD and run the setup.
2. Select *Clean Installation*. Once you come on the Hard drive selection screen select the partition on which you installed windows XP. (Let us assume that the partition on which you installed windows XP operating system is C). Then select *C:* and click *Next*.
3. On this screen you get a message that all files folders and settings of XP are moving to Windows.old and Windows will be installed on Windows folder. Click *OK*.
4. Let the setup complete until it reaches the desktop of Windows 7.
5. Install Windows AIK (Downloaded earlier) on your system.
6. Click *My Computer*, then click *C: Drive* and then click *Program Files*.
7. Click *Windows AIK*, then click *Tools*, and the click *USMT*.
8. In this folder, two more folders are there - x86 and AMD64. Both folders contain USMT files for both the architectures.
9. Now open a new Notepad file and copy the following text in it:

   If exist D:USMT.* xcopy D:USMT*.* /e /v /y C:WindowsUSMT*

   If exist E:USMT.* xcopy E:USMT*.* /e /v /y C:WindowsUSMT*

   If exist F:USMT.* xcopy F:USMT*.* /e /v /y C:WindowsUSMT*

   If exist G:USMT.* xcopy G:USMT*.* /e /v /y C:WindowsUSMT*

   If exist H:USMT.* xcopy H:USMT*.* /e /v /y C:WindowsUSMT*

   If exist I:USMT.* xcopy I:USMT*.* /e /v /y C:WindowsUSMT*

   If exist J:USMT.* xcopy J:USMT*.* /e /v /y C:WindowsUSMT*

   If exist K:USMT.* xcopy K:USMT*.* /e /v /y C:WindowsUSMT*

   Cd c:windowsusmtx86

   scanstate.exe c:store /v:13 /o /c /hardlink /nocompress /efs:hardlink /i:MigApp.xml /i:MigDocs.xml

   /offlineWinDir:c:windows.oldwindows

   loadstate.exe c:store /v:13 /c /lac /lae /i:migapp.xml /i:migdocs.xml /sf /hardlink /nocompress

   :EOF

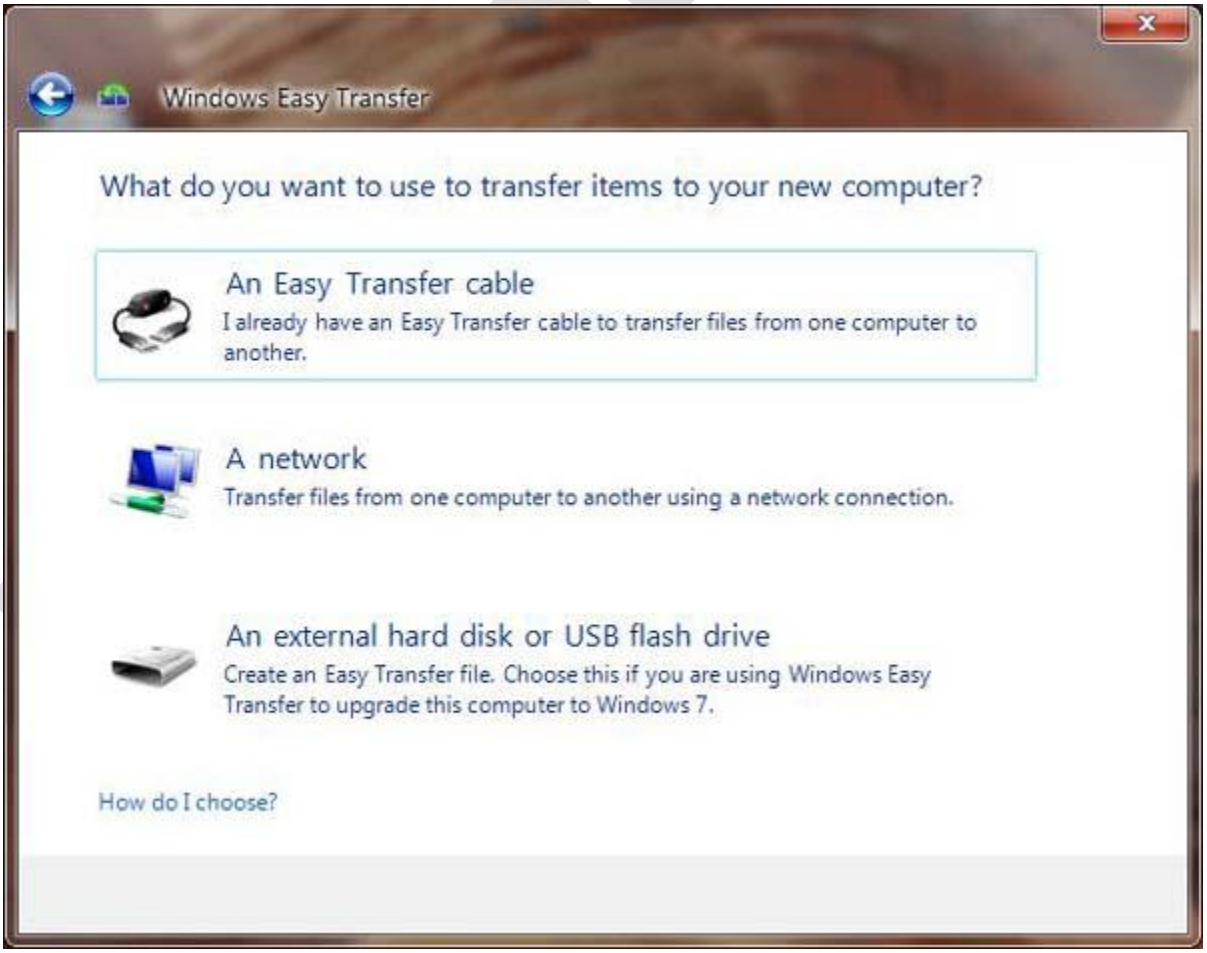
10. Save this file with .bat extension and copy it to the *C:/Program Files/Windows AIK/Tools/USMT* folder.
11. Right-click the file and click Run as Administrator.
12. After this, USMT will start transferring your files and folders and settings into Windows 7 from XP. After the process is complete, you will notice that your desktop icons, your theme and all other settings have been restored to their original form.

Migrating Profiles With Windows Easy Transfer:

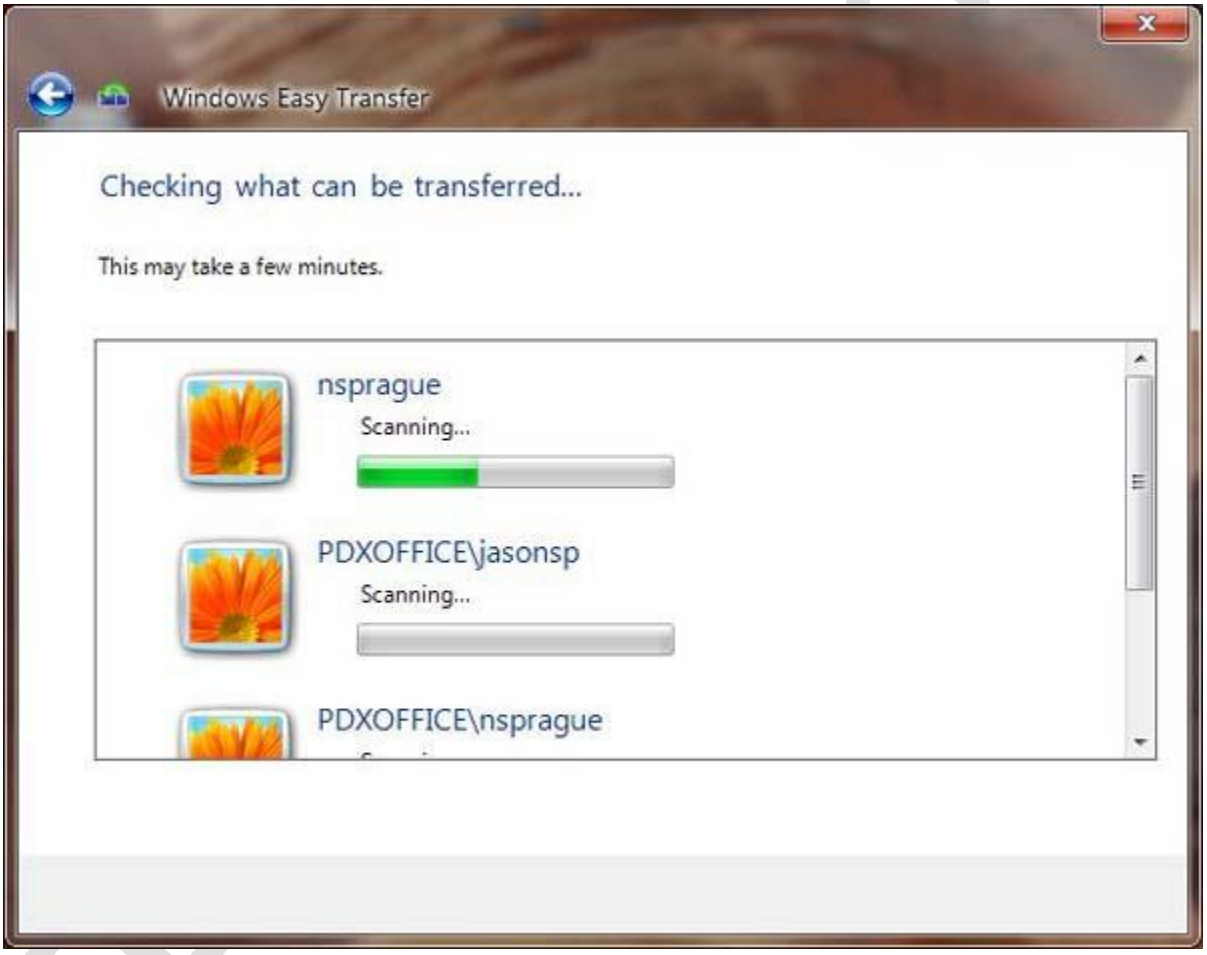
You can install Windows 7 as an upgrade to an existing installation of Windows Vista with Service Pack 1 or Service Pack 2 using the Upgrade option during installation. To maintain settings when installing Windows 7 on a computer running Windows XP, you must migrate files and settings using a tool such as Windows 7 Easy Transfer and then reinstall your software programs. Additionally, if you are installing Windows 7 on a new computer, you can transfer settings and files from any other computer running Windows Vista or Windows XP by using Windows Easy Transfer.

The instructions below show how to tranfer a profile from a computer running Windows XP to a different computer running Windows 7.

1. Boot in to Windows XP and insert the Windows 7 DVD.
2. Navigate to the support folder and open the migwiz (migration wizard) folder and run *migwiz.exe*. This opens the Windows Easy Transfer window which initiates the process of file transfer.
3. It asks you for the media you wish to use to transfer your settings. Select the appropriate media from the options presented by the wizard.



4. It ask whether this is the new computer (to which you wish to copy the settings) or the old computer (from which you wish to copy the settings) select *old computer*. The wizard will now start scanning system for your files.



5. Once scanning is complete, it will provide the list of files in your system for all users and allows you to select which ones you wish to copy. Select the required files from the list.
6. You are then asked to provide a password for the data file. Provide a password for data security. Then press *Save*.
7. Log on to the Windows 7 computer.
8. Click *Start*, then click *All Programs*, and then click *Accessories*.
9. Click *System Tools*, and then click on *Windows Easy Transfer*.
10. It opens the Windows Easy transfer window and asks you to select the media you wish to use (USB, Network or transfer cable). Select the appropriate media from the options presented in the window.
11. Then, it asks you to select whether it's your new or old computer. Select *new computer*.

12. It asks you to browse to the file which you created while copying data from old computer. 13.Click *Transfer* to transfer all files and settings. You can also determine which files should be migrated by selecting only the user profiles you want to transfer, or by clicking *Customize*.
13. Click *Close*.

70-680 Study Guide - Capture, Prepare, and Deploy a System Image

System Images:

A system image is a copy of the current state of your computer's hard disk. It includes all the system settings, files, and the Windows configuration. You can use a system image to recover your data and computer settings in the case of failure of your hard disk drive. All of your current programs, system settings, and files are replaced with the contents of the system image, but you cannot restore individual files or settings with this process.

A system image can also be used when deploying Windows 7 to multiple computers. Deployment Image Servicing and Management (DISM) in the Windows Automated Installation Kit (AIK) provides additional functionality for Windows 7 and Windows Server® 2008 R2–based operating system images. In Windows 7, you can use DISM to enumerate drivers, packages (including updates), and features in the image. You can also use DISM to add and remove flat file drivers from a Windows 7 or Windows Server 2008 R2 system image. DISM consolidates functions previously found across several tools.

Notably, you can also use DISM to manage Windows Preinstallation Environment (Windows PE) images; DISM can manage international configurations and can be used for mounting and unmounting WIM images. Previously, these functions were spread across the PEImg, IntlConfig, and ImageX tools. Finally, DISM contains changes that allow for backward compatibility with Package Manager (PKGMGR) commands that were used for Windows Vista and Windows Server 2008 image files to help ensure that existing tools and scripts written for previous versions of the Windows AIK continue to work. ImageX is still provided with the Windows AIK for system image creation and application functions.

Creating a System Image in Windows 7:

1. Click *Start* and type *back up* in the start search bar. Click *Back up your computer* from the search results.
2. In the left pane of the Backup and Restore Center window, click *Create a system image*.

3. Choose a medium to store the system image. You can back up the system image on an external drive, on DVDs, or on a computer on the network.
4. Select the drives you want to back up. Click *Next*.
5. On the Confirm your settings page, select *Start backup*.
6. After the process is complete, you get the option to create a system repair disc. Click *Yes* to create the system repair disk. Insert a blank CD or DVD to create the image.

You can now find the system image folder named WindowsImageBackup.

Recovering a Computer Using a System Image:

You can only do a system image recovery to a hard disk drive that is the same size or larger than the one the system image was created from. You will not be able to do a system image recovery to a smaller hard disk drive. If your backup image is on an external device, then connect the external drive before starting. A system image recovery will format everything on each hard drive that was included in the system image, and will only restore what is in the system image. To start the recovery of the system, perform these steps:

1. Connect the external drive on which you have stored the system image.
2. Click *Start*, then click *Control Panel*, and then click *Back up your computer*.
3. Click *Recover system settings on your computer*.
4. Click *Advanced recovery methods*.
5. Select *Use a system image you created earlier to recover your computer*.
6. If you want to create the backup immediately, select *Back up now*, or click *Skip and continue the system image recovery without backing up any of your current files*. click *Restart*.
7. Select a language to be used for your keyboard input and click *Next*.
8. Select the system image for recovery using either of the two options:
    1. To use a latest system image for recovery, select *Use the latest available system image* and click *Next*.
    2. To select a system image for recovery, select the location of the backup image for the computer you want to restore from the list, and click *Next*. Then select the date and time of the system image to restore, and click *Next*.
9. After selecting the system image, select the *Format and repartition disks* box.
10. If you want to recover only those drives that are required to run Windows, select the *check box Only restore system drives*. Click *Next*.
11. Click *Finish* and then click *Yes*.
12. Windows will now start restoring your computer from the system image. Once the restoration is complete, click *Restart Now*.
13. If you chose to create the backup immediately in step 6, you will see the option Restore my file after the computer restarts. Select this option to restore the files.

70-680 Study Guide - Configure a VHD

Virtual Hard Disks:

Windows 7 has a new feature called VHD Boot. This feature allows you to boot your entire Windows from a Virtual Hard Disk (VHD) file. There are various advantages of this feature, like:

- The configurations and settings of your entire system are included in one file – .VHD file.
- One VHD file can be based on another one. So if you have different systems, you can create a base copy of Windows 7 on a VHD and make all others incremental. This saves a lot of disk space.

But this feature can only be used on Windows 7, Windows Server 2008 R2, or later operating systems. The operating systems which came before Windows 7 do not support VHD. With VHD your system suffers a performance decrease of about 3%. Windows' hibernate function and BitLocker configurations are not supported by VHD. BitLocker can be used within the guest VHD, but not on the volume where the VHD resides. Also, with VHD, features like Aero don't work because the Windows Experience index is not supported.

Types of Virtual Hard Disks:

Three types of VHD files can be created using the disk management tools:

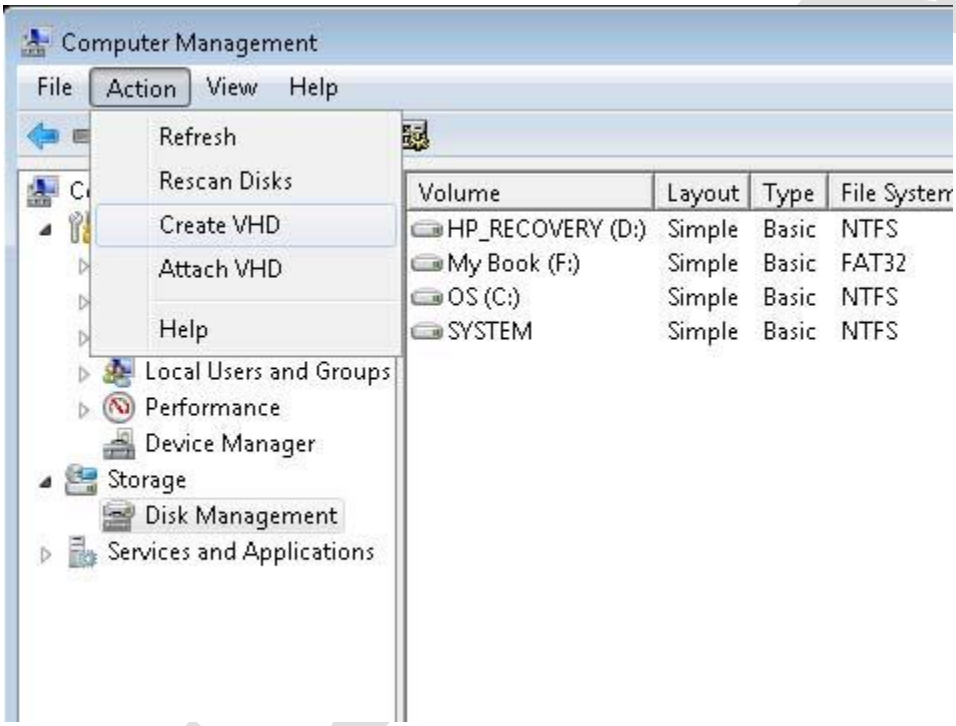
- **Fixed hard-disk image** - A fixed hard-disk image is a file that is allocated to the size of the virtual disk. For example, if you create a virtual hard disk that is 2 gigabytes (GB) in size, the system will create a host file approximately 2 GB in size. Fixed hard-disk images are used for production servers and working with customer data.
- **Dynamic hard-disk image** - A dynamic hard-disk image is a file that is as large as the actual data written to it. As more data is written, the file dynamically increases in size. For example, the size of a file backing a virtual 2 GB hard disk is initially around 2 megabytes (MB) on the host file system. As data is written to this image, it grows with a maximum size of 2 GB. Dynamic hard-disk images are beneficial for development and testing environments. Dynamic VHD files are smaller, easier to copy, and expand after mounting.
- **Differencing hard-disk image** - A differencing hard-disk image describes a modification of a parent image. This type of hard-disk image is not independent, and it depends on another hard-disk image to be fully functional. The parent hard-disk image can be any of the above mentioned hard-disk image types, including another differencing hard-disk image.

Creating a VHD:

Perform these steps to create a VHD file on your Windows 7-based computer:

1. Click *Start* and then right-click *Computer*.

2. Click *Manage*, then in the left pane, right-click *Disk Management*, and then click *Create VHD*.



3. Select a location to save your VHD file. Select the maximum size for your VHD file. You can also choose from either of the two options – Dynamically Expanding, where the size of the VHD expands dynamically to a fixed maximum size, or Fixed Size, where the virtual hard disk uses a fixed amount of space regardless of the size of data stored on it.

4. The new disk will show in the right pane as unallocated space. Right-click the new unallocated VHD Disk number and click *Initialize Disk*.
5. You need to choose if you want the new VHD to have Master Boot Record (MBR) or GUID Partition Table (GPT) partition, and click *OK*.
6. Right-click again on the new unallocated VHD and click *New Simple Volume*.
7. Type how much of the maximum disk space you want to use for this VHD partition, and click *Next*.
8. Select the file system for your VHD from either FAT or NTFS, and enter a name for your VHD. Select the *Perform a quick format* check box, and click *Next*.
9. Click *Finish*. The system creates a new simple volume on your VHD, which is already attached.

Installing a VHD-Boot Machine:

Perform these steps to install Windows 7 with VHD file:

1. Boot the system with a Windows 7 setup DVD or any other boot media.
2. On the setup screen, don't choose Install Now, but press *Shift-F10* to get into command line mode.

3. Type *diskpart* on the command line mode to start the partitioning utility.
4. You need to create a new VHD file. Type the following command to create this file:
   create vdisk file="D:\pathToVhd.vhd" type=expandable maximum=maxsizeInMegabyte
5. Select the new VHD and attach it as a physical disk. Use the following command to perform this task:
   select vdisk file="D:\pathToVhd.vhd" attach vdisk
6. Proceed with the normal setup and make sure that you install Windows on the correct disk. You may receive a warning Windows cannot install to this disk. Ignore this warning.
7. At next startup, you'll see Windows 7 in the boot menu. If you want to add a VHD manually to the boot menu, use this command:
   bcdedit /copy {originalguid} /d "New Windows 7 Installation"
   bcdedit /set {newguid} device vhd=[D:]\Image.vhd
   bcdedit /set {newguid} osdevice vhd=[D:]\Image.vhd
   bcdedit /set {newguid} detecthal on
8. Click *Start*, right-click *Computer*, and select *Manage*.
9. To attach an existing VHD File, in the left pane, right-click *Disk Management* and then click *Attach VHD*.
10. Click *Browse*, navigate to the VHD file location, select the file, and then click *Open*. If you want the VHD to be read-only, select the check box. Click *OK*.

70-680 Study Guide - Configure Devices

Device Manager:

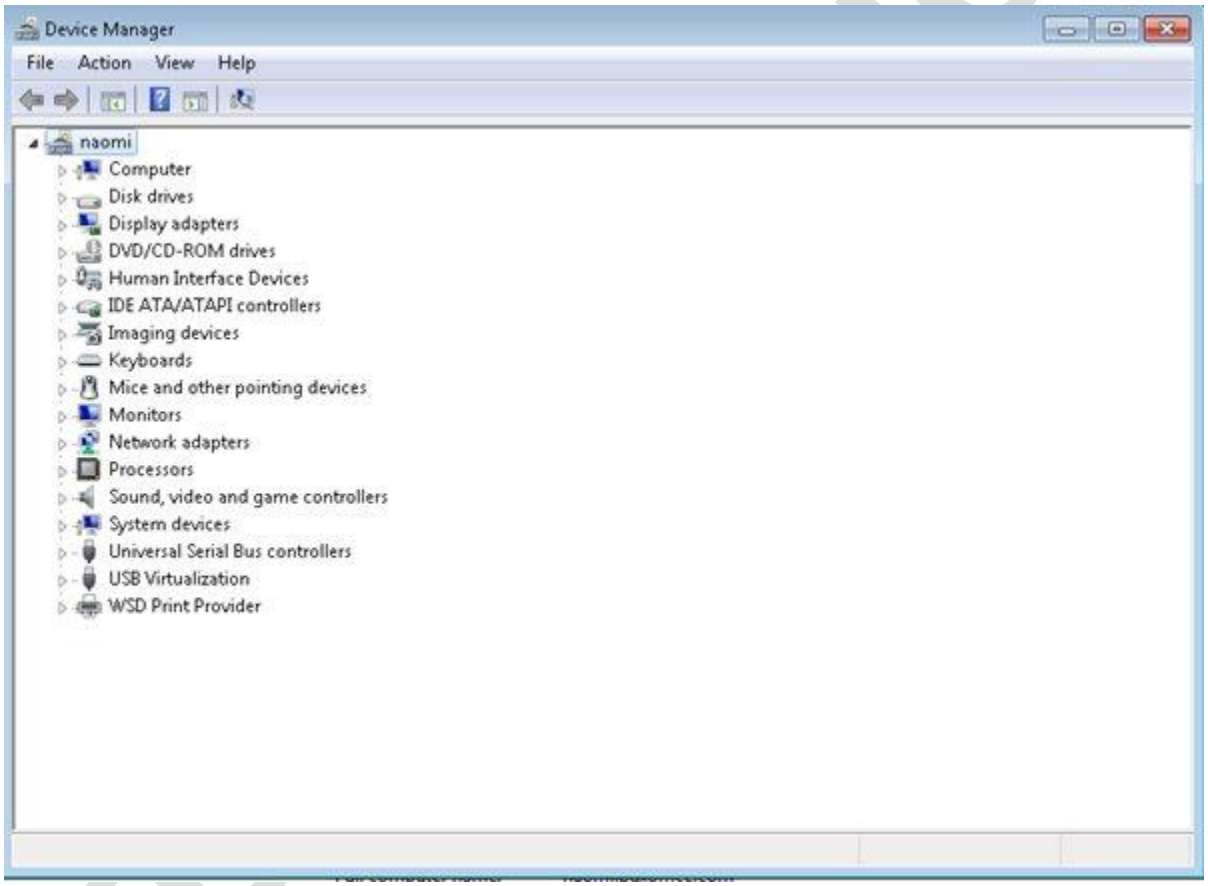
Device Manager provides you the facility to graphically view the hardware that is installed on your computer. The Device Manager shows you the devices that are integrated in and connected to your computer, and their drivers. You can use Device Manager to manage devices only on a local computer. Using Device Manager you can:

- Determine whether the hardware on your computer is working properly.
- Change hardware configuration settings.
- Identify the device drivers that are loaded for each device, and obtain information about each device driver.
- Change advanced settings and properties for devices. Install updated device drivers.
- Enable, disable, and uninstall devices.
- Roll back to the previous version of a driver.
- View the devices based on their type, by their connection to the computer, or by the resources they use.
- Show or hide hidden devices that are not critical to view but might be necessary for advanced troubleshooting.

Accessing Device Manager:

There are a few ways to open the device manager and you should be familiar with them. For the purposes of this guide, we are going to open it as follows:

1. Click *Start*.
2. Right click on *Computer* and select *Properties*.
3. In the left menu, click on *Device Manager*



If you see a yellow exclamation point next to a device, it means that there is a conflict or problem with the driver as shown below:

Right clicking on the device will allow you to update, disable, or uninstall a problem driver.

Read Device Manager for more information.

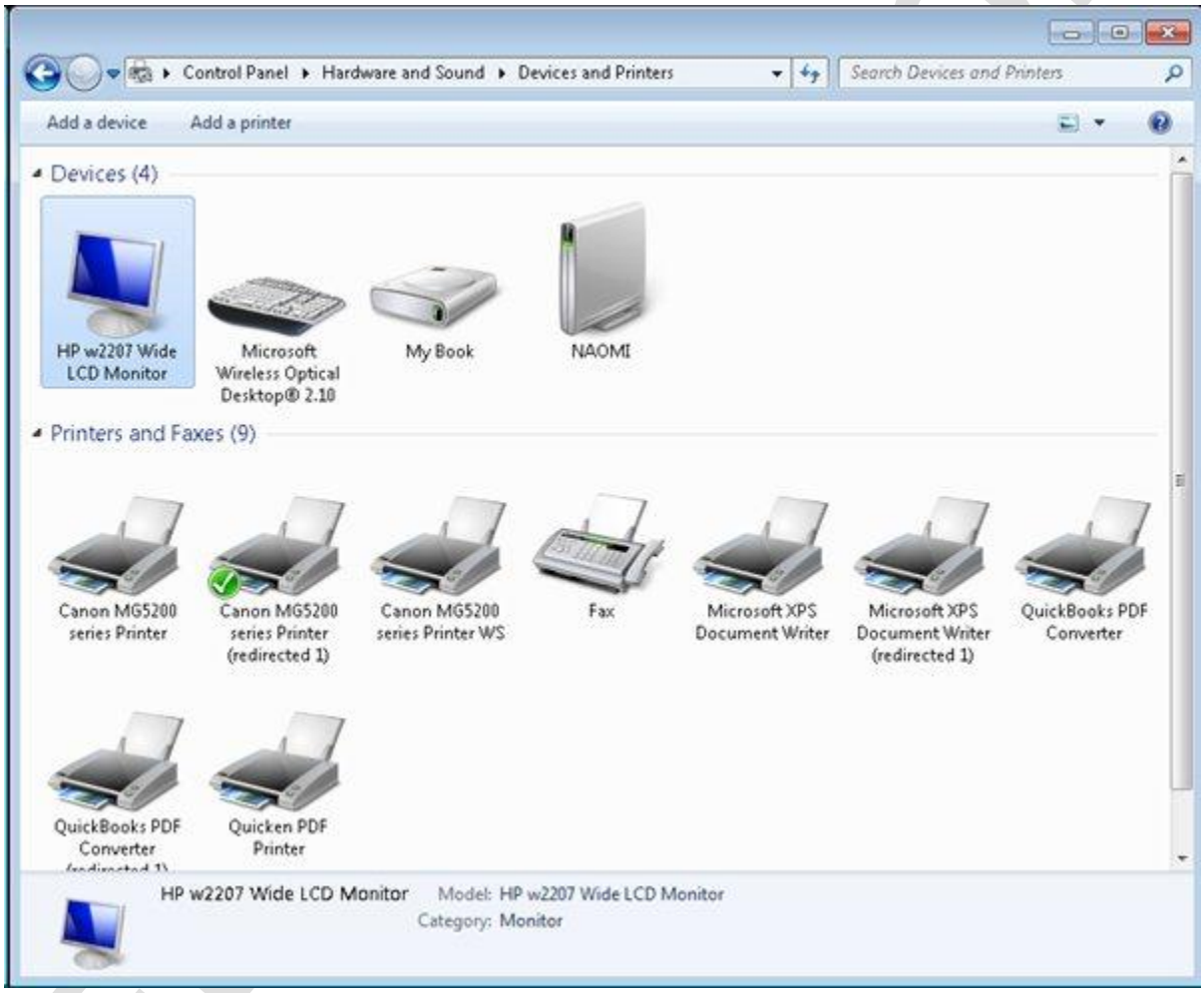
Signed Drivers:

A signed driver is a device driver that includes a digital signature. A digital signature is an electronic security mark that can indicate the publisher of the software, as well as whether someone has changed the original contents of the driver package. If a driver has been signed by a publisher that has verified its identity with a certification authority, you can be confident that the driver actually comes from that publisher and hasn't been altered.

Steps for Staging a Device Driver Package in the Driver Store

Devices and Printers Control Panel:

Another place for device management is in the Devices and Printers Control Panel. Here you can add a device or printer, view and modify drivers, eject devices, and other tasks.



The top menu changes depending on which device is selected.

70-680 Study Guide - Configure Application Compatibility

Program Compatibility Mode:

Program compatibility is a mode in Windows that lets you run programs written for earlier versions of Windows. Most programs written for Windows Vista also work in Windows 7, but some older programs might run poorly or not run at all.

If an older program doesn't run or install correctly, the first, and easiest, thing to try is the Program Compatibility troubleshooter. It can automatically detect and fix common problems that prevent older programs from installing or running correctly.

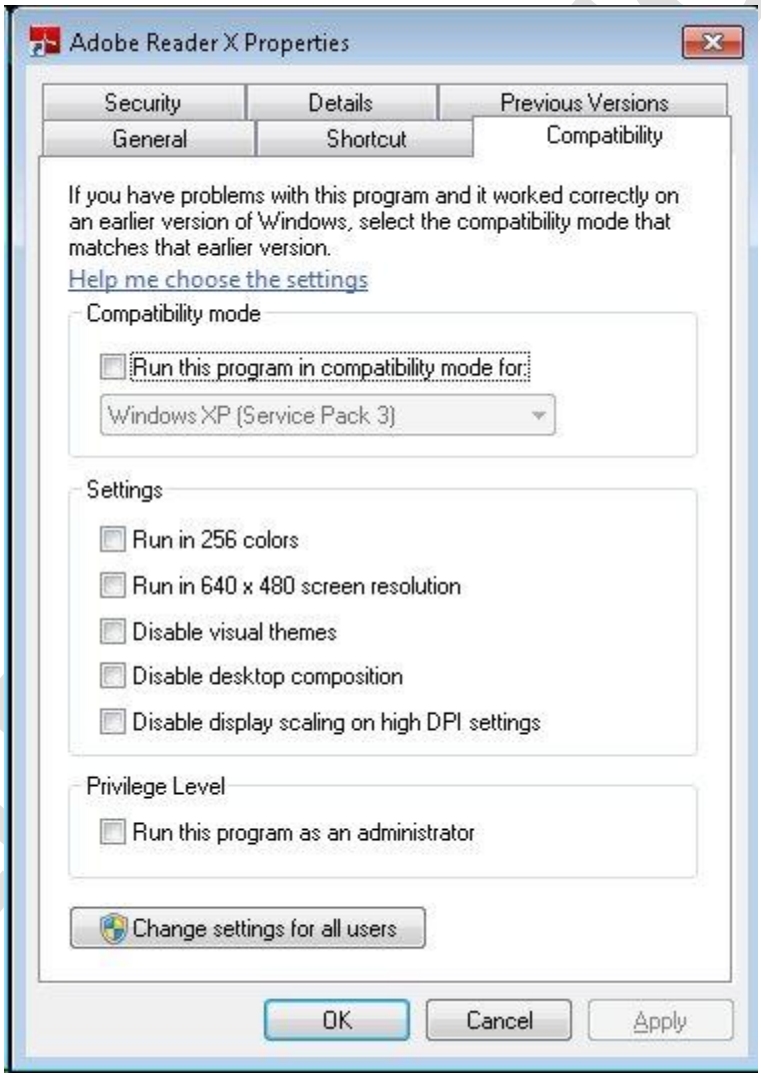
Open the Program Compatibility troubleshooter by doing the following:

1. Click the *Start* button, then *Control Panel*.
2. In the search box, type *troubleshooter*, and then click *Troubleshooting*.
3. Under Programs, click *Run programs made for previous versions of Windows*. As an alternative to these first 3 steps, you can right click on the program's icon or shortcut and select *Troubleshoot Compatibility*.
4. If you click on *Advanced*, you can opt to run as administrator which may find more issues, and you can choose to have Windows automatically fix problems.
5. Click *Next* and Windows searches for issues.
6. You will be presented with a list of applications. Choose the one you are having problems with and click *Next*
7. You can now choose to try running the program using Microsoft's changes and see if the problem is solved. If the problem is solved, you can elect to apply the changed. If it does not solve your problem, you may choose *troubleshoot program* which will begin a troubleshooting wizard.

Don't use the Program Compatibility troubleshooter on older antivirus programs, disk utilities, or other system programs, because using outdated programs of this type might cause data loss or create a security risk.

Instead of using the wizard above, you can manually set the compatibility mode as follows:

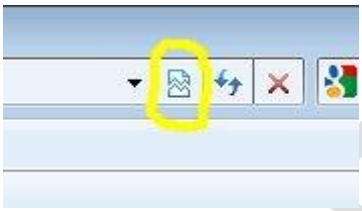
1. Right click on the program's icon or setup file (typically setup.exe) and select *Properties*.
2. In the window that appears, click the *Compatibility* tab as shown below.



3. If you want to run the application in a particular operating system mode, click the *Run this program in compatibility mode for:* checkbox and then select the operating system from the drop-down menu below.
4. On this screen, you can also troubleshoot issues by trying 1 or more of the checkboxes that affect display properties.

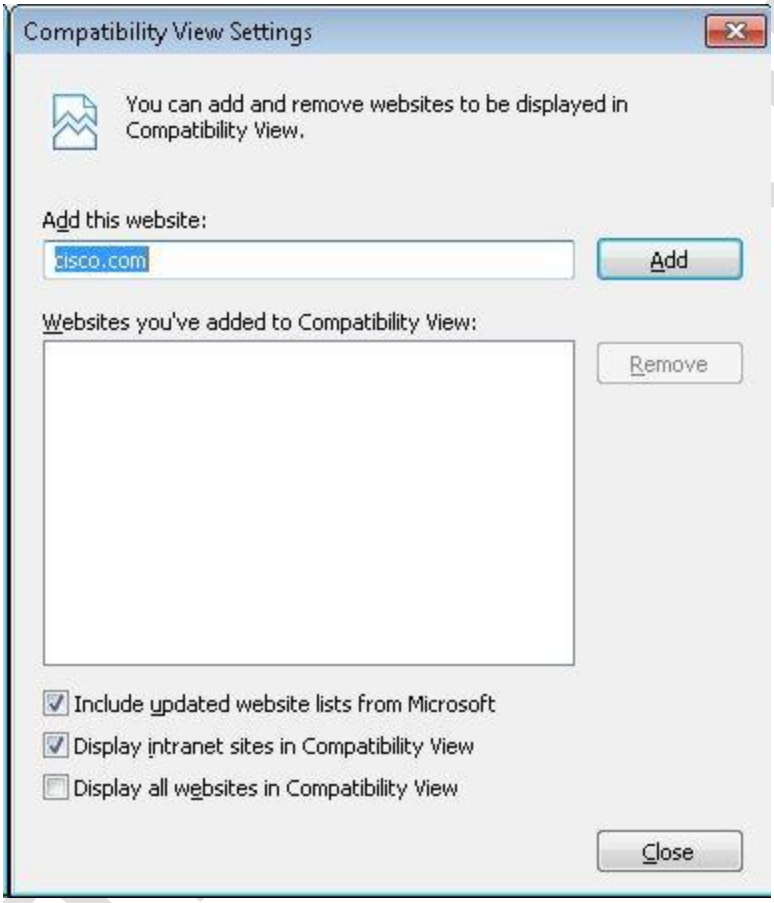
Internet Explorer Compatibility:

Typically when Microsoft releases a new version of IE, some web pages no longer display properly. If Internet Explorer recognizes a webpage that is not compatible, the *Compatibility View* icon will appear on the Address bar as shown below.



Clicking on this button will switch IE to compatibility view for this page. Clicking the button again, will turn it off. The same goal can be accomplished by clicking on *Compatibility View* from the tools menu. If the option is grayed out, it means that IE has not detected any compatibility issues with the web page.

There are a few IE compatibility settings that can be modified by clicking on the *Tools* menu and selecting *Compatibility View Settings*.



Shims:

As the Windows operating system evolves from version to version—changing to support new technology, incorporate bug fixes, and implement a modification in strategy—changes to the implementation of some functions may affect applications that depend on them. Because of the nature of software, modifying the function again to resolve this compatibility issue could break additional applications or require Windows to remain the same regardless of the improvement that the alternative implementation could offer. We can circumvent this possibility by placing branches directly in the source code for Windows, but doing so presents a long-term challenge for the serviceability and reliability of the Windows operating system. Using the Shim Infrastructure, however, you can target a specific application fix but only for a particular application (and typically, for particular versions of that application), with these fixes housed outside the core Windows functions and maintained separately.

Deploying a custom shim database to users requires the following two actions:

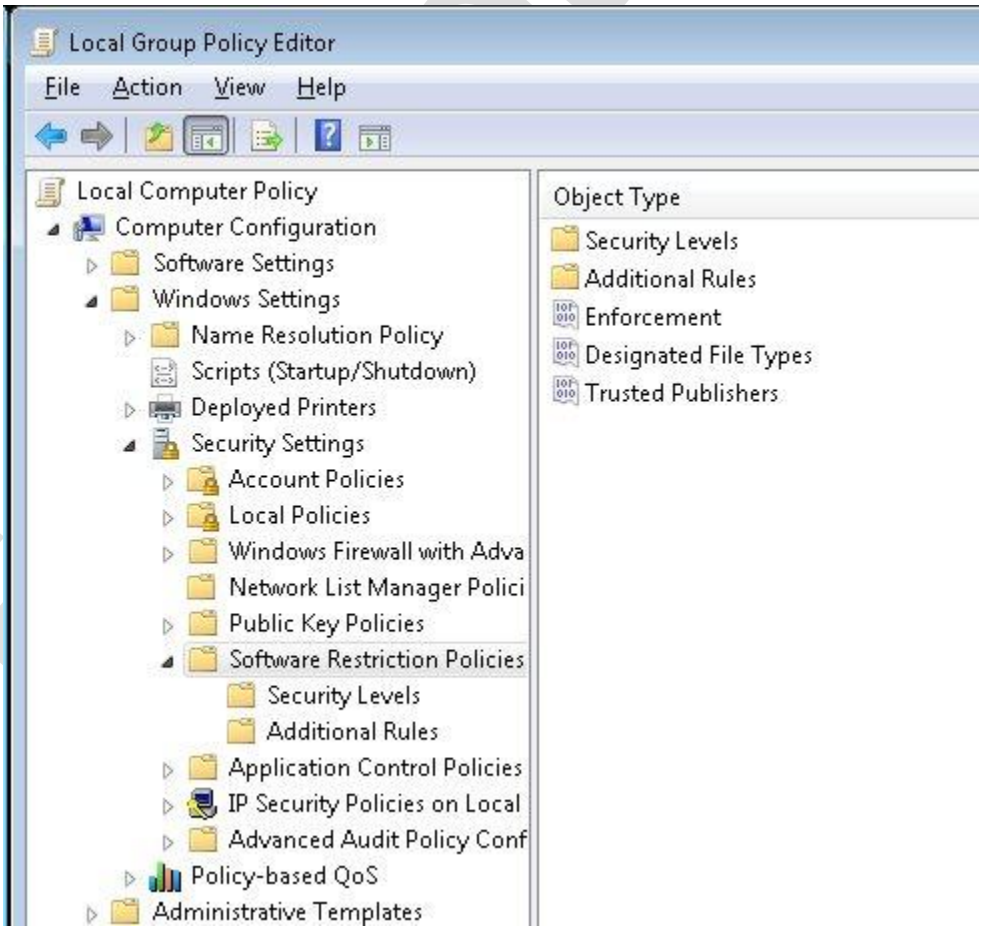
- Placing the custom shim database (*.sdb file) in a location to which the user's computer has access (either locally or on the network).
- Calling the sdbinst.exe command-line utility to install the custom shim database locally.

70-680 Study Guide - Configure Application Restrictions

Software Restriction Policies:

Software restriction policies can help organizations protect themselves because they provide another layer of defense against viruses, Trojan horses, and other types of malicious software. You can configure the Software Restriction Policies settings in the following location within the Group Policy Management Console:

Computer Configuration\Windows Settings\Security Settings\Software Restriction Policies



Software restriction policies do not prevent restricted processes that run under the System account. For example, if a malicious program has set up a malicious service that starts under the Local System account, it starts successfully even if there is a software restriction policy configured to restrict it. A flawed software restriction policy implementation can disable necessary applications or allow malicious software to run.

A policy consists of a default rule that specifies whether programs are allowed to run and exceptions to that rule. The default rule can be set to *Unrestricted* (the program is allowed to run) or *Disallowed* (the program is not allowed to run). Setting the default rule to *Unrestricted* allows an administrator to define exceptions (programs that are not allowed to run). A more secure approach is to set the default rule to *Disallowed*, and specify only the programs that are known and trusted to run.

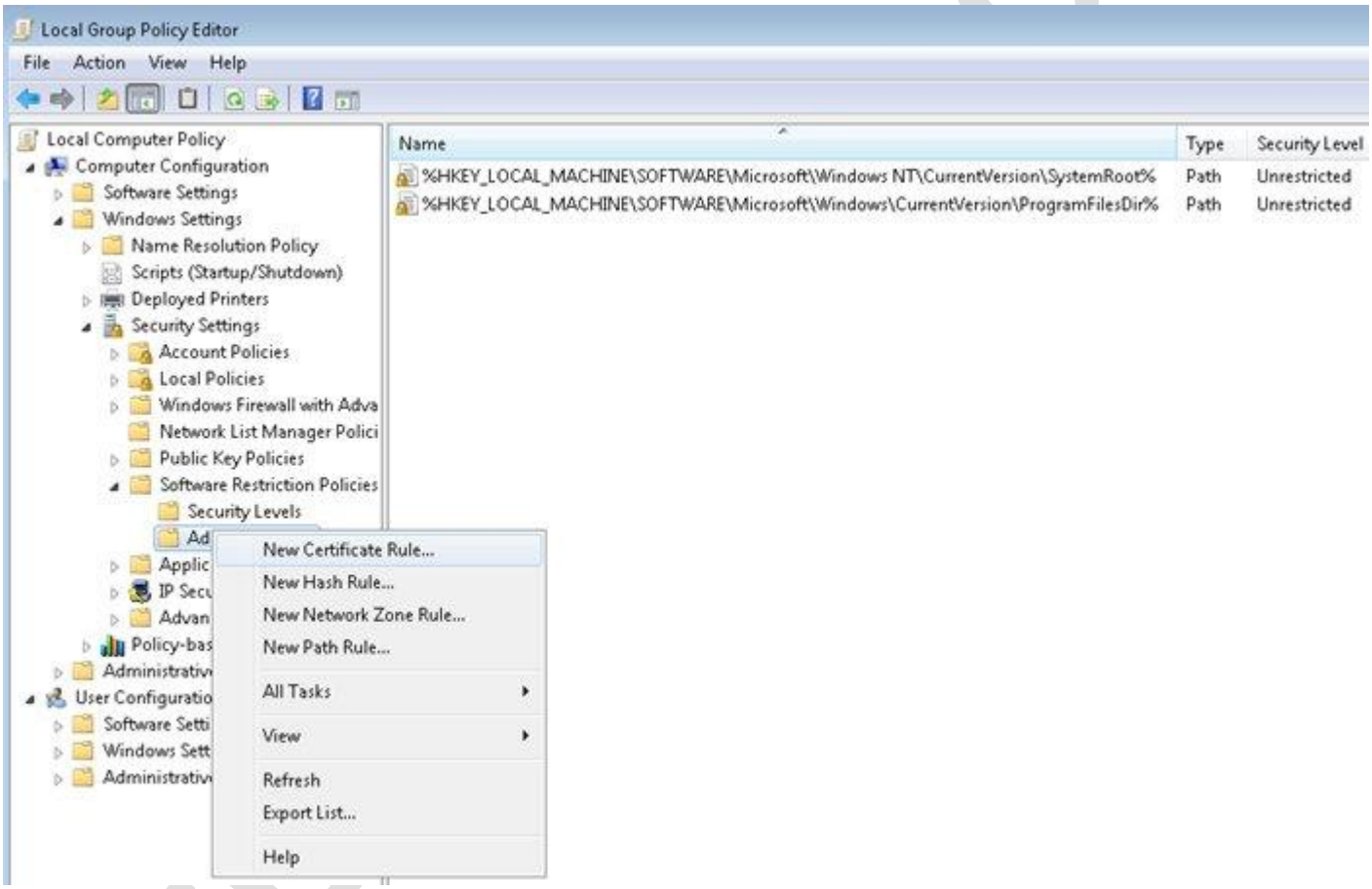
There are two ways to use software restriction policies:

- If an administrator knows all of the programs that should run, then a software restriction policy can be applied to allow only this list of trusted applications.
- If all the applications that users might run are not known, then administrators can disallow undesired applications or file types as needed.

Software Restriction Policies has four rules with which to identify software. The purpose of a rule is to identify one or more software applications, and specify whether or not they are allowed to run. Creating rules largely consists of identifying software that is an exception to the default rule. Each rule can include descriptive text to help communicate why the rule was created.

A software restriction policy supports the following four ways to identify software:

- Hash: A cryptographic fingerprint of the file.
- Certificate: A software publisher certificate that is used to digitally sign a file.
- Path: The local or universal naming convention (UNC) path of where the file is stored.
- Zone: The Internet zone as specified through Internet Explorer.



Applocker:

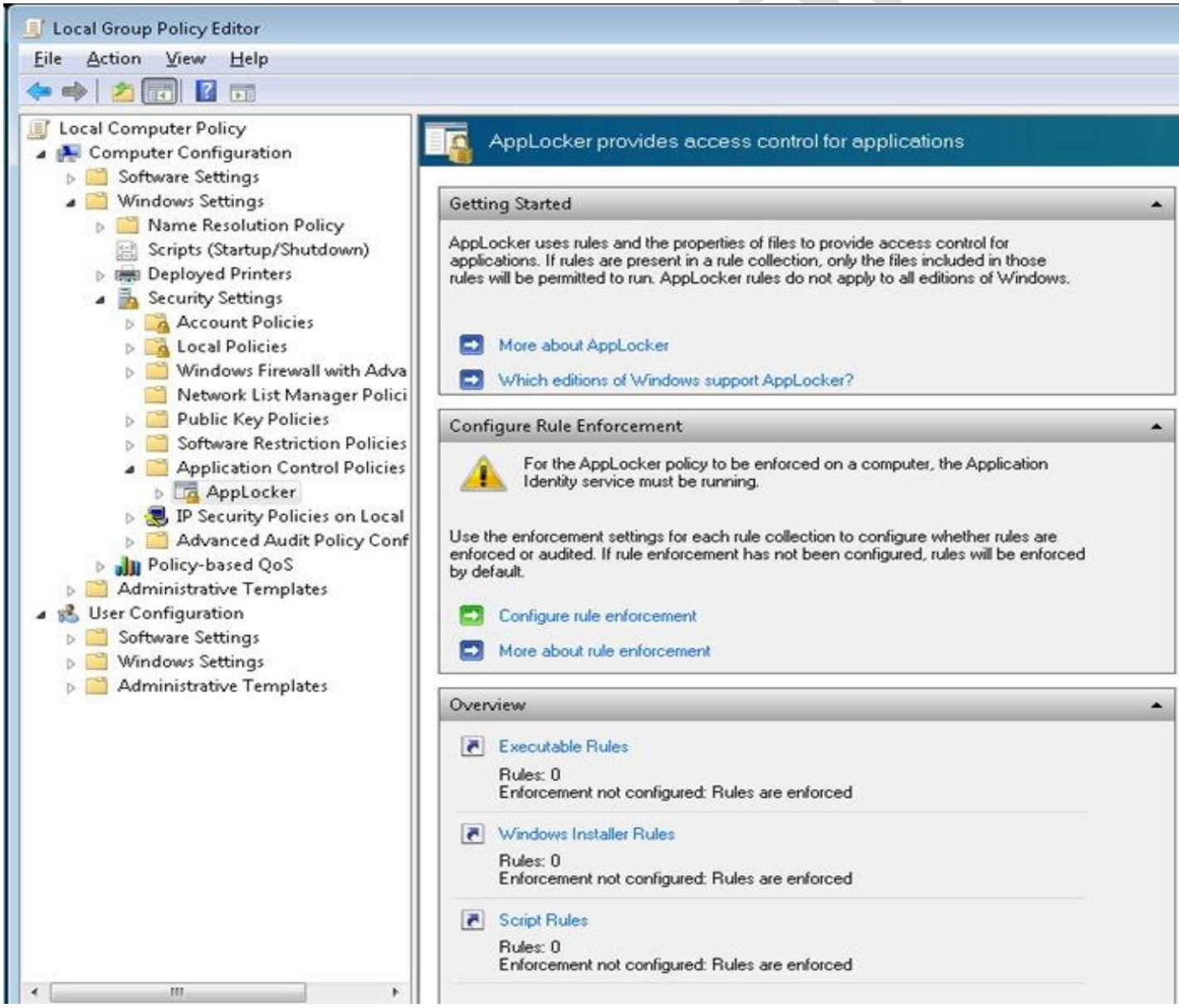
You can configure application restrictions in Windows 7 by using a tool called Applocker. With it you can configure Application Control Policies, which allow you to block the execution of a program by file name or hash calculation. Applocker helps you to allow the applications you want, and block the rest. But AppLocker is present only in the Enterprise and Ultimate editions of Windows 7. Applocker provides the following functionalities:

- Prevent unlicensed software from running in the desktop environment if the software is not on the allowed list
- Prevent vulnerable, unauthorized applications from running in the desktop environment, including malware

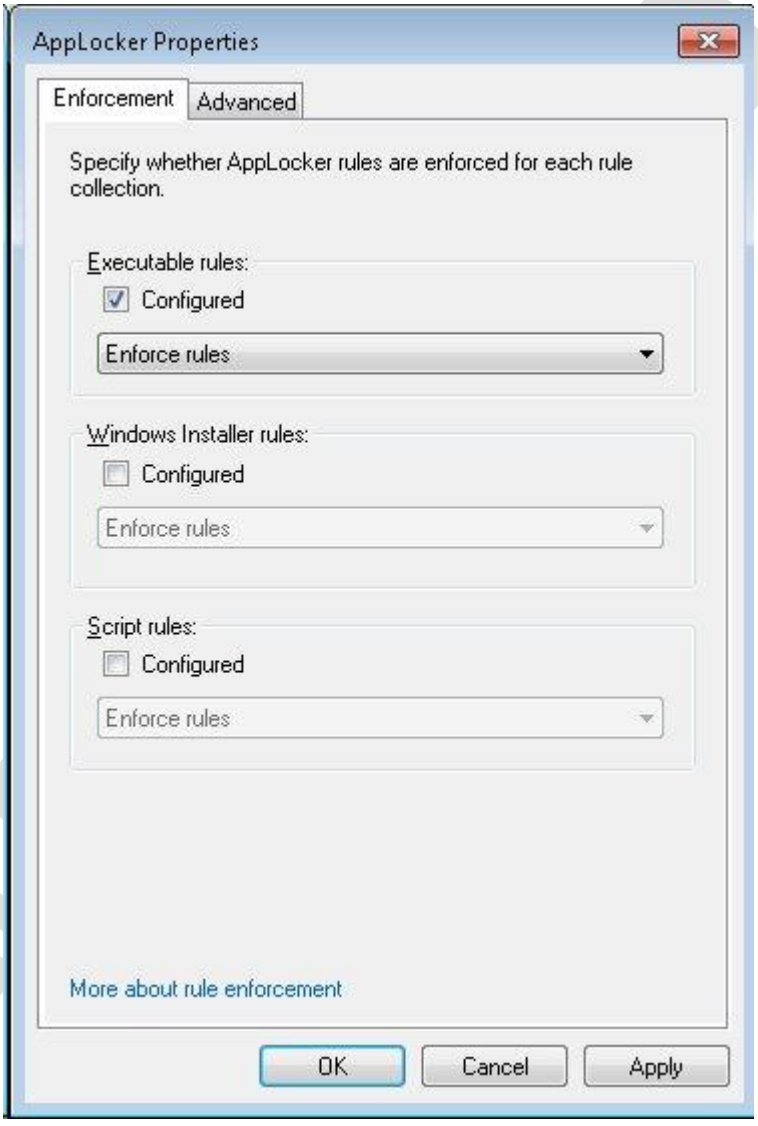
- Stop users from running applications that needlessly consume network bandwidth or otherwise affect the enterprise computing environment
- Prevent users from running applications that destabilize their desktop environment and increase help desk support costs
- Provide more options for effective desktop configuration management
- Allow users to run approved applications and software updates based upon policies while preserving the requirement that only users with administrative credentials can install or run applications and software updates
- Help to ensure that the desktop environment is in compliance with corporate policies and industry regulations
- AppLocker introduces publisher rules that are based upon application digital signatures. Publisher rules make it possible to build rules that survive application updates by being able to specify attributes such as the version of an application.

To access Applocker and block applications with it, follow these steps:

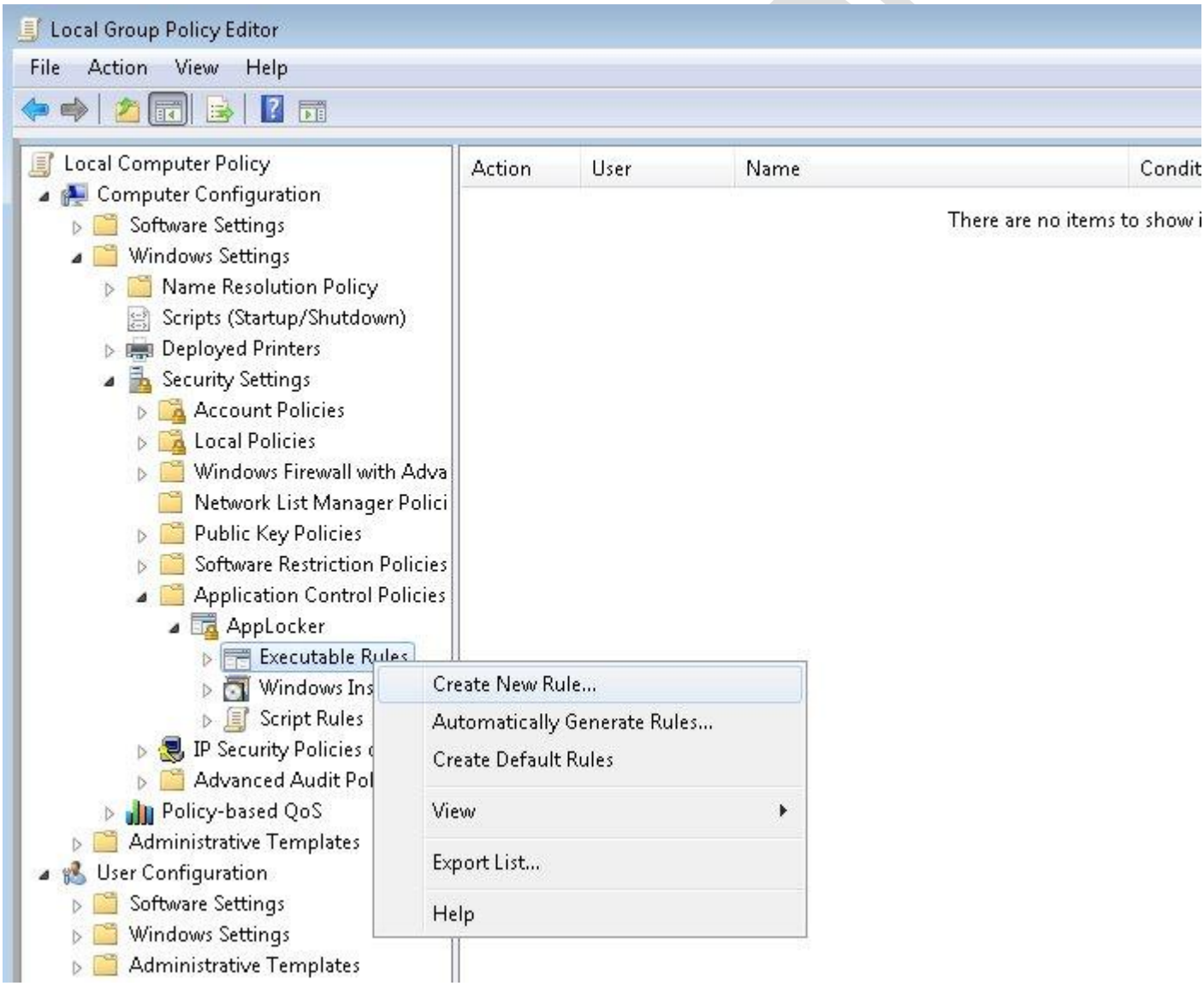
1. Click *Start* and type *gpedit.msc* into the search box.
2. In Local Computer Policy go to *Computer Configuration* \ *Windows Settings* \ *Security Settings* \ *Application Control Policies* \ *AppLocker*. Here you can see overall controls for the applications.



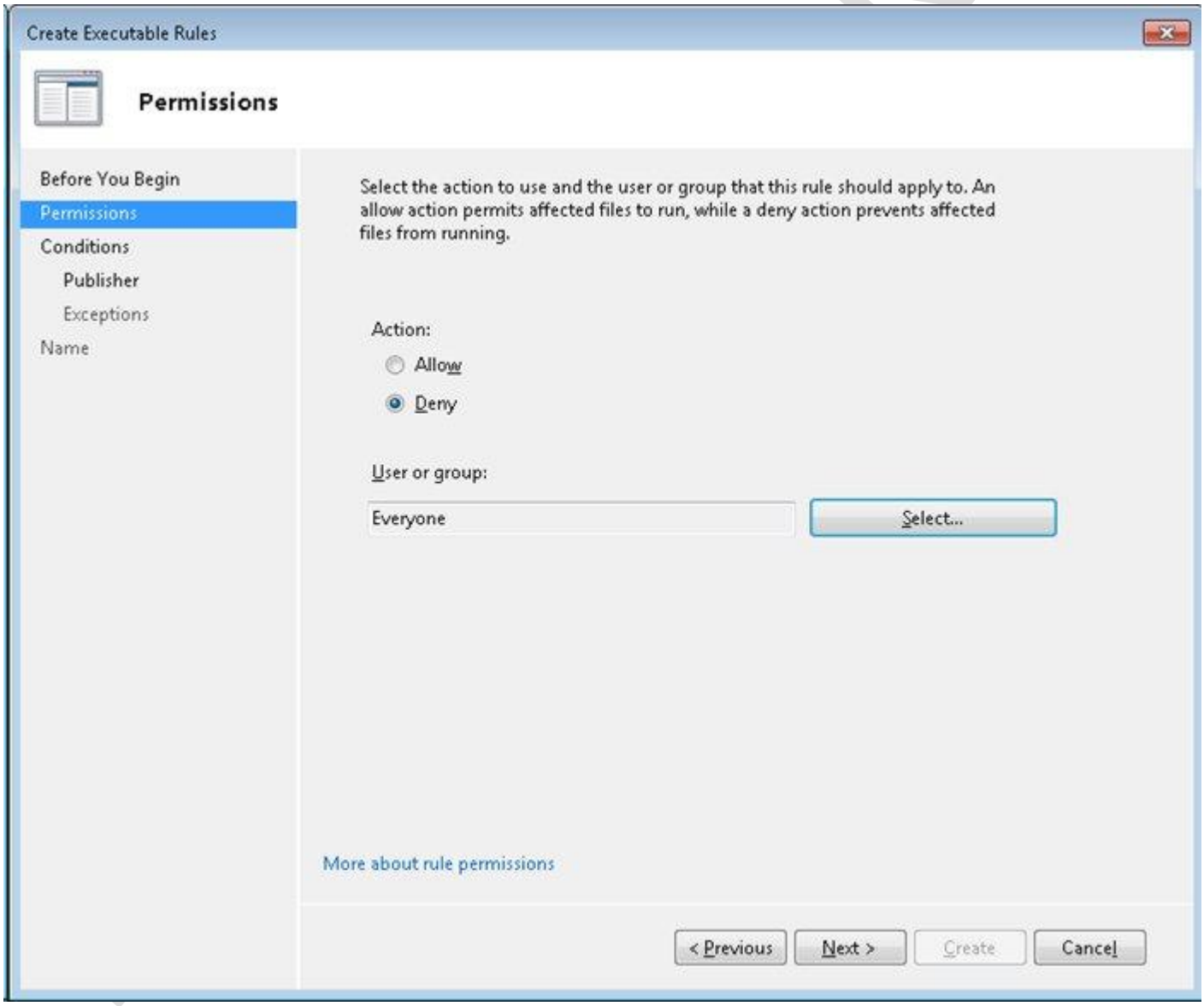
3. In the *Configure Rule Enforcement* window, click the *Configure rule enforcement* link.
4. In Applocker properties Window, click the checkbox for *Executable Rules*, *Windows Installer Rules*, or *Script Rules* depending on which type of application you are trying to control (in this example, we selected *Executable Rules*). Click *OK*.



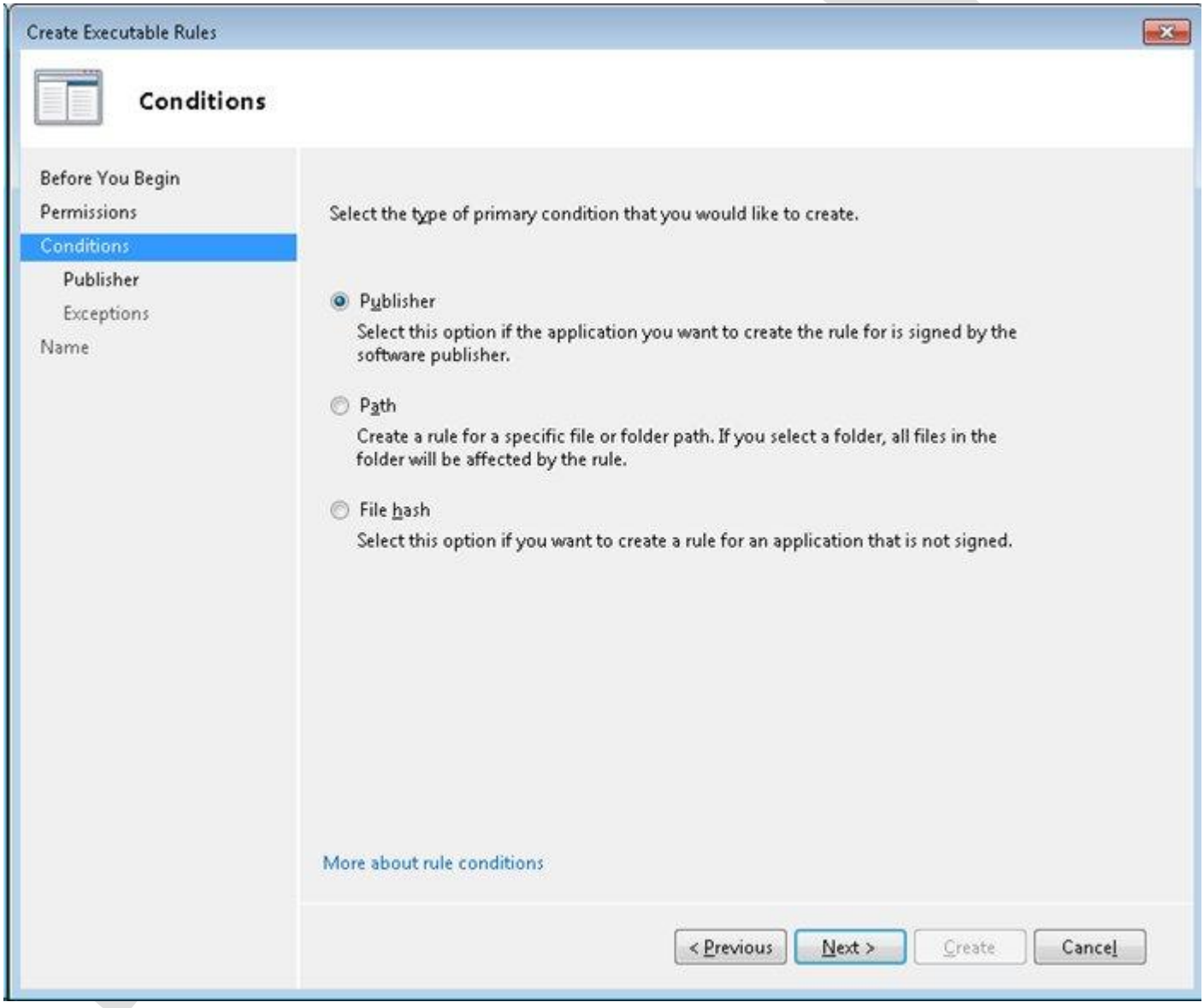
5. In the Overview window, click the *Executable Rules*.
6. Right-click and select *Create New Rule*. This opens up the Create Executable Rules wizard and you can select not to show the introduction screen at start up for the next time you access it by clicking the checkbox skip this page by default.



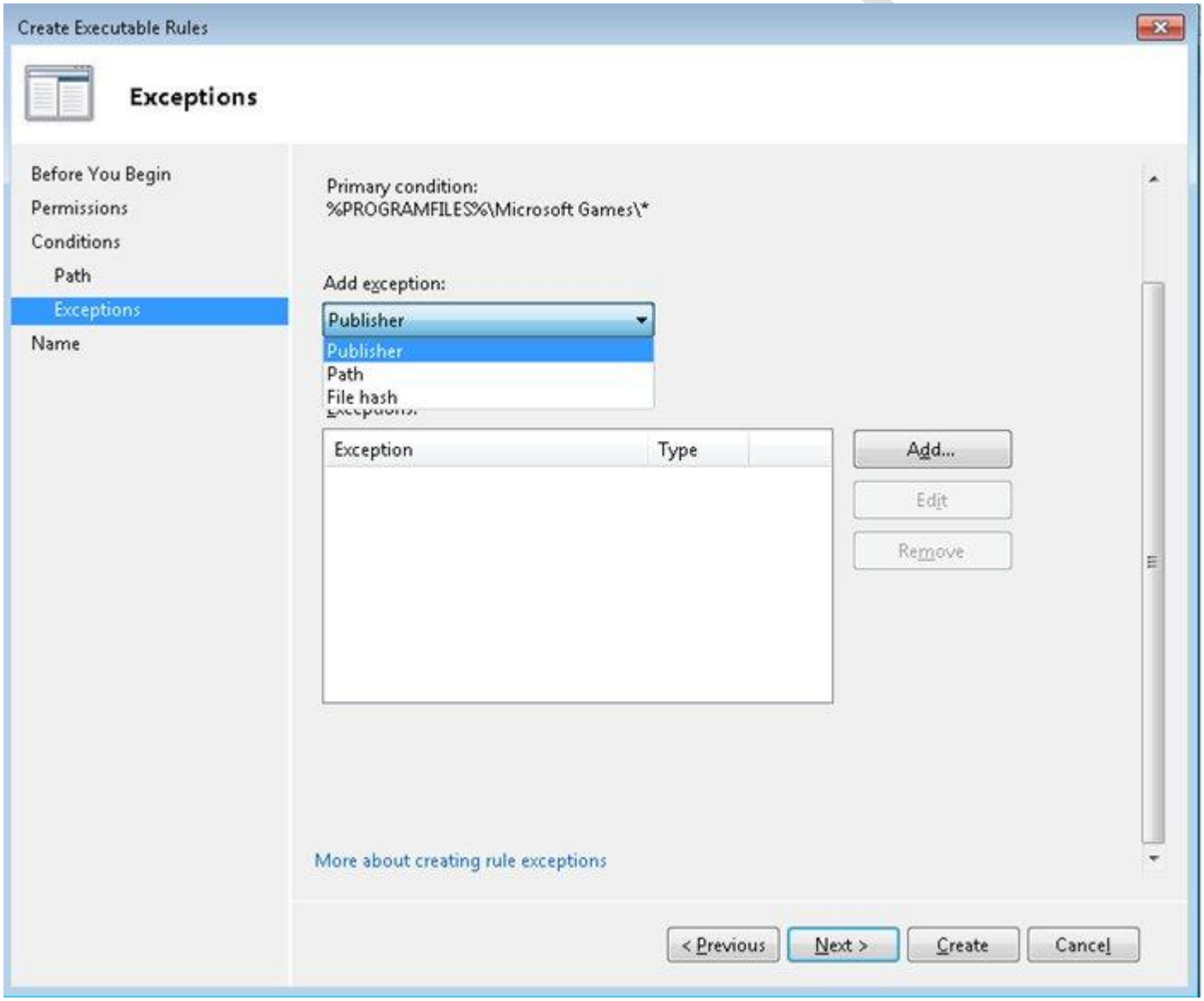
7. Select *Permissions* under *Action*, select *Deny*. Add the user name for whom you want to block the application.



8. In Conditions you can select from *Publisher*, *Path* or *File hash*, whichever you want to block. For example, if you want to block games, for example, select *Path*. Click *Next*.



9. Click *Browse Folders* and select the *Microsoft Games* folder. If you wanted to block a specific game(s) only, you would click on *Browse Files* and select the games in you wanted blocked.
10. On the next screen you can add Exceptions like allowing certain applications.



11. Add a description to the rule, and click *Create* and then click *Yes*.
12. After creating the rule, start Application Identification and set it to automatically, otherwise the rules won't work. By default this service is not started so you need to enable it.

Both SRP and AppLocker use Group Policy for domain management. However, when both SRP policies and AppLocker policies exist in the same Group Policy object (GPO), AppLocker policies will take precedence over SRP policies.

70-680 Study Guide - Configure Internet Explorer

About Internet Explorer:

Microsoft Internet Explorer (IE) is the most common browser available because it comes with every version of Windows. Windows 7 includes Internet Explorer 8.0, which has new functionality while reducing online risks. Some of the new features of IE 8 include:

- Tabbed browsing that enables you to open multiple webpages in a single browser window.
- The Instant Search box allows you search the Web from the Address bar.
- You can delete your temporary files, cookies, webpage history, saved passwords, and form information from one place.
- Printing now scales webpages to fit the paper you're using.
- The Zoom feature lets you enlarge or reduce text and images.
- InPrivate, helps protect privacy by preventing one's browsing history, temporary Internet files, from data, cookies, usernames, and passwords from being retained by the browser.
- The SmartScreen Filter offers protection from phishing sites.
- When a site or browser add-on causes a tab to crash, only that tab is affected. In many cases, IE can recover the tab..

Configuring Browsing History:

1. Click on *Tools* on the explorer tool bar in the upper right of the page.
2. Click *Internet Options* in the drop-down menu. This opens the Internet Options dialog window.
3. Click on the *General* tab.
4. Go to the *Browsing History* section.
5. Click the *Settings* button. This opens the Temporary Internet Files window.
6. Here you can modify settings such as when IE checks for new versions of cached pages, the location of the temporary internet files, the size of the temporary internet files folder, and the number of days that IE should keep visited pages in history.
7. Click *OK* after making the appropriate selections.

Security Zones:

Internet Explorer assigns all websites to one of four security zones: Internet, Local intranet, Trusted sites, or

Restricted sites. The zone to which a website is assigned specifies the security settings that are used for that site.

The following table describes the four Internet Explorer security zones.

Zone	Description
Internet	The level of security set for the Internet zone is applied to all websites by default. The security level for this zone is set to Medium High (but you can change it to either Medium or High). The only websites for which this security setting is not used are those in the Local intranet zone or sites that you specifically entered into the Trusted or Restricted site zones.
Local intranet	The level of security set for the Local intranet zone is applied to websites and content that is stored on a corporate or business network. The security level for the Local intranet zone is set to Medium (but you can change it to any level).
Trusted sites	The level of security set for Trusted sites is applied to sites that you have specifically indicated to be ones that you trust not to damage your computer or information. The security level for Trusted sites is set to Medium (but you can change it to any level).
Restricted sites	The level of security set for Restricted sites is applied to sites that might potentially damage your computer or your information. Adding sites to the Restricted zone does not block them, but it prevents them from using scripting or any active content. The security level for Restricted sites is set to High and can't be changed.

Configuring Internet and Local Internet Security Settings:

1. Select the *Security* tab at the top of the Internet Options dialog window.
2. Change the security level from IE's default setting of *Medium-High*, by adjusting the slide bar upward or downward to your desired setting.
3. Click on the *Custom Level* button if you would like to make the adjustment manually.
4. Click *OK* when finished.

Adding Trusted Sites:

1. Click the *Trusted Sites* icon from the security tab.
2. Click on the *Sites* button.
3. Enter the links to any sites that you know for sure are not a threat.
4. Click the *Add* to enter each link.
5. Click *Close*.

Adding Restricted Sites:

1. Click the *Restricted Sites* icon from the *security* tab.
2. Click the *Sites* button.
3. Enter the links to any sites that you know for sure will damage your computer.
4. Click *Add* to enter each link.

5. Click *Close*.
6. Click *Apply*.

Managing Cookies:

Websites use cookies to offer a personalized experience to users and to gather information about website use. Many websites also use cookies to store information that provides a consistent experience between sections of the site, such as a shopping cart or customized pages. With a trusted website, cookies can enrich your experience by allowing the site to learn your preferences or allowing you to skip having to sign in every time you go to the website. Disabling cookies can greatly reduce the ease of use on many sites, however, some cookies, such as those saved by banner ads, might put your privacy at risk by tracking sites you visit.

Internet Explorer provides many different ways to control the cookies that are stored on your computer. You can block or allow cookies or you can choose the specific sites that you'll accept cookies from. When you make these sorts of changes, the cookies that are already stored on your computer will not be affected. For that reason, you might want to delete the cookies already stored on your computer.

IE provides the ability to completely turn off cookies, although this is not recommended in most cases. Another approach is to manually configure which sites you will accept cookies from. This can be done as follows:

1. Select the *Privacy* tab at the top of the Internet Options dialog window
2. Click the *Sites* button. This opens the Per Site Privacy Actions window.
3. Enter the links to sites that you want to allow or block from using cookies on your Computer.
4. Click the *Block* or *Allow* button as desired to add each link.
5. Click *OK*.

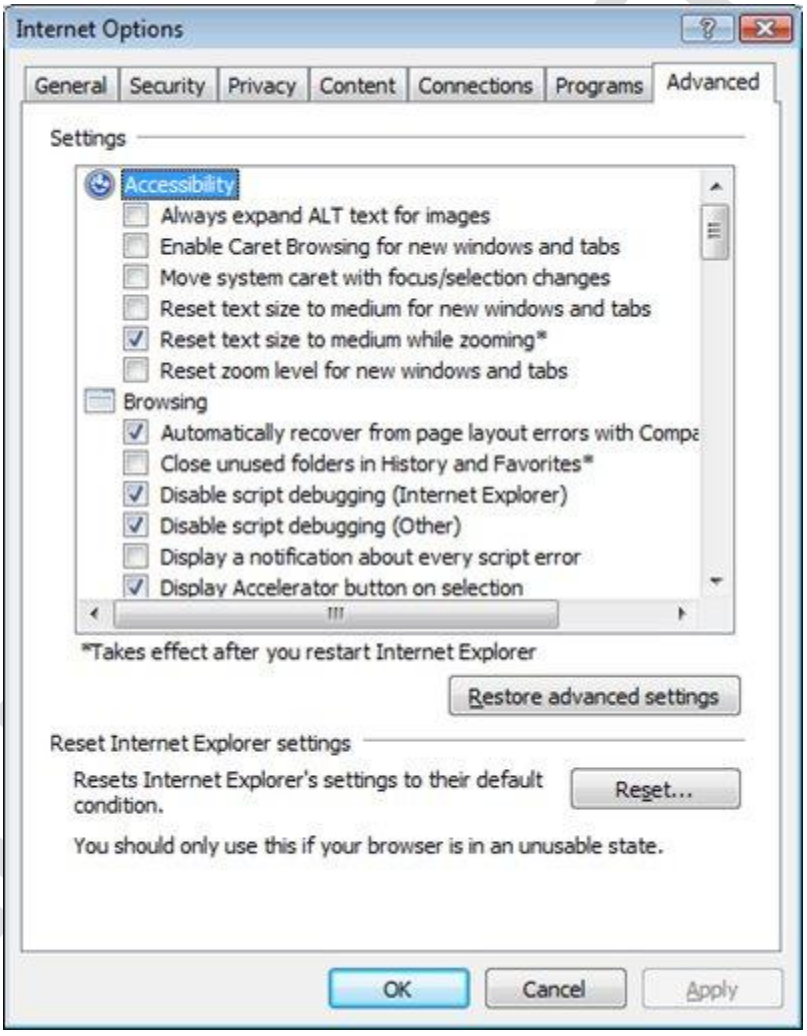
Configuring Internet Explorer to use a Proxy:

1. Select *Tools*, then select the Internet Options dialog window.
2. In the Internet Options window, click on the *Connections* tab.
3. Click *LAN Settings* and enable the checkbox for *Use a proxy server for your LAN*.
4. In the Address field, type in *127.0.0.1* and in the Port field type in *8081*.
5. Enble the check-box for *Bypass proxy server for local addresses*.
6. Click *Advanced*. In the Do not use proxy server for addresses beginning with: field, type the addresses which you want to to view some sites directly and not through the proxy.

Advanced Settings:

The advanced tab of the Internet Options dialogue box has several important security features including:

- Checking for server and publisher certificate validity, or certificate address mismatches. (Default is checked)
- Checking for signatures on downloaded programs. (Default is checked)
- Emptying the temporary internet files folder when IE is closed. (Default is unchecked)
- Enabling the SmartScreen Filter which detects phishing sites. (Default is checked)



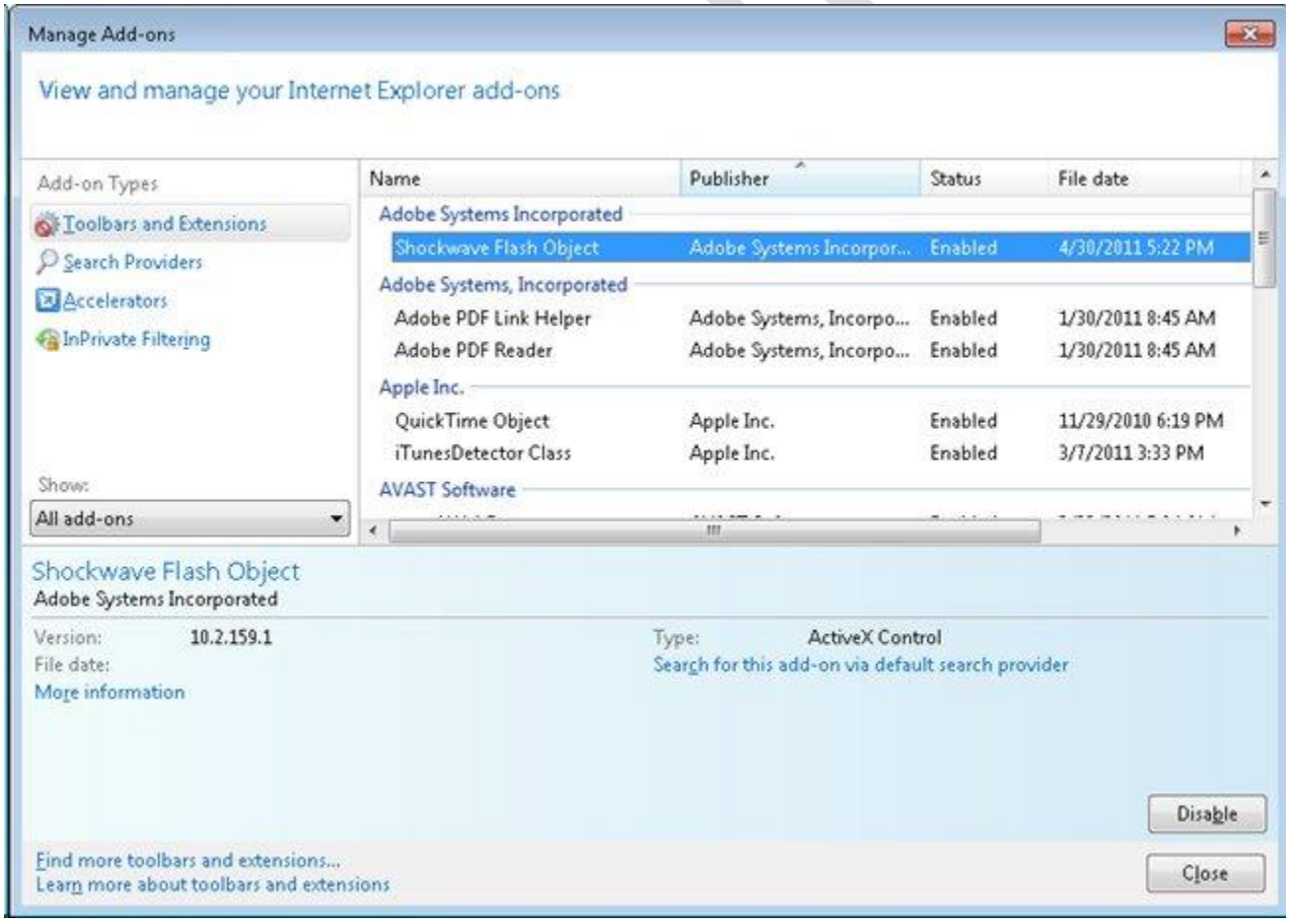
Managing Add-Ons:

Add-Ons, also known as browser plug-ins, are software programs that add functionality to IE. There are four basic add-on types supported by IE:

- Search providers
- Toolbars and extensions
- Accelerators
- InPrivate filtering

While add-ons can extend the functionality of your browser, they are often responsible for conflicts, crashes, and security breaches. Fortunately, IE allows you to manage add-ons in a way that can help you troubleshoot which object is causing the problem and then take necessary actions. To manage add-ons, follow these steps:

1. Click the *Tools* button and then click *Manage Add-ons*.



2. In the *Show* drop-down menu, select one of the following options:
   - To display a complete list of the add-ons that reside on your computer, click *All Add-ons*.
   - To display only those add-ons that were needed for the current webpage or a recently viewed webpage, click *Currently loaded Add-ons.*

- To display add-ons that were pre-approved by Microsoft, your computer manufacturer, or a service provider, click *Add-ons that run without permission*.
- To display only 32-bit ActiveX controls, click *Downloaded Controls*.

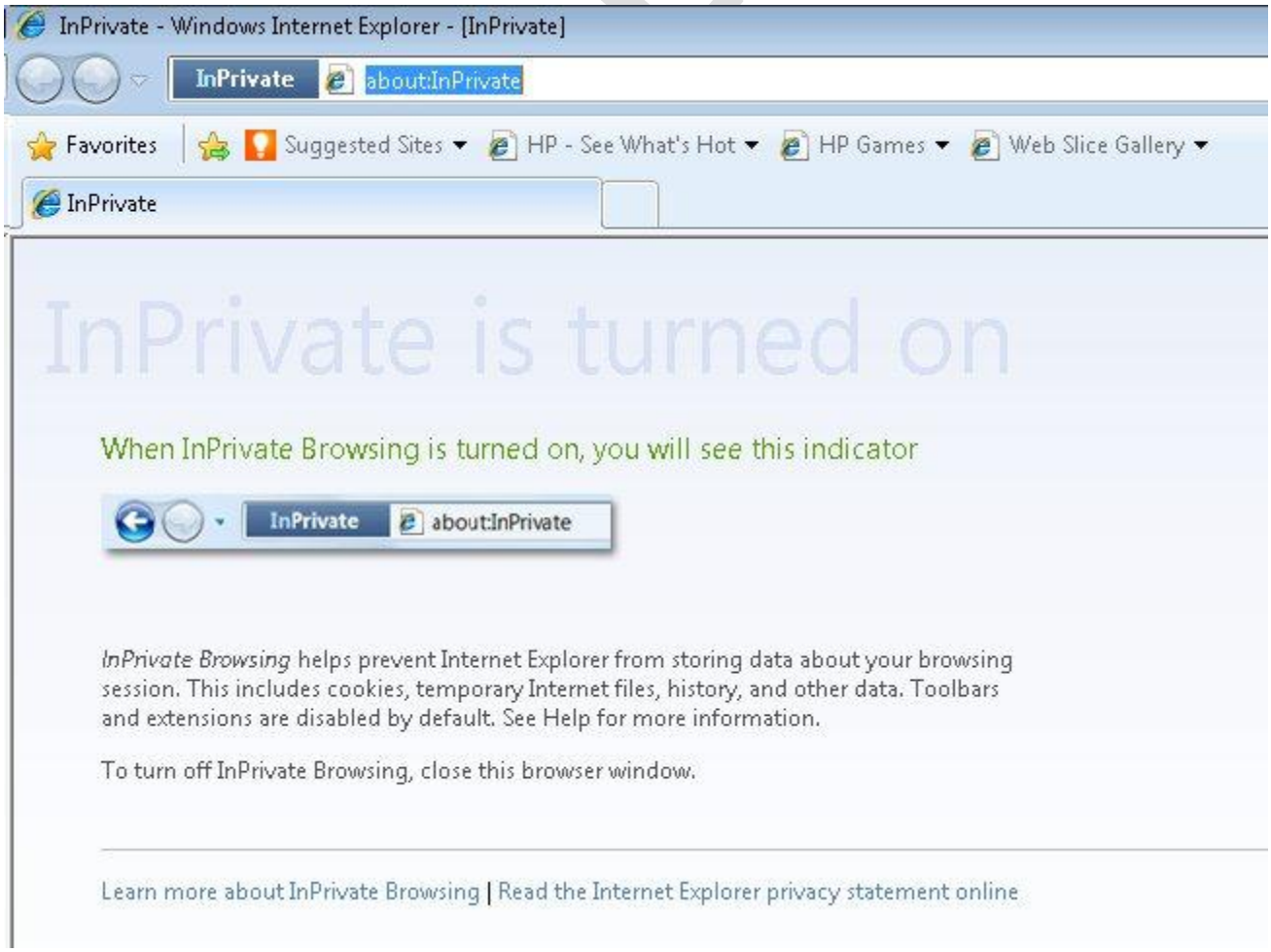
3. Selecting an add-on will allow you to view more information and/or disable it. Disabling add-ons can help you determine which one is causing problems.

InPrivate Browsing:

InPrivate Browsing enables you to surf the web without leaving a trail in Internet Explorer. This helps prevent anyone else who might be using your computer from seeing where you visited and what you looked at on the web.

To turn on InPrivate Browsing, follow these steps:

1. From the *Safety* menu, select *InPrivate Browsing*.
2. The browser's appearance will change to that shown in the image below:



When you start InPrivate Browsing, Internet Explorer opens a new browser window. The protection that InPrivate Browsing provides is only in effect during the time that you use that window. You can open as many tabs as you want in that window, and they will all be protected by InPrivate Browsing. However, if you open another browser window, that window will not be protected by InPrivate Browsing. To end your InPrivate Browsing session, close the browser window.

While you are surfing using InPrivate Browsing, Internet Explorer stores some information—such as cookies and temporary Internet files—so that the webpages you visit will work correctly. However, at the end of your InPrivate Browsing session, this information is discarded.

InPrivate Filtering:

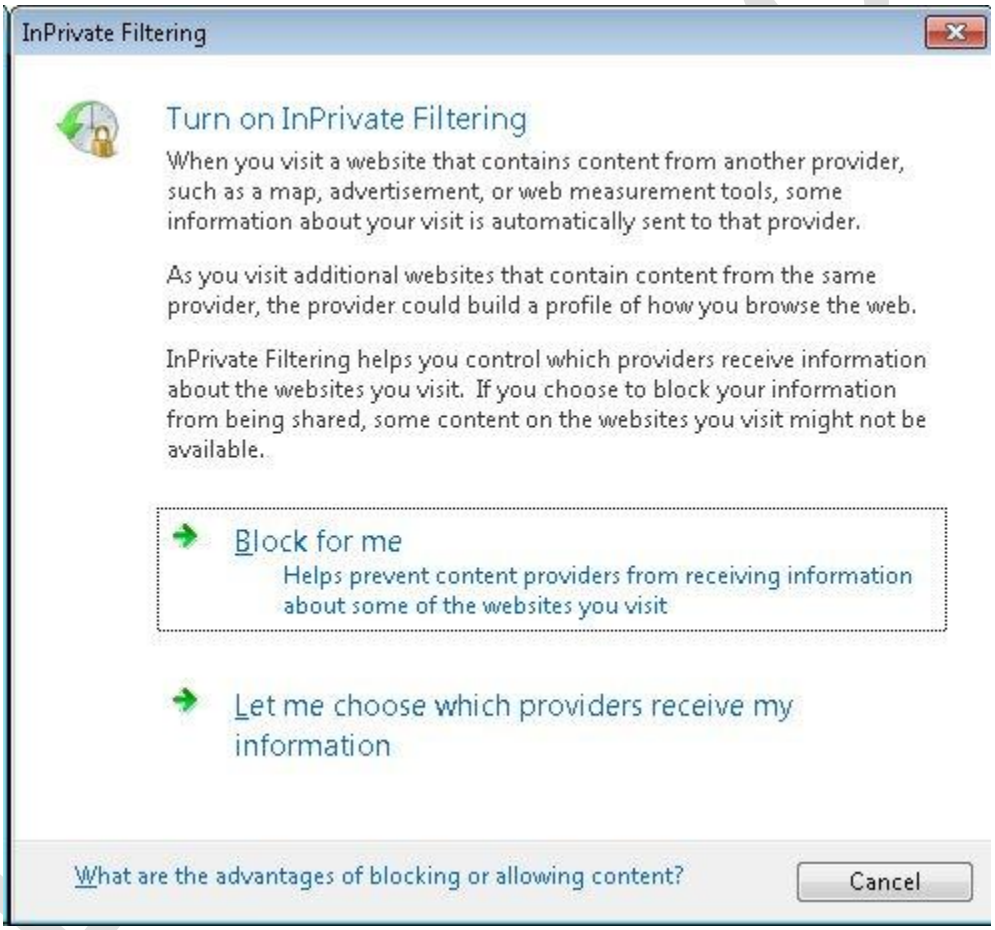
InPrivate Filtering helps prevent website content providers from collecting information about sites you visit. Many webpages use content—such as advertisements, maps, or web analysis tools—from websites other than the one you are visiting. These websites are called content providers or third-party websites. When you visit a website with third-party content, some information about you is sent to the content provider. If a content provider offers content to a large number of the websites you visit, the content provider could develop a profile of your browsing preferences. Profiles of browsing preferences can be used in a variety of ways, including for analysis and serving targeted advertisements.

Usually this third-party content is displayed seamlessly, such as in an embedded video or image. The content appears to originate from the website you originally went to, so you may not know that another website might be able to see where you are surfing. Web analysis or web measurement tools report website visitors' browsing habits, and are not always obvious to you. While these tools can sometimes appear as visible content (such as a visitor counter, for example), they are often not visible to users, as is often the case with web beacons. Web beacons are typically single-pixel transparent images whose sole purpose is to track website usage, and they do not appear as visible content.

InPrivate Filtering works by analyzing web content on the webpages you visit, and if it sees the same content being used on a number of websites, it will give you the option to allow or block that content. You can also choose to have InPrivate Filtering automatically block any content provider or third-party website it detects, or you can choose to turn off InPrivate Filtering.

To turn on InPrivate Filtering, follow these steps:

1. From the *Safety* menu, select *InPrivate Filtering*.
2. Next, you will be able to choose to have IE decide which content to block, or manually choose which content providers to block.

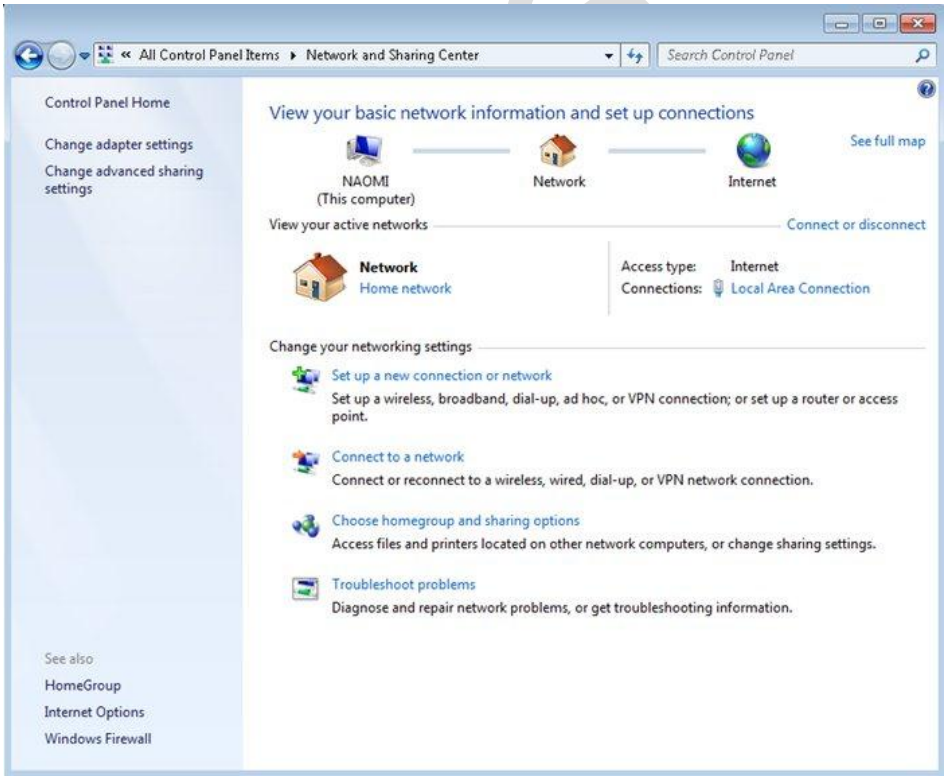


If you choose to turn on InPrivate Filtering, some content on websites may not be available.

70-680 Study Guide - Configure IPv4 and IPv6 Network Settings

Network and Sharing Center:

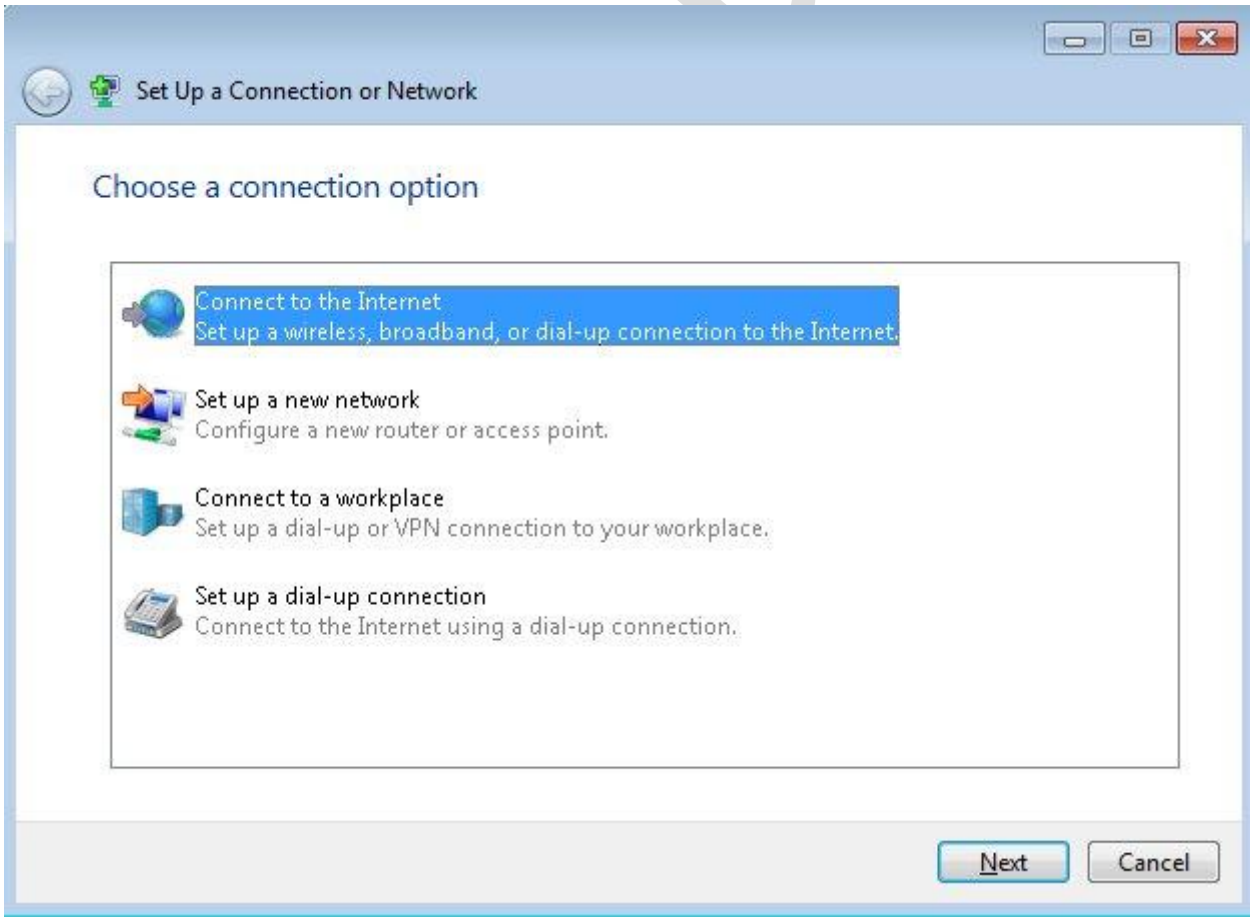
Windows 7 networking starts with the Network and Sharing Center which provides a centralized location where you can view, create, and modify local area network (LAN), wireless local area network (WLAN), virtual private network (VPN), dial-up, and Broadband connections on your client and server computers. In addition, you can configure connections to the local computer and sharing options that specify the content that is available to other computers and devices on the network; and you can use Network and Sharing Center tools like Network Map and Network Location to view and specify additional settings about networks and network profiles. It can also be used to troubleshoot network connectivity issues. The Network and Sharing center can be accessed via the control panel.



Adding a Network Connection:

If your computer has a network adapter that is connected to a local area network, you do not need to manually create a LAN connection, because Windows automatically creates and configures the connection when you start your computer. Other types of connections such as VPN and dial-up can be configured as follows:

1. Open the *Network and Sharing Center* control panel.
2. In Change your network settings, click *Set up a new connection or network*. The Set up a new connection or network wizard opens.



3. Select the type of network or connection you wish to establish and complete the rest of the wizard.

Network Locations:

The first time that you connect to a network, you must choose a network location. This automatically sets the appropriate firewall and security settings for the type of network that you connect to. If you connect to networks in different locations (for example, a network at your home, at a local coffee shop, or at work), choosing a network location can help ensure that your computer is always set to an appropriate security level.

There are four network locations:

- **Home Network** - For home networks or when you know and trust the people and devices on the network. Computers on a home network can belong to a homegroup. Network discovery is turned on for home networks, which allows you to see other computers and devices on the network and allows other network users to see your computer. For more information, see What is network discovery?
- **Work Network** - For small office or other workplace networks. Network discovery, which allows you to see other computers and devices on a network and allows other network users to see your computer, is on by default, but you can't create or join a homegroup.
- **Public Network** - For networks in public places (such as internet cafes or airports). This location is designed to keep your computer from being visible to other computers around you and to help protect your computer from any malicious software on the Internet. HomeGroup is not available on public networks, and network discovery is turned off. You should also choose this option if you're connected directly to the Internet without using a router, or if you have a mobile broadband connection.
- **Domain Network** - Used for domain networks such as those at enterprise workplaces. This type of network location is controlled by your network administrator and can't be selected or changed.

About IPv4:

Once your network connection(s) are established, it is time to configure IP settings. Every IP address can be broken down into 2 parts, the Network ID and the Host ID. All hosts on the same network must have the same netid. Each of these hosts must have a hostid that is unique in relation to the netid. IPv4 addresses are divided into 4 octets with each having a maximum value of 255. We view IPv4 addresses in decimal notation such as 124.35.62.181, but it is actually utilized as binary data.

IP addresses are divided into 3 classes as shown below:

Class	Range
A	1-126
B	<128-191
C	192-223

NOTE: 127.x.x.x is reserved for loopback testing on the local system and is not used on live systems. The following address ranges are reserved for private networks:

10.0.0.0 - 10.254.254.254
172.16.0.0 - 172.31.254.254
192.168.0.0 - 192.168.254.254

About IPv6:

IPv4 has nearly run out of available IP addresses due to the large influx of internet users and expanding networks. As a result, the powers that be had to create a new addressing scheme to deal with this situation and developed IPv6. This new addressing scheme utilizes a 128 bit address (instead of 32) and utilizes a hex numbering method in order to avoid long addresses such as 132.64.34.26.64.156.143.57.1.3.7.44.122.111.201.5. The hex address format will appear in the form of 3FFE:B00:800:2::C for example. The IPv6 equivalent of IPv4's loopback address is 0:0:0:0:0:0:0:1. This can be abbreviated as ::1.

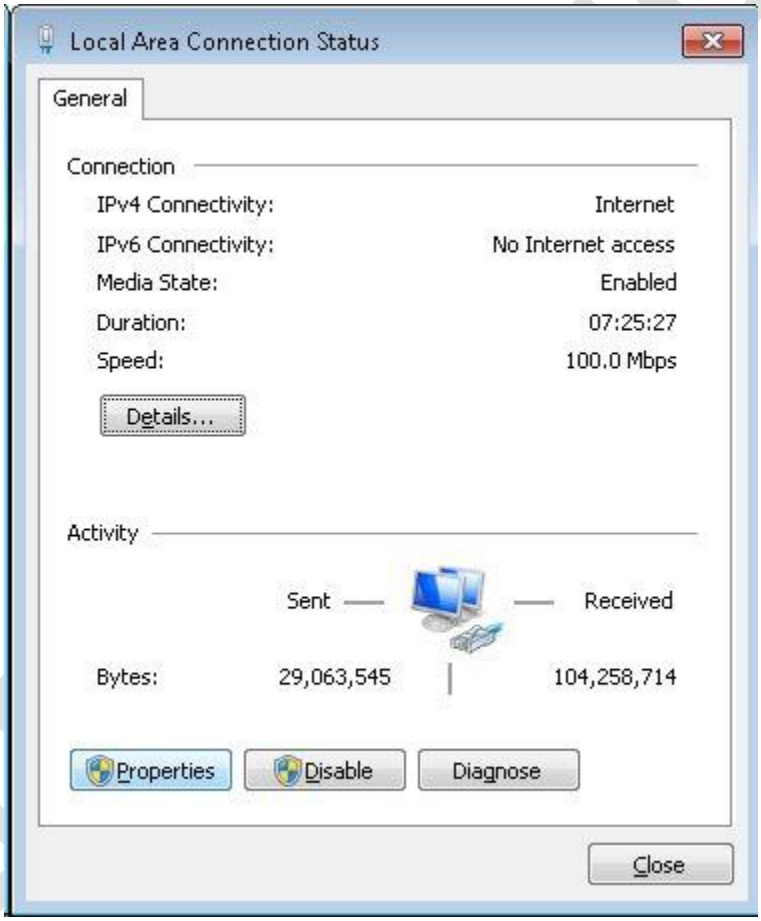
Windows 7 supports both IPv4 and IPv6 through a dual-IP-layer architecture and both are installed and enabled by default. This architecture enables you to tunnel IPv6 traffic across an IPv4 network in addition to tunneling IPv4 traffic across an IPv6 network.

Configuring IP Settings:

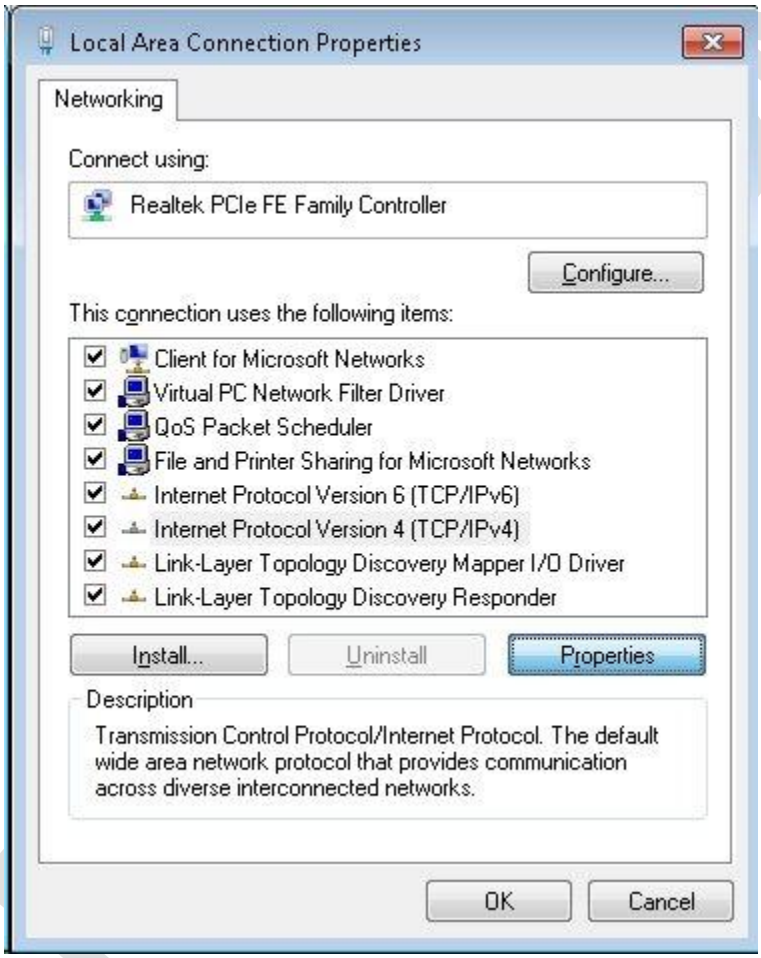
You can configure network settings on your Windows 7 computer either statically or dynamically. Static network settings include assigning the IP address, and other related information like gateway, DNS etc manually which enable it to become a part of a network. Dynamic settings make use of Dynamic Host Configuration Protocol (DHCP) to assign IP address and other networking information to your system automatically from a pre-set pool of addresses.

Follow these steps to configure TCP/IP settings manually on your computer:

1. Open Network Connections by clicking the *Start* button, then click *Control Panel* and *Network and Internet* inside the control panel.
2. Click *Network and Sharing Center* on your computer.
3. Click *Local Area Connections* and then click *Properties* to configure network addresses and other information.



4. Click the *Networking* tab and then, click either *Internet Protocol Version 4 (TCP/IPv4)* or *Internet Protocol Version 6 (TCP/IPv6)* and then click *Properties*.



5. To specify IPv4 IP address settings:
   - To configure IP address automatically, click *Obtain an IP address automatically*, and then click *OK*. This option will only work if there is a DHCP server on your network with available addresses to lease.
   - To specify an IP address manually, click *Use the following IP address*, and then, in the IP address, Subnet mask, and Default gateway boxes, type the IP address settings.
6. To specify DNS server address settings:
   - To get the DNS server address automatically, click *Obtain DNS server address automatically*, then click the *Advanced* button. Select the *WINS* tab. Under *NetBIOS setting*, select the *Default* and then click *OK*.
   - To specify a DNS server address manually, click *Use the following DNS server addresses* radio button, and then, for the Preferred DNS server and Alternate DNS server, type the addresses of the primary and secondary DNS servers.
7. Click *OK*. This will make the appropriate changes in the TCP/IP configuration of tour computer.

Note: If you wish to configure IPv6 to obtain an IP address (and other settings) automatically, your network must have a DHCPv6 capable DHCP server.

TCP/IP Fundamentals for Microsoft Windows
TCP/IP (v4 and v6) Technical Reference

Automatic Private IP Addressing (APIPA):

A Windows 7 computer that is configured to use DHCP can automatically assign itself an Internet Protocol (IP) address if a DHCP server is not available. For example, this could occur on a network without a DHCP server, or on a network if a DHCP server is temporarily down for maintenance.

The Internet Assigned Numbers Authority (IANA) has reserved 169.254.0.0-169.254.255.255 for Automatic Private IP Addressing. As a result, APIPA provides an address that is guaranteed not to conflict with routable addresses.

After the network adapter has been assigned an IP address, the computer can use TCP/IP to communicate with any other computer that is connected to the same LAN and that is also configured for APIPA or has the IP address manually set to the 169.254.x.y (where x.y is the client's unique identifier) address range with a subnet mask of 255.255.0.0. Note that the computer cannot communicate with computers on other subnets, or with computers that do not use automatic private IP addressing. This also means that a computer with an APIPA address cannot connect to the internet, only other computers with APIPA addresses. Automatic private IP addressing is enabled by default.

If a DHCP enabled computer is using an IP address in the APIPA range, it often indicates that the computer is unable to contact the DHCP server.

Link-Local Multicast Name Resolution:

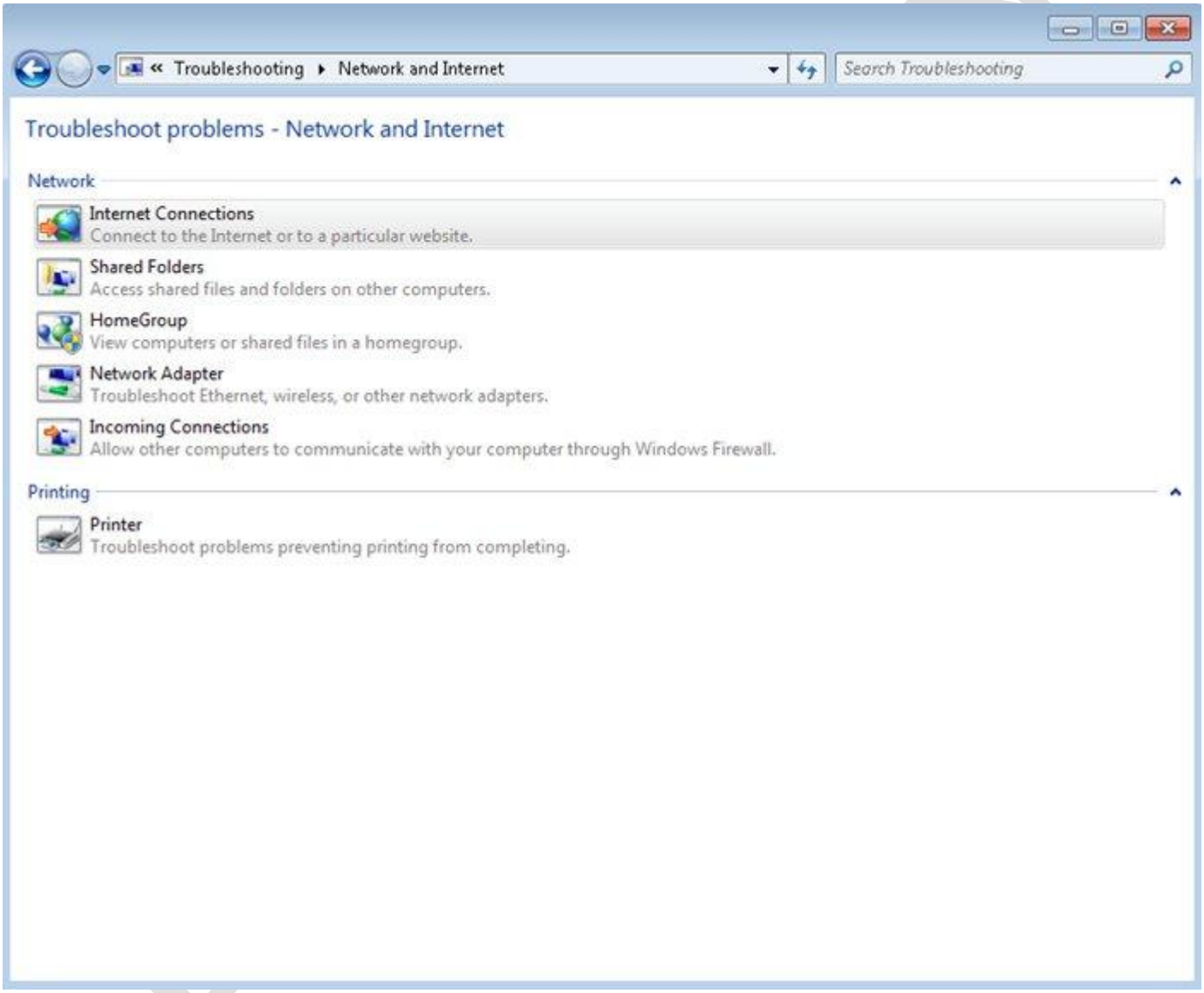
LLMNR is a Microsoft designed protocol that can be used on private networks where there is no DNS server, as a mechanism for providing name resolution like DNS does. It is one of many protocols that do similar things for zero-configuration networks - they basically allow private networks to function as IP networks without requiring hosts to be configured with addresses.

Link-Local Multicast Name Resolution

Resolving Connectivity Issues:

Windows offers a number of tools and utilities for troubleshooting connectivity and other network problems. A good place to start is by clicking on the *Troubleshoot problems* option in the Network and Sharing Center. This

opens the Windows Network Diagnostics tool. If Windows 7 detects the problem, it may be able to automatically fix it, or possibly offer a solution.

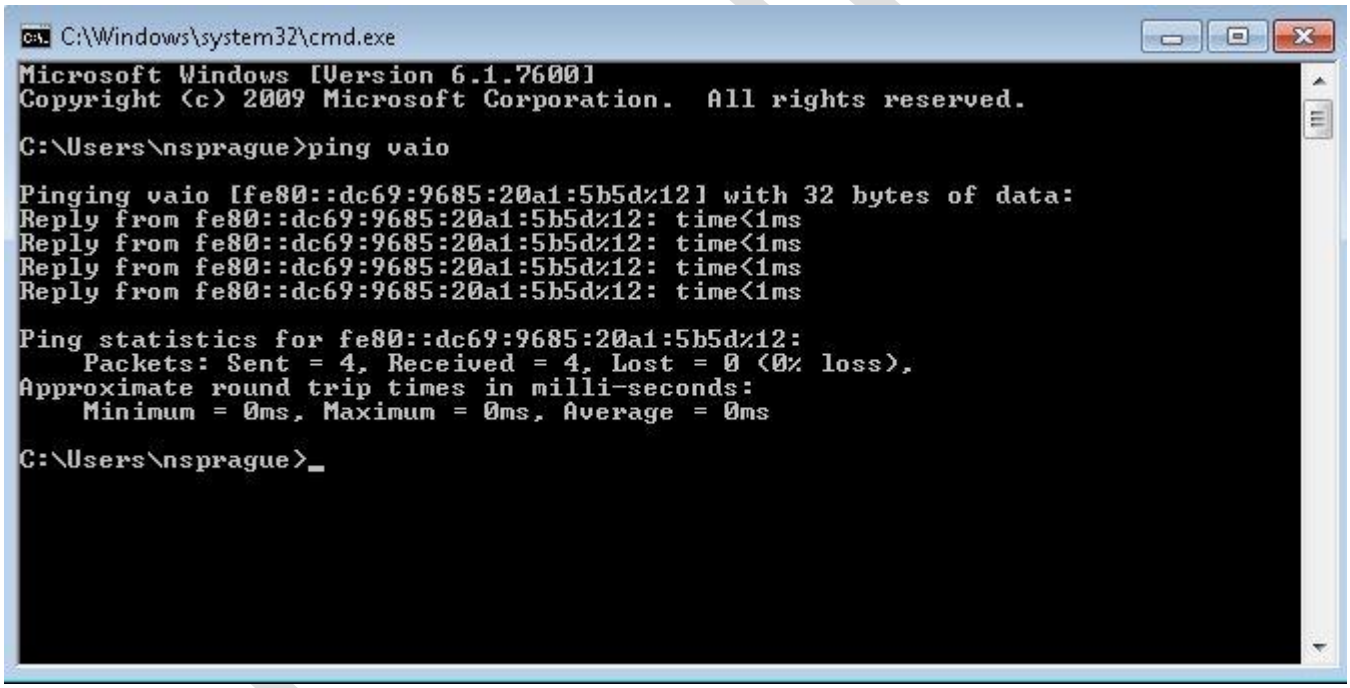


If this wizard is unable to fix the problem or offer a solution, there are a number of other tools listed below that can help.

- **IPCONFIG** - This command is used to view network settings from a Windows computer command line. Below are the ipconfig switches that can be used at a command prompt:

- *ipconfig /all* will display all of your IP settings.
- *ipconfig /renew* forces the DHCP server, if available to renew a lease.
- *ipconfig /renew6* renews n IPv6 DHCP lease.
- *ipconfig /flushdns* purges the DNS resolver cache.
- *ipconfig /registerdns* refreshes all DHCP leases and reregisters DNS names.
- *ipconfig /release* forces the release of a lease.

- **PING (Packet InterNet Groper)** - PING is a command-line utility used to verify connections between networked devices. PING uses ICMP echo requests that behave similarly to SONAR pings. The standard format for the command is *ping [IP address or hostname]*. If successful, the ping command will return replies from the remote host with the time it took to receive the reply. If unsuccessful, you will likely recieve and error message. This is one of the most important tools for determining network connectivity between hosts.



- **TRACERT** - A command-line troubleshooting tool that enables you to view the route to a specified host. This will show how many hops the packets have to travel and how long it takes. Basic usage looks like: *tracert [IP address or hostname]*.

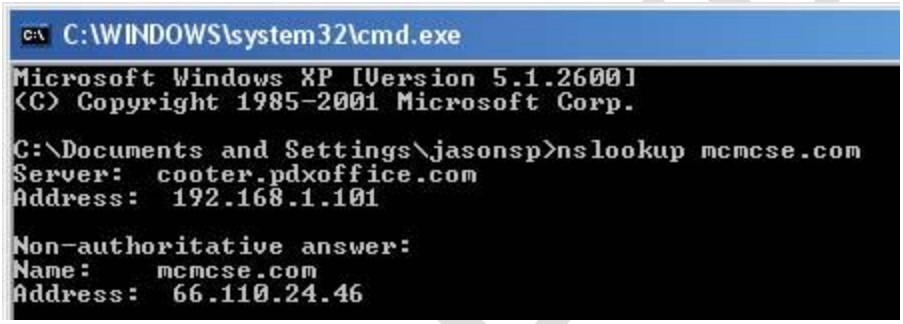
```
[root@mcmcse root]# traceroute in-portal.net
traceroute to in-portal.net (66.110.24.202), 30 hops max, 38 byte packets
 1  209.211.248.254 (209.211.248.254)  64.784 ms  310.778 ms  1.341 ms
 2  bos-edge-02.inet.qwest.net (67.130.100.217)  1.963 ms  1.788 ms  1.758 ms
 3  bos-core-02.inet.qwest.net (205.171.28.29)  1.826 ms  1.705 ms  1.663 ms
 4  jfk-core-01.inet.qwest.net (205.171.8.18)  6.996 ms  6.901 ms  6.942 ms
 5  jfk-brdr-02.inet.qwest.net (205.171.230.25)  6.842 ms  6.822 ms  6.914 ms
 6  if-4-0-3.mcore3.nyy-newyork.teleglobe.net (216.6.81.1)  6.965 ms  7.443 ms  6.949 ms
 7  216.6.97.41 (216.6.97.41)  8.198 ms  7.959 ms  7.838 ms
     MPLS Label=116 CoS=7 TTL=1 S=0
 8  if-3-0.core2.ct8-chicago.teleglobe.net (66.110.14.21)  33.005 ms  32.984 ms  32.950 ms
     MPLS Label=35 CoS=7 TTL=1 S=0
 9  vlan2.msfc1.ct8-chicago.teleglobe.net (66.110.15.3)  29.961 ms  29.894 ms  30.033 ms
10  in-commerce.net (66.110.24.202)  32.928 ms !<10>  32.767 ms !<10>  32.832 ms !<10>
```

- **PATHPING** - This tool is very similar to tracert, however, pathping provides more detailed statistics on individual hops.
- **ARP (Address Resolution Protocol)** - A host PC must have the MAC and IP addresses of a remote host in order to send data to that remote host, and it's ARP that allows the local host to request the remost host to send the local host its MAC address through an ARP Request. The *ARP -a [IP Address]* command will show you the MAC address associated with a computer or device's IP address.

```
C:\Documents and Settings\jasonsp>arp -a

Interface: 192.168.1.6 --- 0x2
  Internet Address      Physical Address      Type
  192.168.1.1           00-1e-e5-a2-ee-eb     dynamic
  192.168.1.4           00-19-21-40-be-bc     dynamic
  192.168.1.101         00-10-dc-25-a0-3b     dynamic
```

- **NSLOOKUP** - This is a command that queries a DNS server for machine name and address information. To use nslookup, type *nslookup [IP address or computer name or domain name]*. NSLOOKUP will return the name, all known IP addresses and all known aliases (which are just alternate names) for the identified machine. NSLOOKUP is a useful tool for troubleshooting DNS problems.



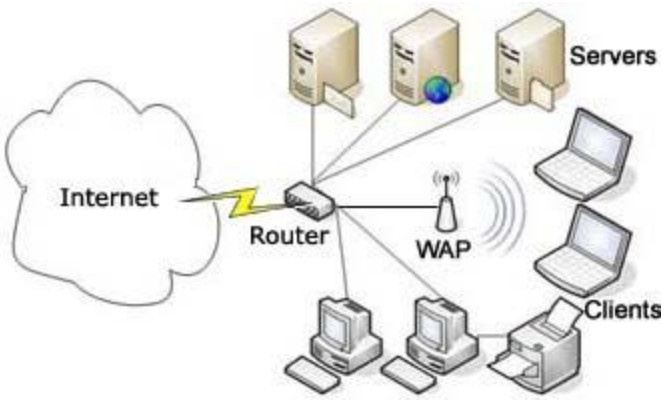
70-680 Study Guide - Configure Networking Settings

Note: This section should probably be read before the previous one, "Configure IP4 and IP6 Network Settings", however, this is how Microsoft listed their exam objectives. Furthermore, since most of the information about setting up networks in Windows 7 was covered in the previous section, this section will mostly focus on wireless networking.

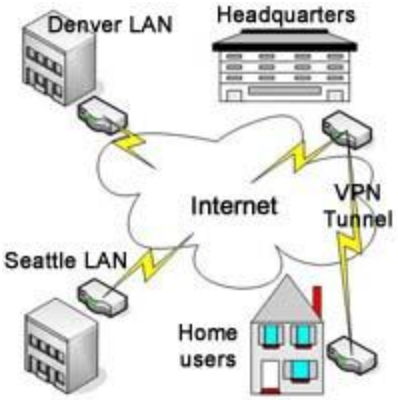
Network Types:

There are 2 basic types of networks, Wide Area Networks (WANs) and Local Area Networks (LANs). Most LANs are confined to a single building or group of buildings. However, one LAN can be connected to other LANs over nearly any distance via telephone lines (DSL/ISDN), coaxial cable, fiber, wi-fi, etc. A system of LANs connected in this way is a WAN. Although we will be focusing on LANs in the guide, the figures below illustrate the difference between the 2 types of networks.

Local Area Network (LAN)



Wide Area Network (WAN)



Note that the LAN image shows a hybrid network consisting of wired and wireless connections. Also note that on smaller LANs, the wireless access point (WAP) and router are often the same device.

Introduction to Wireless Networks:

Wireless networks allow computers to comunicate without the use of cables using IEEE 802.11 standards, also known as Wi-Fi. A connection is made from a device, which is usually a PC or a Laptop with a wireless network interface card (NIC), and a Wireless Access Point (WAP), which acts as a bridge between the wireless stations and Distribution System (DS) or wired networks. An 802.11 wireless network adapter can operate in two modes, Ad-Hoc and Infrastructure. In infrastructure mode, all your traffic passes through the WAP. In Ad-hoc mode your computers talk directly to each other and do not need an access point. The table below shows the various standards.

Standard	Speed	Distance	Frequency
802.11a	54 mbps	100 ft	5 GHz
802.11b	11 mbps	300 ft	2.4 GHz
802.11g	54 mbps	300 ft	2.4 GHz
802.11n	540 mbps	600 ft	5 GHz and/or 2.4 GHz

Wireless Authentication and Encryption:

By default, wireless signals can be intercepted and captured by anyone within range of the WAP which is a huge security concern. For that reason, it is always recommended that you use some form of encryption. Below is a list of common encryption types:

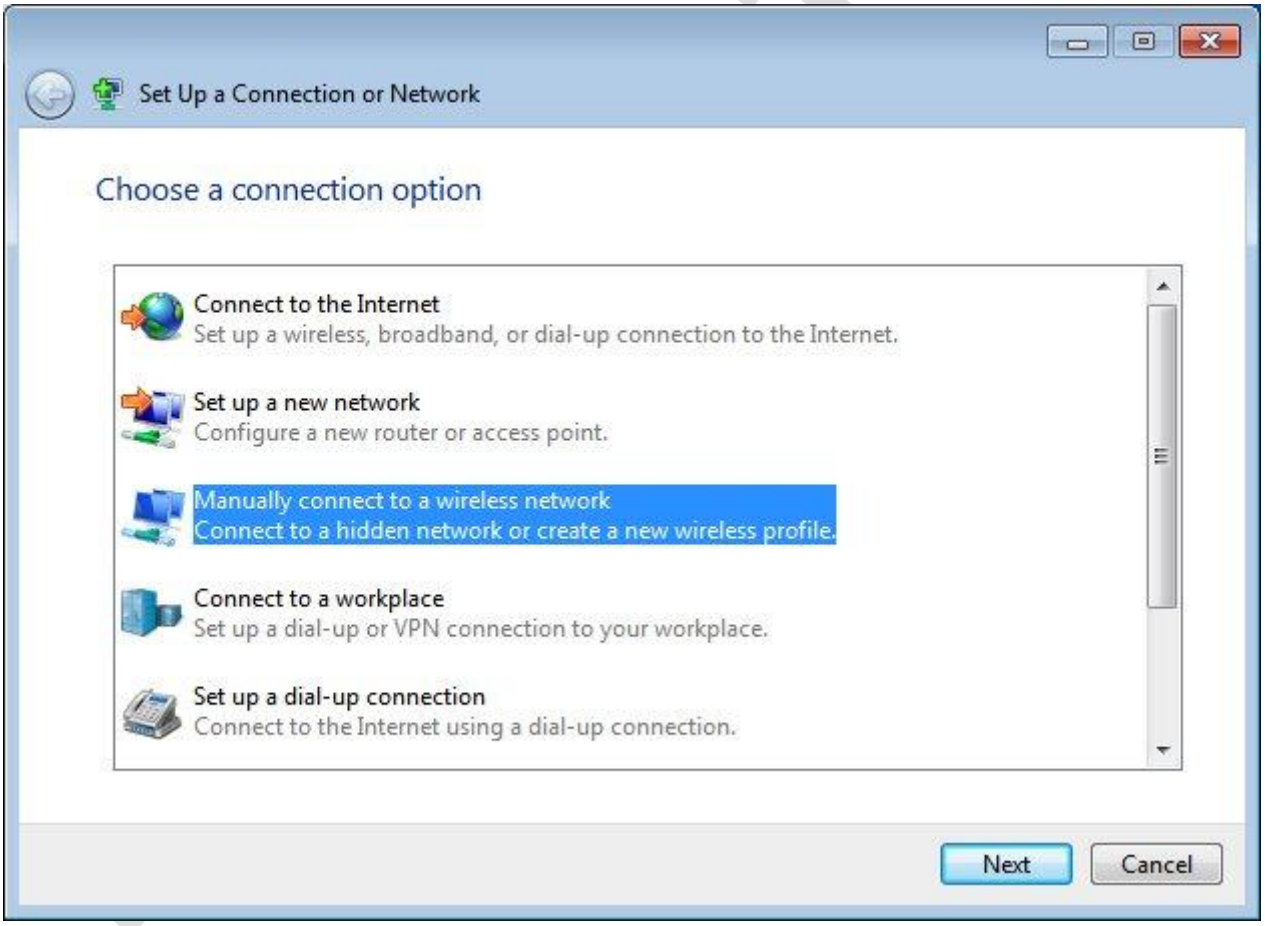
- **WEP** - Wired Equivalent Privacy is a security encryption algorithm that is easily cracked. For this reason, it has been replaced by other technologies.
- **TKIP** - Temporal Key Integrity Protocol was designed as a solution to replace WEP without requiring the replacement of legacy hardware. TKIP suffered from similar flaws as WEP and has been replaced by more secure encryption schemes.
- **RADIUS** - Remote Authentication Dial In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for computers to connect and use a network service. RADIUS is often used by ISPs and enterprises to manage access to the Internet or internal networks, and wireless networks. Microsoft's answer to corporate wireless security is the use of RADIUS authentication through its Internet Authentication Services (IAS) product.
- **WPA** - The original WPA standard used TKIP, but was later replaced by WPA2 which uses a more secure AES-based algorithm. WPA uses a 256 bit key to encrypt data. This key may be entered either as a string of 64 hexadecimal digits, or as a passphrase of 8 to 63 characters. It is susceptible to brute force attacks when a weak passphrase is used. In most cases, WPA2 is the recommended option to use.

It is also important to change the default username and password on your wireless access point/router.

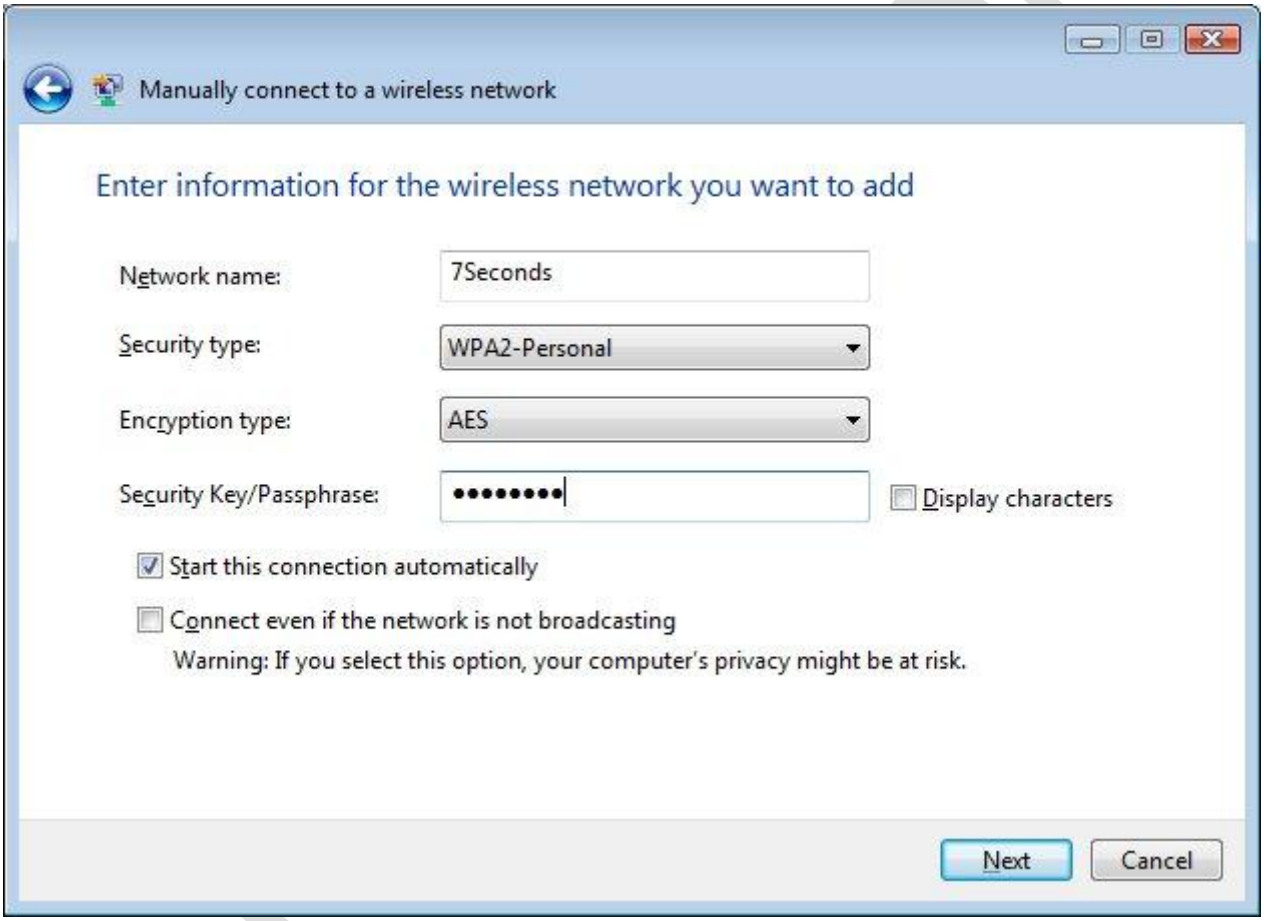
Setting Up a Wireless Network:

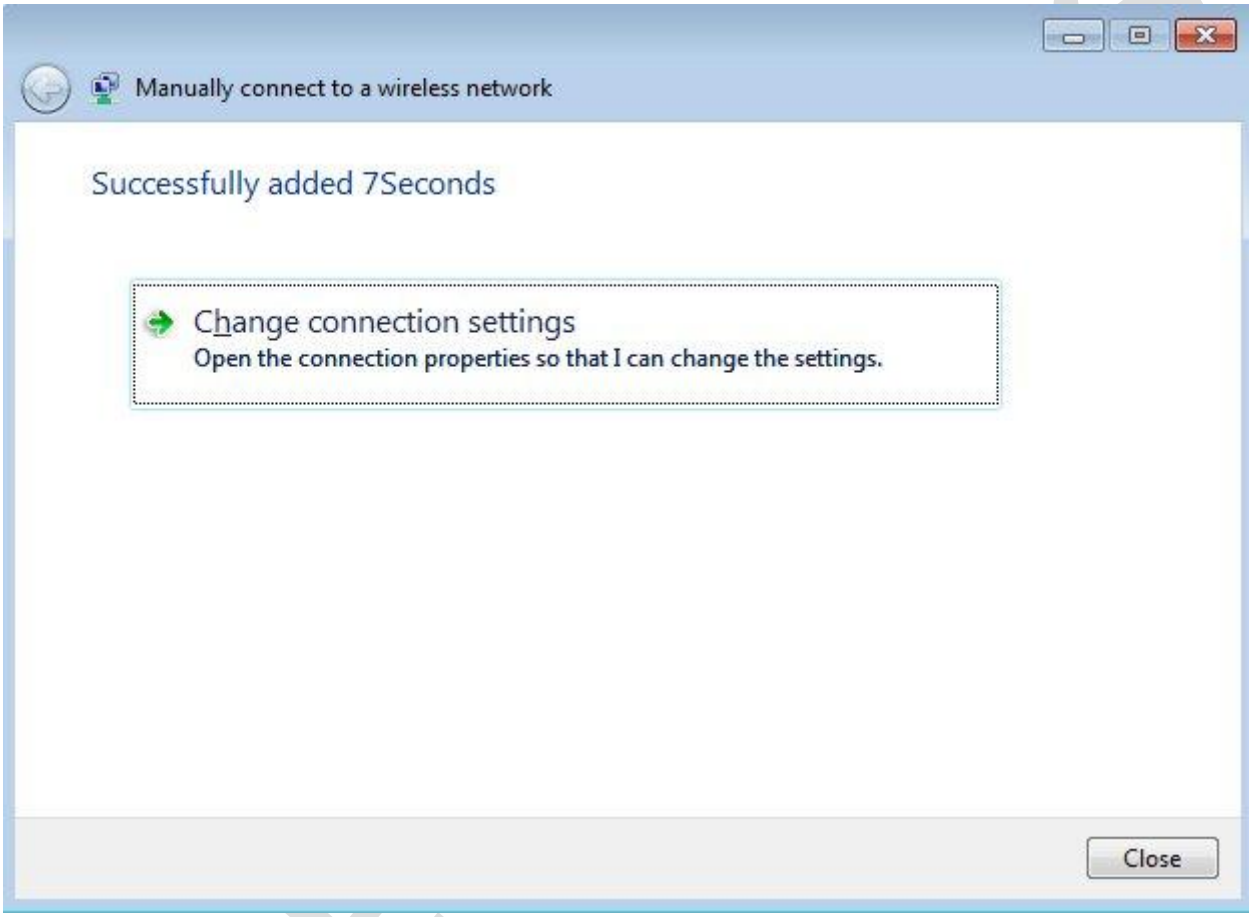
Once your wireless access point is properly configured, you can follow these steps to set up your wireless network in Windows:

1. Open Network and Sharing Center by clicking the *Start* button , and then clicking *Control Panel*. In the search box, type *network*, and then click *Network and Sharing Center*.
2. Click *Set up a new connection or network*.
3. Click *Set up a new network*, and then click *Next*.



4. The wizard will walk you through creating a network name and entering the security key you configured on the WAP. The network name is the SSID that you entered when configuring your access point. Make sure that this SSID is unique or your computer could end up trying to switch back and forth between the connections and cause connectivity problems.





Note that if you are using a laptop, you need to make sure the wireless switch on the computer is turned on.

If you have multiple computers that need to be configured to connect to a wireless network, you can use a USB flash drive to set up the connection on other computers. To save your wireless network settings to a USB flash drive, insert a USB flash drive into the computer, and then follow these instructions:

1. Open the *Network and Sharing Center*.
2. In the left pane, click *Manage wireless networks*.
3. Right-click the network and then click *Properties*.
4. Click *Copy this network profile to a USB flash drive*.
5. Select the USB device and then click *Next*.
6. When the wizard is complete, click the *Close button*.

Now take the USB drive to a destination computer and do the following:

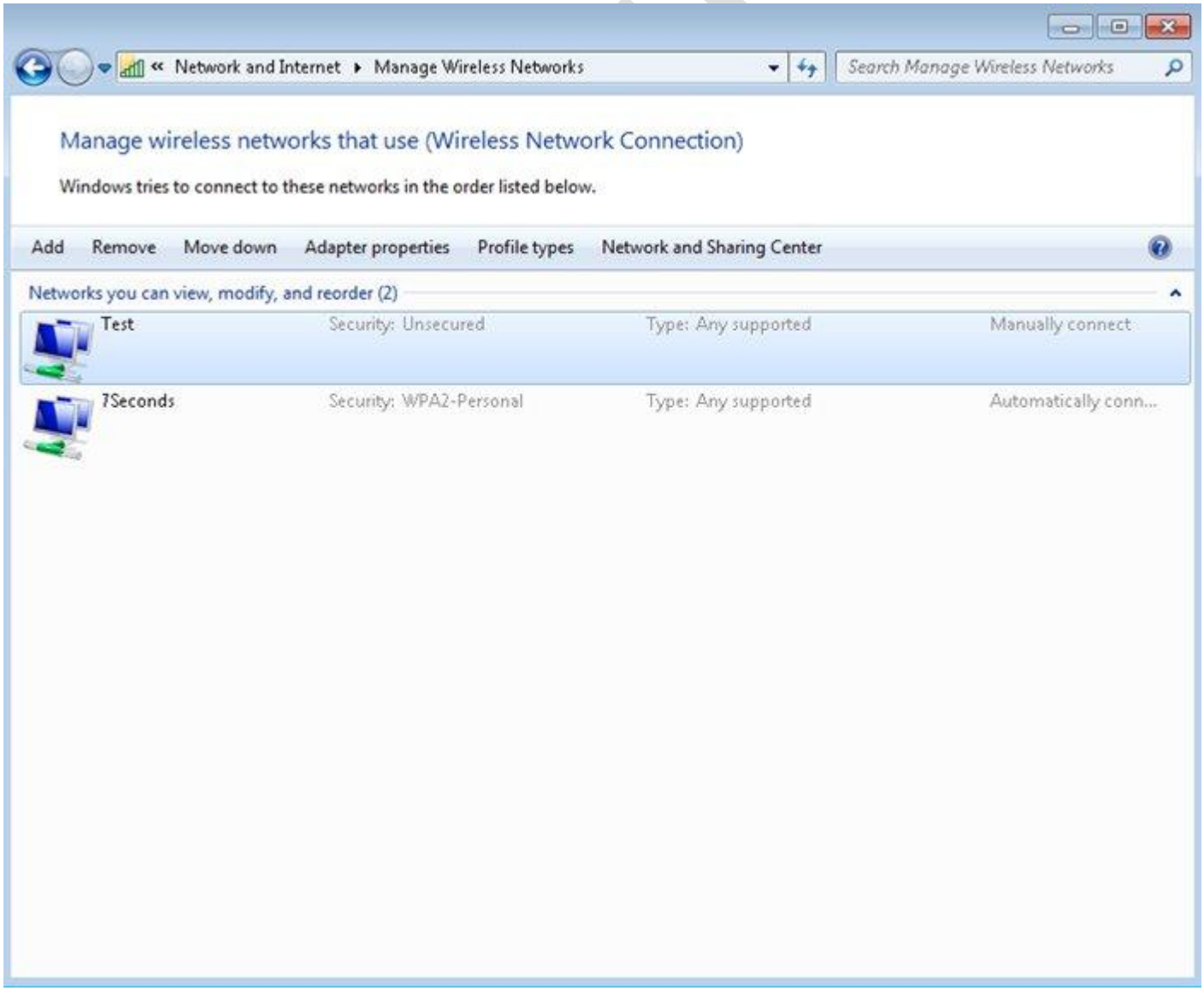
1. Plug the USB flash drive into a USB port on another computer.
2. For a computer running Windows 7, in the AutoPlay dialog box, click *Connect to a Wireless Network*.

3. When asked if you want to add the network, click the *Yes* button.
4. After you get the successful configuration message, click the *OK*.

Setting Preferred Wireless Networks:

If your computer continously attempts to connect to a different wireless network than you would like, you can change the order of your preferred wireless networks as follows:

1. Open the *Network and Sharing Center*.
2. Click *Manage wireless networks*.



3. Here you can click on a network and then move it up or down. You can also add and remove connections from this window.

Setting Up an Ad Hoc Wireless Network:

You can set up a temporary wireless network, or ad hoc network, between two or more computers running Windows 7 (or between computers running Windows 7 and Windows Vista) provided they are all within 30 feet of each other. An access point is not required to set up an ad hoc network. This enables users to share folders and other resources without needing to connect to an organizational network.

To set up an ad hoc connection, on the first computer on the network, open *Network And Sharing Center* and click *Set Up A New Connection Or Network*. Select *Set Up A Wireless Ad Hoc (Computer To Computer) Network*. You give the network a name and (if you want) set up a security key so that users joining the network need to supply a password. Other users join the ad hoc network as they would any other wireless network. You can choose to save the network settings if you want to set up an ad hoc network with the same configuration sometime in the future Ad hoc networks use IPv6 and do not require IPv4 connectivity.

Connecting to a Wireless Network:

After setting up a wireless connection for the first time as illustrated in the instructions above, Windows connects to the network automatically if you checked the *Start this connection automatically* checkbox. If you want to connect to another wireless network (such as at an internet cafe, for example), you can click the network icon on your toolbar at the bottom right section of your screen. This displays all wireless networks within range, and you can double-click the network to which you want to connect. Alternatively, you can open Network And Sharing Center and click *Connect To A Network*. To view and change your connection status, you can click *Connect or Disconnect* beside View Your Active Networks in Network And Sharing Center. This again presents you with a list of the wireless networks within range.

Location Aware Printing:

Location Aware Printing allows you to choose different default printers for different networks. This capability is useful for people who use one laptop in multiple locations—for example, at work and at home. This feature is only available on laptops and other portable devices that use a battery and are running Windows 7 Professional or higher. This can be configured using the following instructions:

1. Click the *Start* button, and then click *Devices and Printers*.
2. Under *Printers and Faxes*, select a printer by clicking on it.
3. In the menu bar, click *Manage Default Printers*.
4. In the Manage Default Printers dialog box, click *Change my default printer when I change networks*, specify which printer should be the default for each network, and then click *OK*.
5. In the *Select network list*, select a network.
6. In the *Select printer list*, click a printer to use as the default printer for that network and click *Add*.

70-680 Study Guide - Configure Windows Firewall

Introduction to Firewalls:

Firewalls are either a hardware or software entity (or a combination of both) that protects a network by stopping network traffic from passing through it. In most cases, a firewall is placed on the network to allow all internal traffic to leave the network (email to the outside world, web access, etc.), but stop unwanted traffic from the outside world from entering the internal network. This is achieved by using rules. There are 3 basic types of rules as follows:

- **Inbound rules**: These rules help protect your computer from other computers making unsolicited connections to it.
- **Outbound rules**: These rules help protect your computer by preventing your computer from making unsolicited connections to other computers.
- **Connection-specific rules**: These rules enable a computer's administrator to create and apply custom rules based on a specific connection. In Windows, this is referred to as Network Location Awareness.

Windows 7 uses two firewalls that work together: Windows Firewall and Windows Firewall with Advanced Security (WFAS). The primary difference between them being the complexity of the rules that can be configured for them.

Firewall Types:

There are 2 basic types of firewalls:

- **Network perimeter firewalls** - Network firewalls are located at the boundary between the internal network and external networks such as the Internet and provide a variety of services. This type of firewall is illustrated in the image above. Such products are either hardware-based, software-based, or can be a combination of both. Some of these firewalls also provide application proxy services like Microsoft Internet Security and Acceleration (ISA) Server. Most of these types of network firewall products provide following functionality:
    - Management and control of network traffic by performing stateful packet inspection, connection monitoring, and application-level filtering.
    - Stateful connection analysis by inspecting the state of all communications between hosts and by storing the connection data in state tables.
    - Virtual private network gateway functionality by providing IPsec authentication and encryption along with Network Address Translation-Traversal (NAT-T). It allows permitted IPsec traffic to traverse the firewall with public to private IPv4 address translation.

- **Host-based firewalls** - Network perimeter firewalls cannot provide protection for traffic generated inside a trusted network. Therefore host-based firewalls running on individual computers are needed. Host-based firewalls protect a host from unauthorized access and attack.

  Apart from blocking unwanted incoming traffic, you can configure Windows Firewall with Advanced Security to block specific types of outgoing traffic as well. Host-based firewalls provide an extra layer of security in your network.

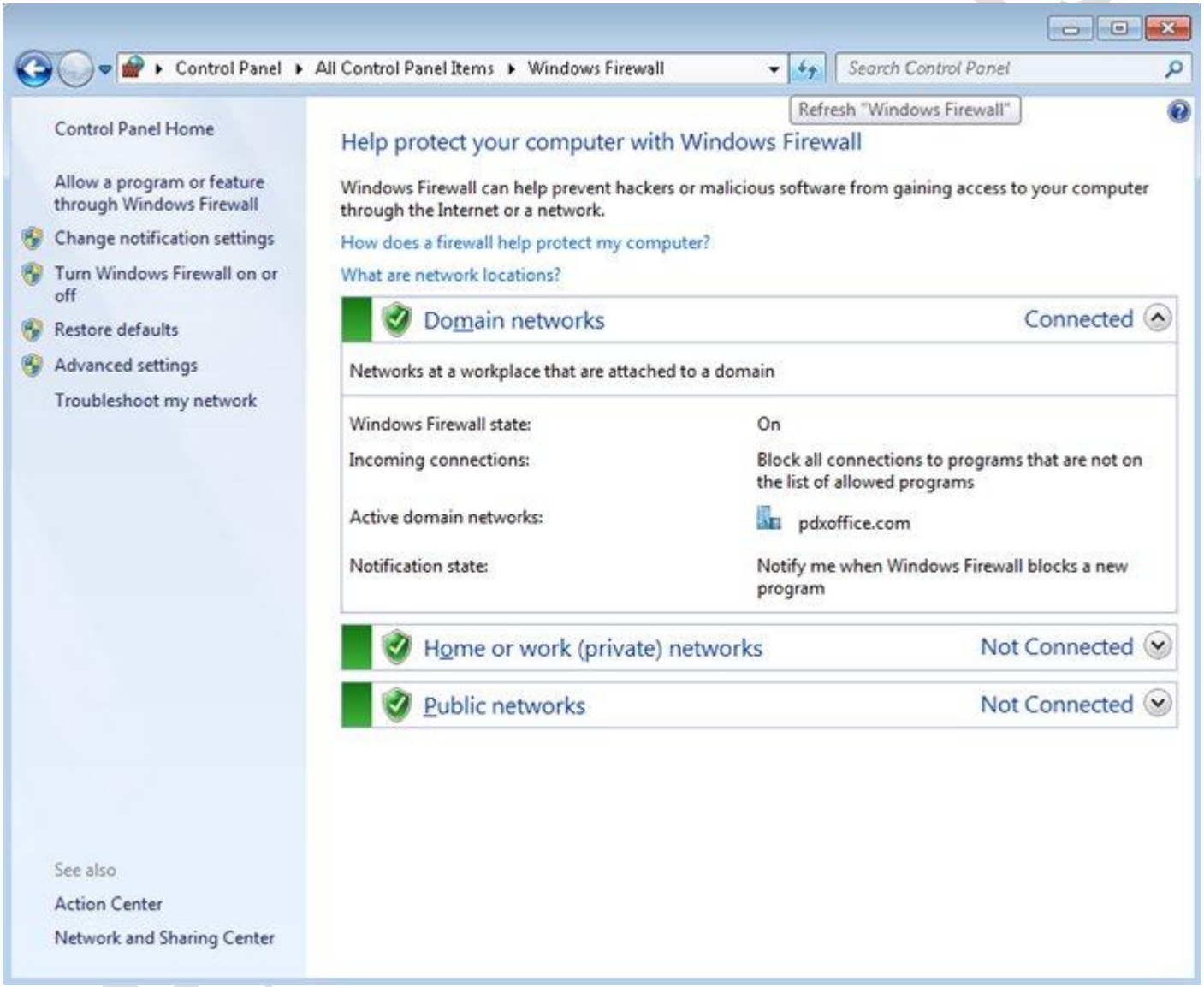
  In Windows Firewall with Advanced Security, firewall filtering and IPsec are integrated together. This integration reduces the possibility of conflict between firewall rules and IPsec connection security settings.

Network Location Awareness:

Windows 7 supports network location awareness, which enables network-interacting programs to change their behavior based on how the computer is connected to the network. In the case of Windows Firewall with Advanced Security, you can create rules that apply only when the profile associated with a specific network location type is active on your computer. There are 3 location types:

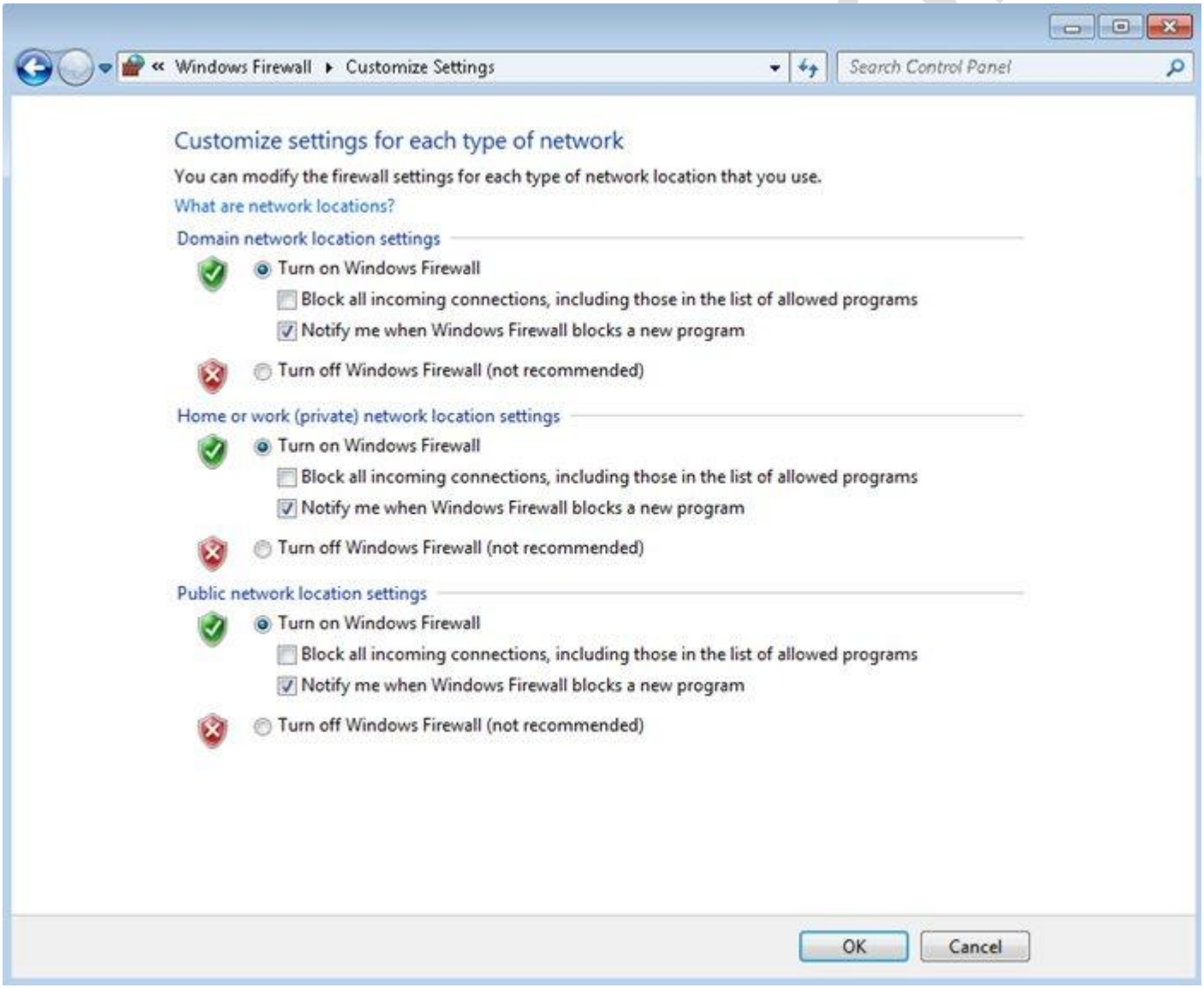
- **Public** - By default, the public network location type is assigned to any new networks when they are first connected. A public network is considered to be shared with the world, with no protection between the local computer and any other computer. Therefore, the firewall rules associated with the public profile are the most restrictive.
- **Private** - The private network location type can be manually selected by a local administrator for a connection to a network that is not directly accessible by the public. This connection can be to a home or office network that is isolated from publicly accessible networks by using a firewall device or a device that performs network address translation (NAT). Wireless networks assigned the private network location type should be protected by using an encryption protocol such as Wi-Fi Protected Access (WPA) or WPAv2. A network is never automatically assigned the private network location type; it must be assigned by the administrator. Windows remembers the network, and the next time that you connect to it, Windows automatically assigns the network the private network location type again. Because of the higher level of protection and isolation from the Internet, private profile firewall rules typically allow more network activity than the public profile rule set.
- **Domain** - The domain network location type is detected when the local computer is a member of an Active Directory domain, and the local computer can authenticate to a domain controller for that domain through one of its network connections. An administrator cannot manually assign this network location type. Because of the higher level of security and isolation from the Internet, domain profile firewall rules typically permit more network activity than either the private or public profile rule sets. On a computer

that is running Windows 7, if a domain controller is detected on any network adapter, then the Domain network location type is assigned to that network adapter.



Turning Windows Firewall On and Off:

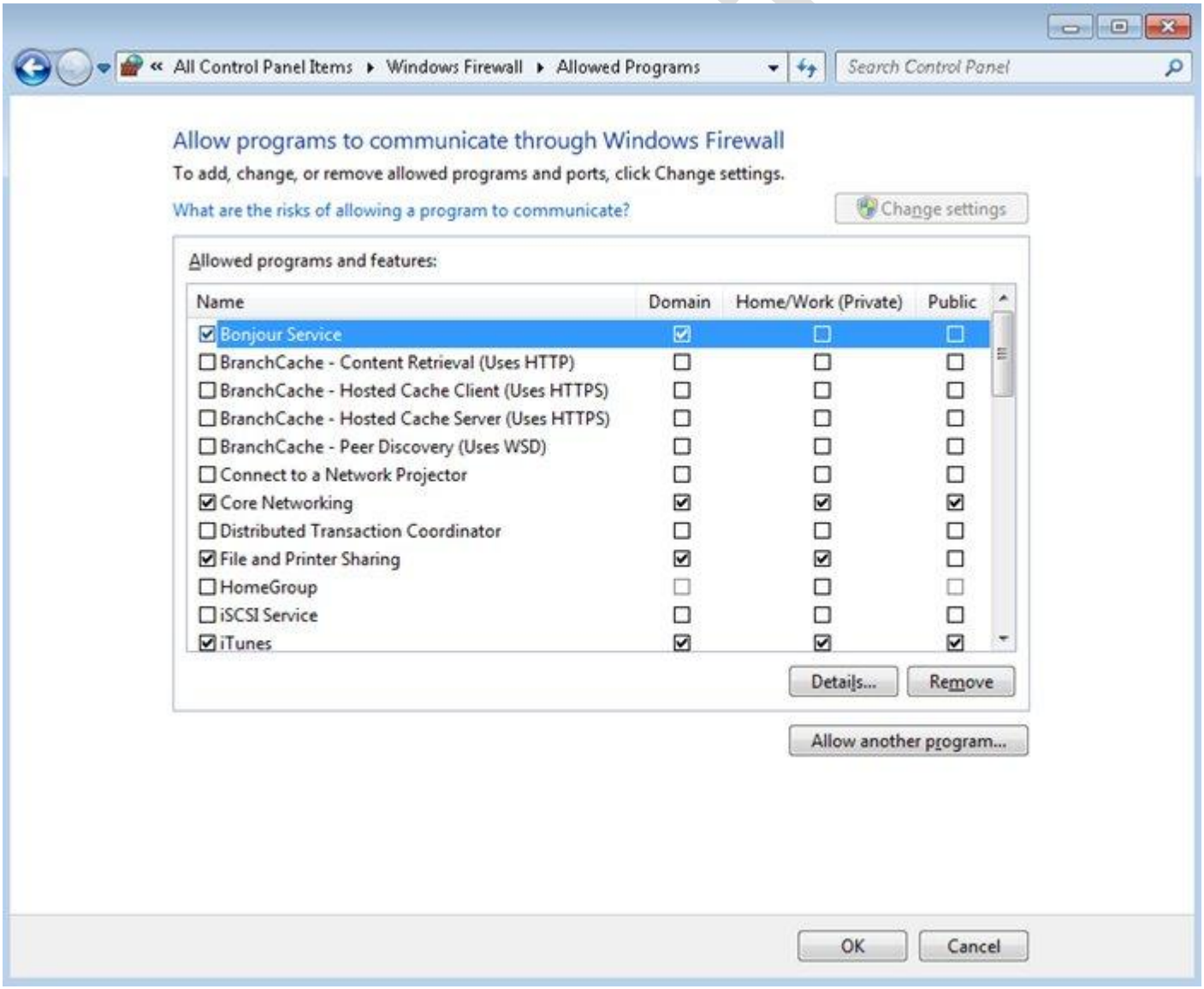
To turn Windows Firewall on or off, simply open the Windows Firewall control panel and click *Turn Windows firewall on or off*. The *Change notification settings* link brings up the same screen as shown below:



Not only can you turn the firewall on and off for each network location, you can also block all programs, and set notification when a program is blocked. One of the few reasons you would ever want to turn this off is if you had another firewall program that you want to use instead.

Allowing Programs:

Traditionally with firewalls, you can open or close a protocol port so that you can allow or block communication through the firewall. With Windows Firewall included in Windows 7, you specify which programs or features you want to communicate through the firewall. The most common options are available by clicking the *Allow a program or feature through Windows Firewall* option on the left pane of the Windows Firewall control panel. Only users that are members of the local Administrators group, or who have been delegated the appropriate privileges are able to modify Windows Firewall settings. If you need to open a port instead of specifying a program, you have to use the Windows Firewall with Advanced Security which is discussed later in this tutorial.



If a program that you want to create a rule for is not present on this list, click *Allow Another Program*. This opens the Add A Program dialog box. If the program that you want to create a rule for is not listed, click *Browse* to add it. Click the *Network Location Types* button to specify the network profiles in which the rule should be active.

If a program is blocked, the first time you try to run it you are notified by the firewall, allowing you to configure an exception that allows traffic from this program in the future. If an exception is not configured at this time, you will need to use the steps above to allow traffic through.

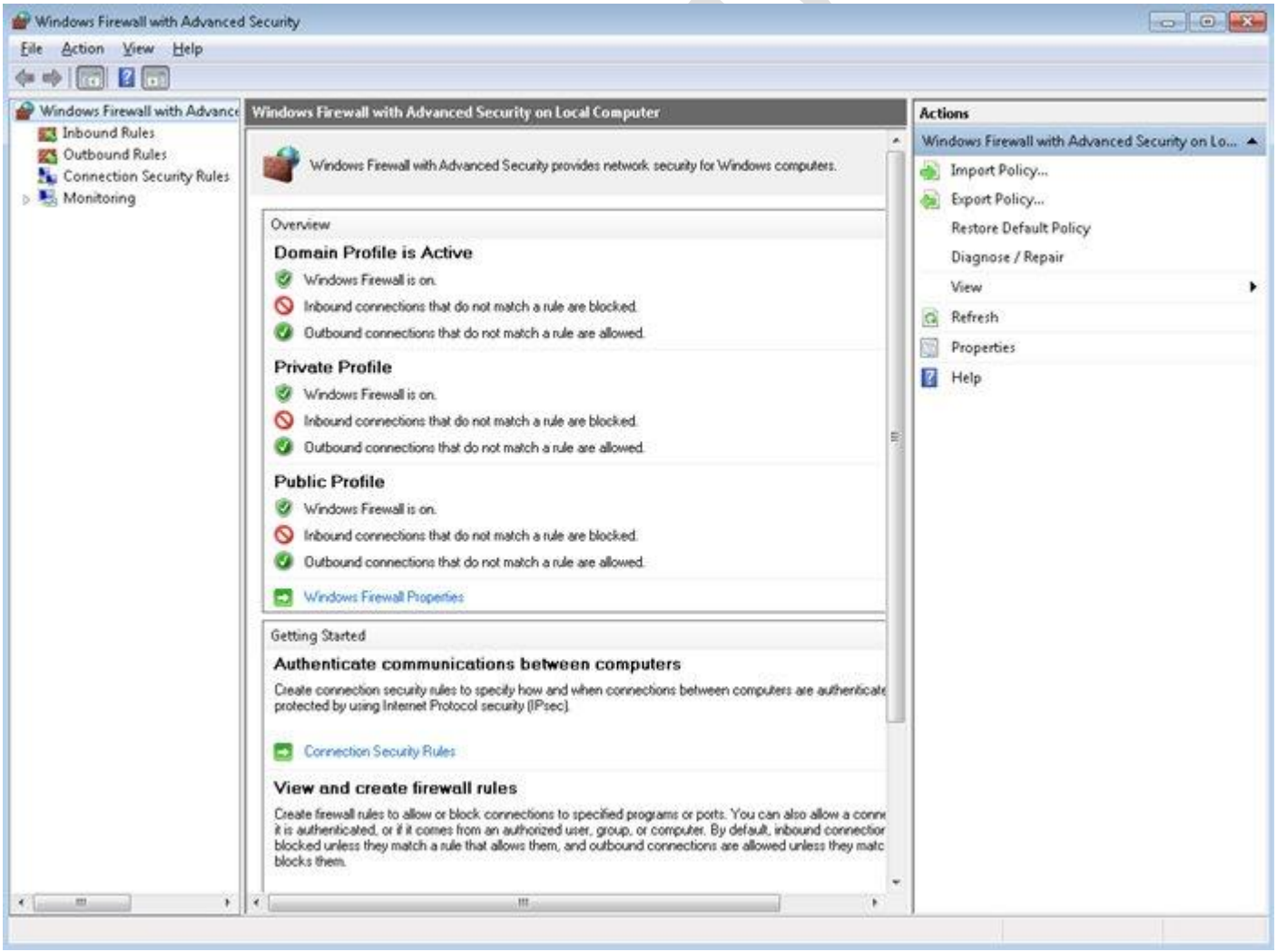
Introduction to Windows Firewall with Advanced Security:

Windows Firewall with Advanced Security is designed for advanced users and IT professionals, and offers more powerful configuration options than the standard Windows Firewall. You can now configure Inbound and Outbound Rules, Block or Allow incoming or outgoing connections based off Protocols and Ports and/or Programs and Services, and configure IPSec. The Inbound and Outbound Rules can be enforced on predefined profiles, Public, Private, Domain or all Profiles. WFAS becomes handy in instances where you need to enable a rule that allows traffic for a specific service while connected to one network profile, but not on another. For example, you

can allow FTP traffic for the Domain (Work) Profile but not for the Public Profile. This would mean that computers at your work place can connect to your computer hosting an FTP service, whereas such traffic is blocked when you're connected to another network.

The default Inbound rule settings is to block all connections that do not have rules (exceptions) that allow the connection unless the incoming request is a response from the client. The default Outbound rule is to allow all outbound connections unless you have explicitly blocked an outbound connection.

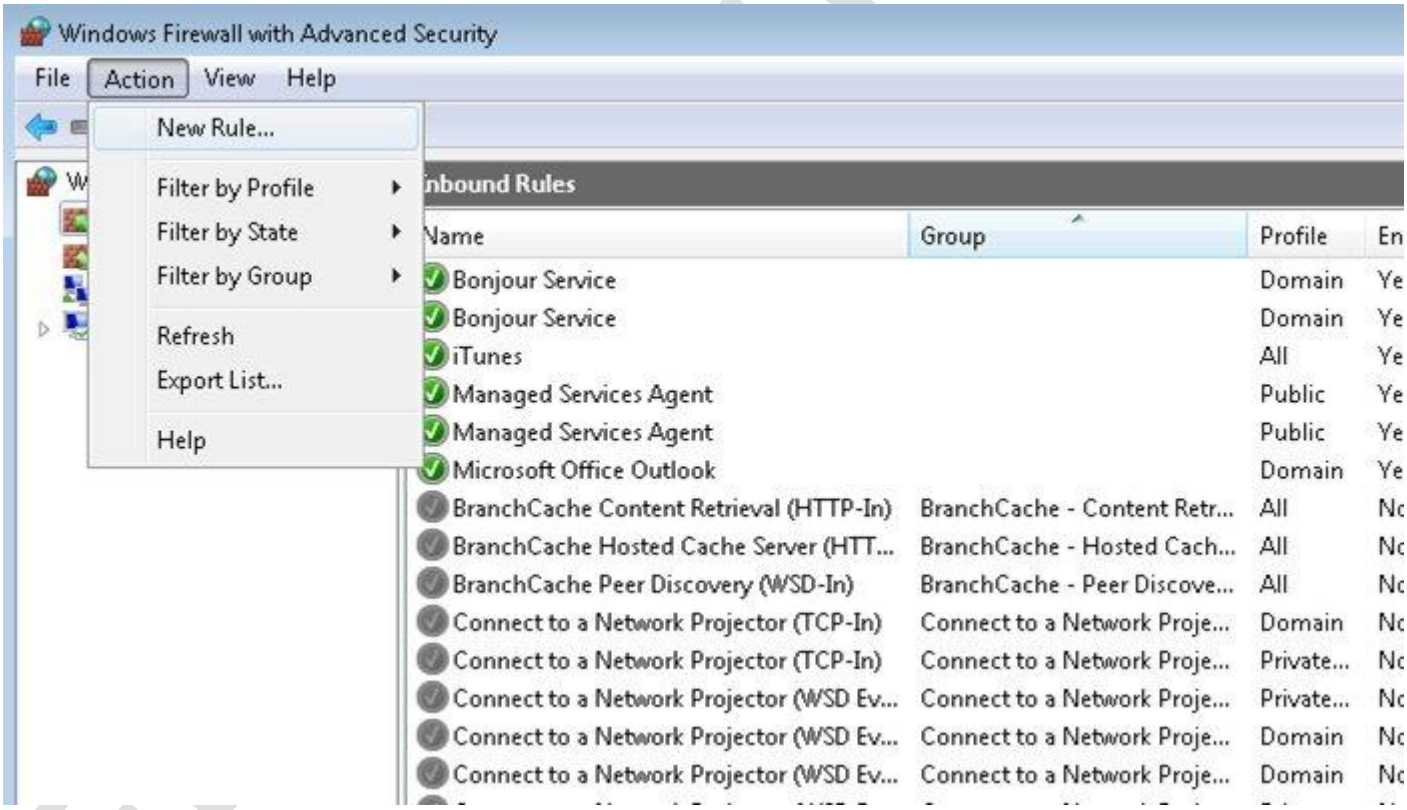
To access Windows Firewall with Advanced Security snap-in, open the Network and Sharing Center and click on *Advanced Settings* in the left pane. Or, you can type *Windows Firewall with Advanced Security* into the *Search Programs And Files* box in the Start menu. You must be a member of the administrators group.



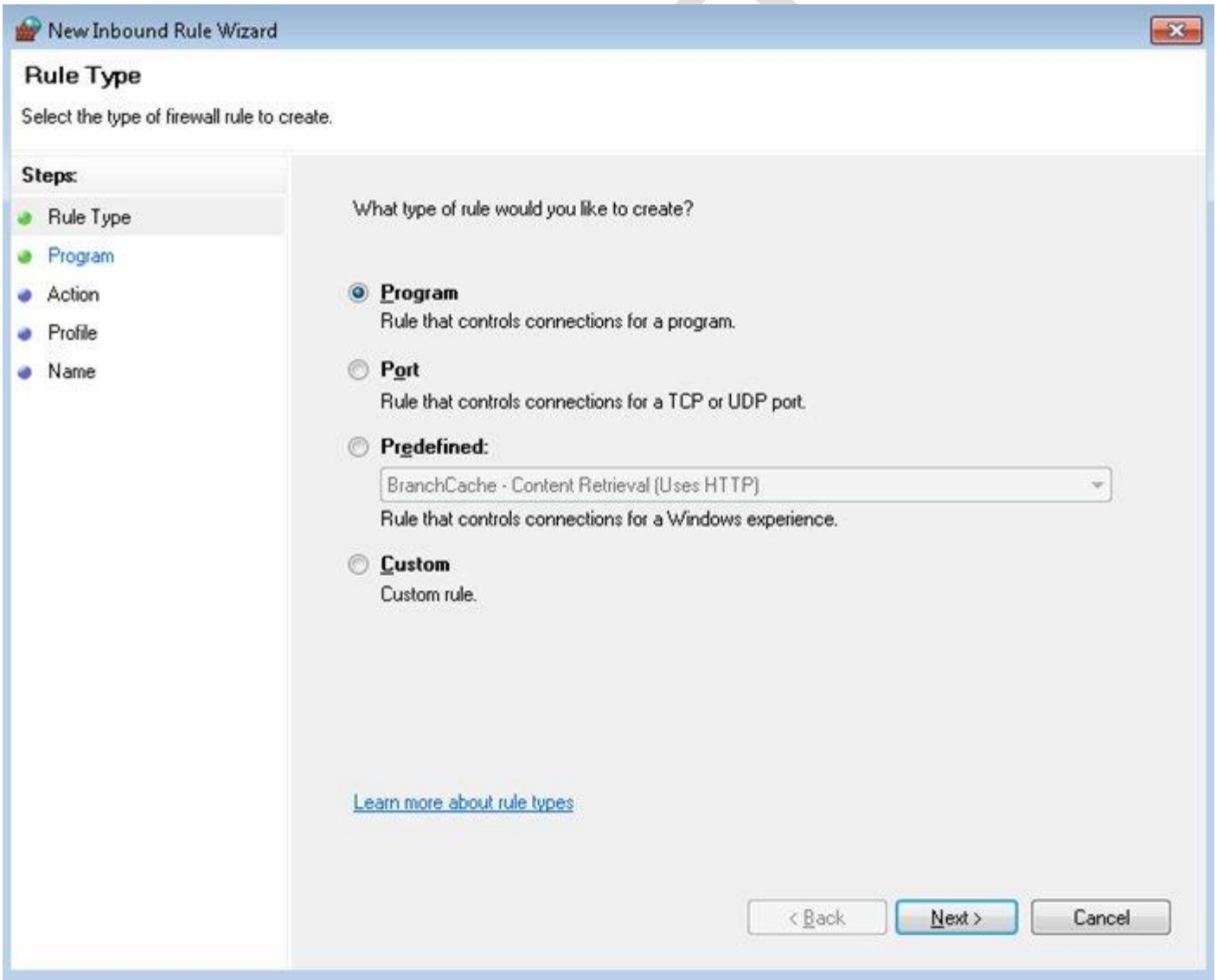
Creating Rules:

To create and inbound or outbound rule, follow these steps:

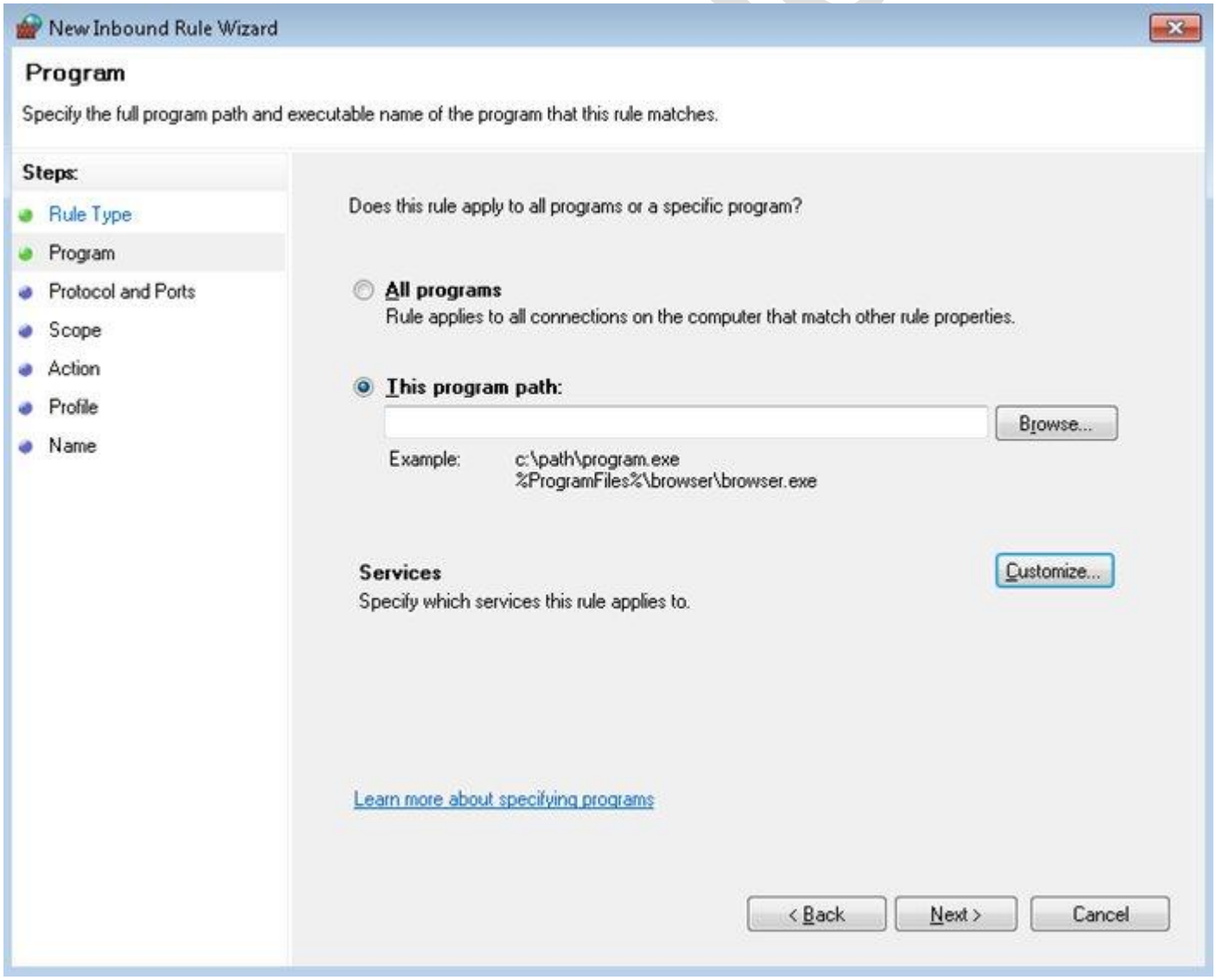
1. First click on *Inbound Rules* or *Outbound Rules* in the left pane depending on which type of rule you are trying to create. In this case, we selected Inbound Rules.
2. Click on the *Action* menu and select *New Rule*.



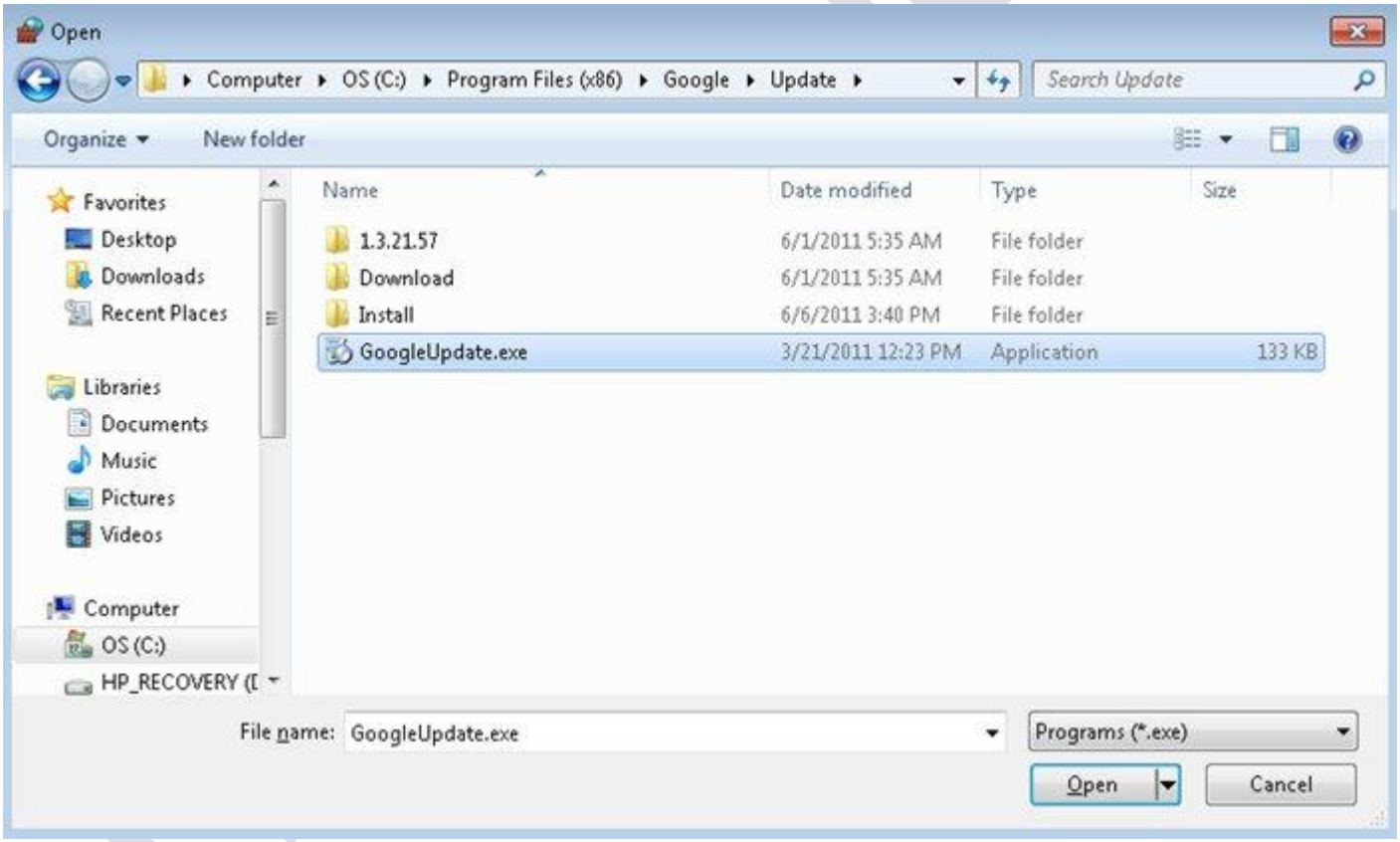
3. This brings up the New Inbound Rules Wizard. In this window you can define a rule based on a program, a port, a predefined service or feature, or multiple parameters (custom rule). The program and predefined rules are the same as those found in the standard Windows Firewall. The custom rule allows you to configure a rule based on more than one option, for example, a rule that involves a specific program and ports.



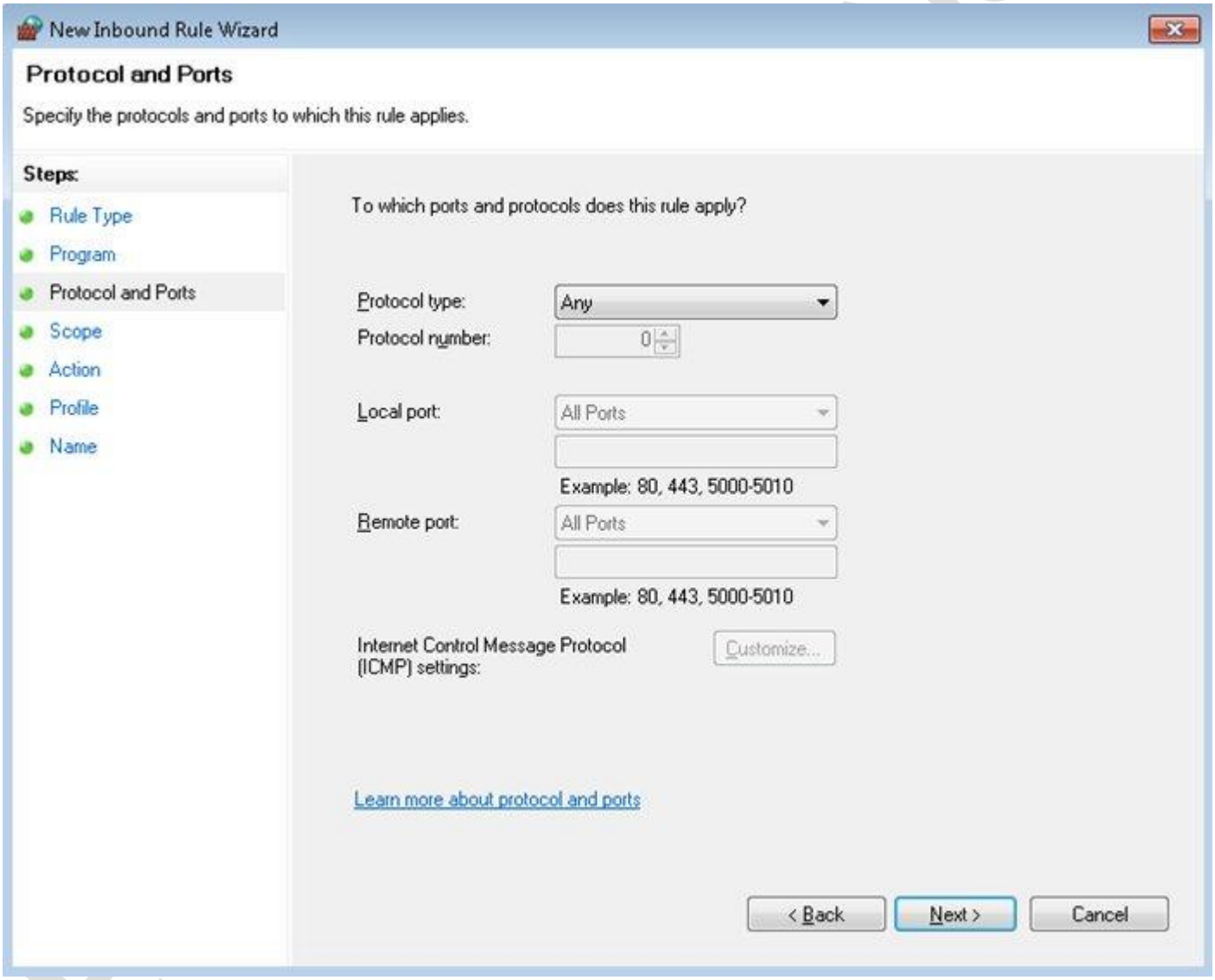
4. What happens from here depends on the type of rule you are going to create and we suggest that you familiarize yourself with all of them. In this case, we are going to create a custom rule.



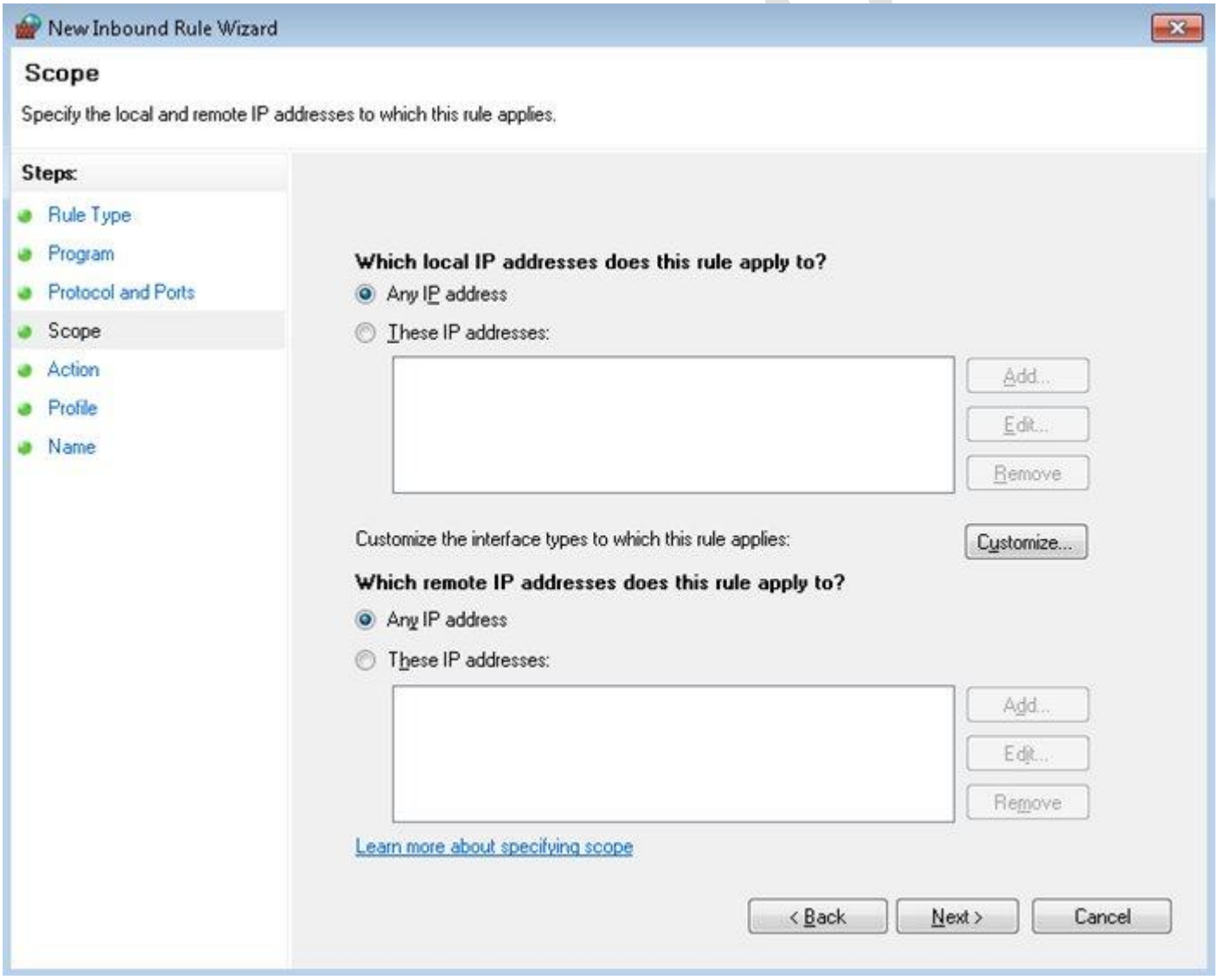
5. Here you can apply the rule to all programs, browse to a specific program, or a service. We're going to apply ours to a specific program by clicking the *Browse* and selecting a program.



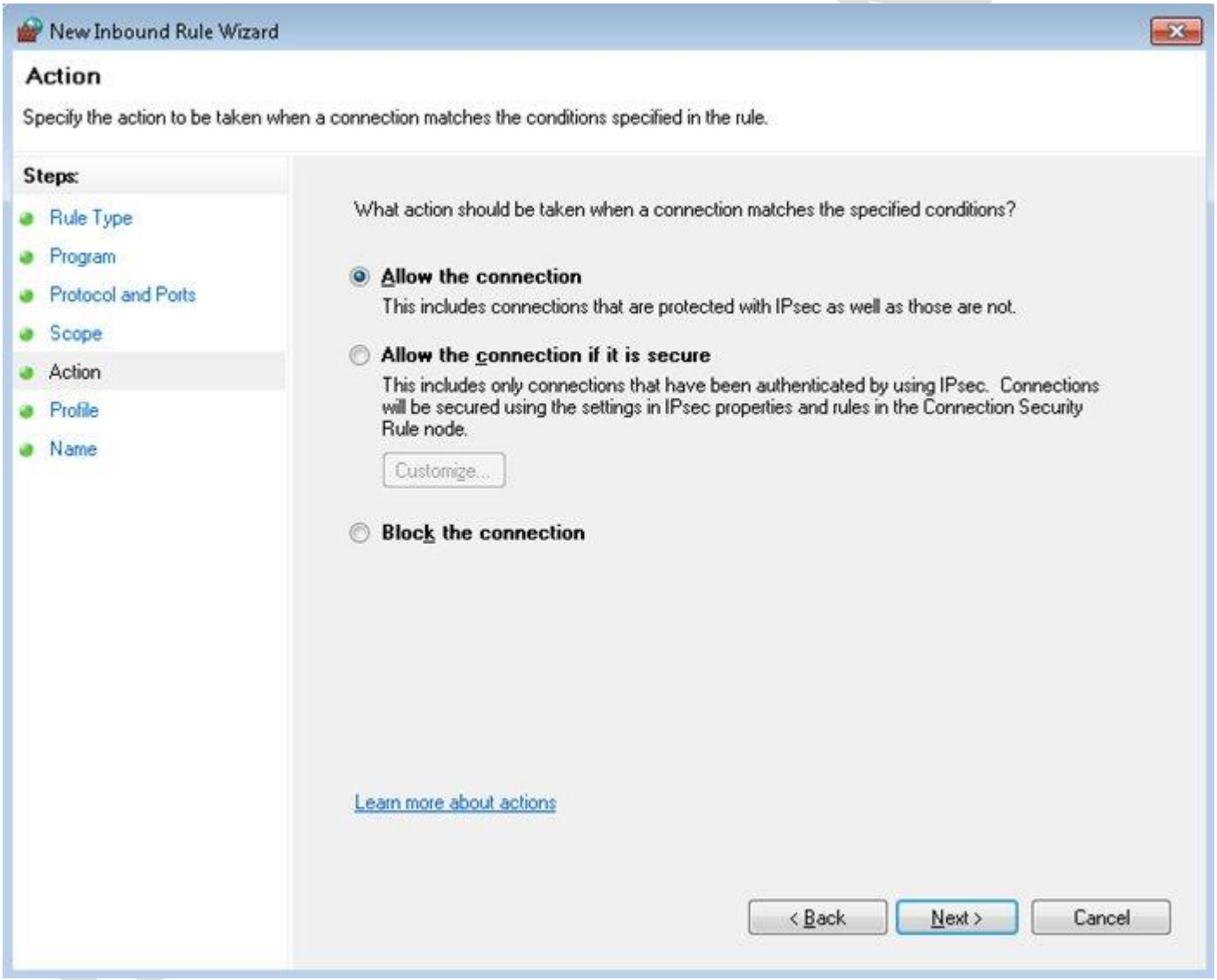
6. Here we can apply the rule to specific protocols and ports. We selected a TCP port.



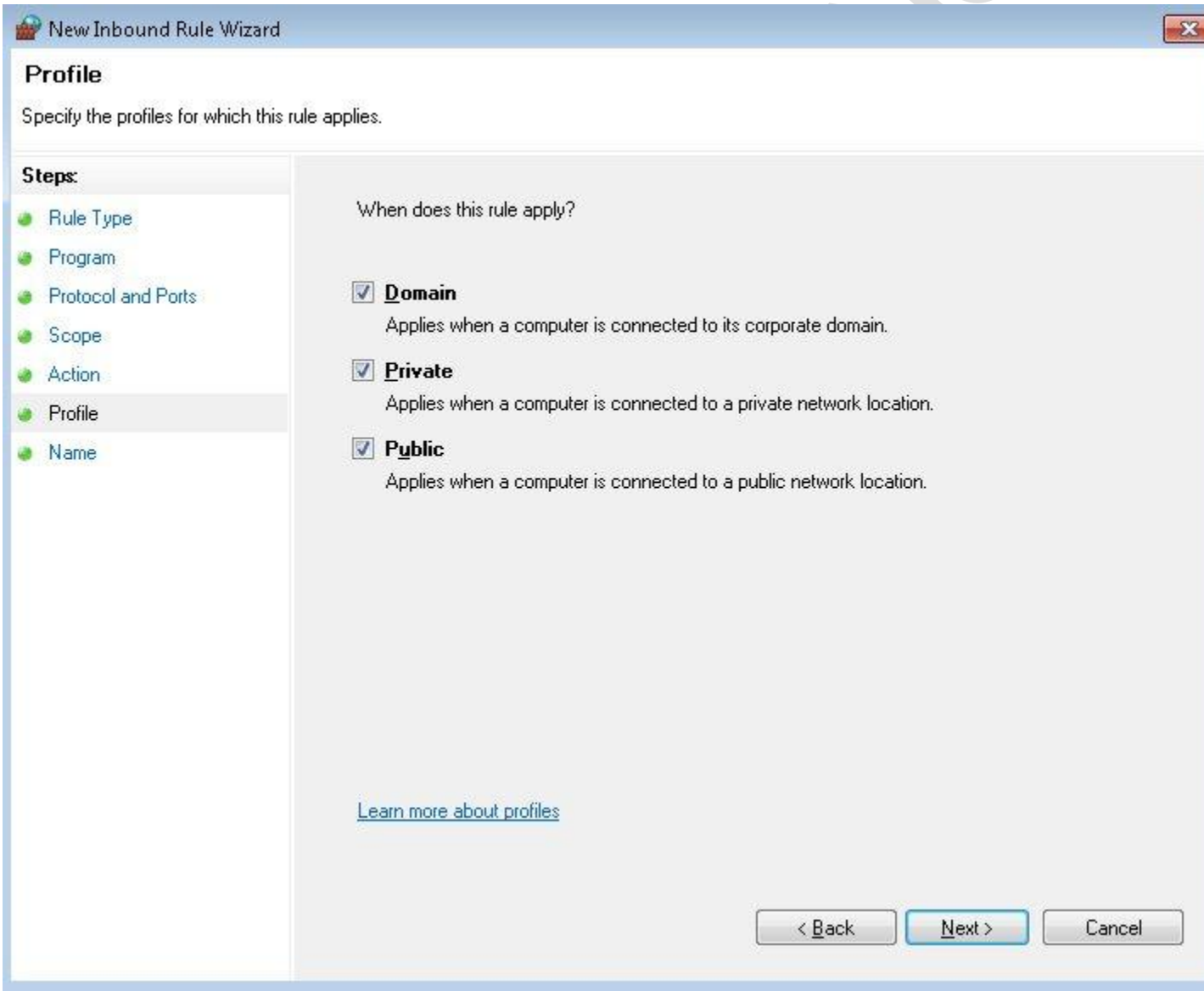
7. Next we define the scope of the rule. We have the option to configure local and remote addresses. The local IP address is used by the local computer to determine if the rule applies. The rule only applies to network traffic that goes through a network adapter that is configured to use one of the specified addresses. Specify the remote IP addresses to which the rule applies. Network traffic matches the rule if the destination IP address is one of the addresses in the list.



8. Next, we can allow the connection, allow the connection if it is secure, or block the connection.



9. Now we choose which network locations the rule will apply to.



10. In the final step, we enter a name and description for the rule and click *Finish*

The above instruction only demonstrate one of the possible types of rules you can create, and the dialogue boxes will vary depending on the type of rule and selections you make.

In addition to inbound and outbound rules, you can also configure Connection Security Rules. For more

information about this, read Understanding Connection Security Rules.

Import and Export:

WFAS allows you to import and export the current firewall configuration for the purpose of easy configuration on stand-alone computers. To roll out the firewall configuration on a company network, it is better to use group policy. The import and export feature also essentially enables you to make a backup copy of your configuration before you make changes to it. Exported policy files are binary with a .wfw extension.

70-680 Study Guide - Configure Remote Management

Introduction to Remote Desktop:

The Remote Desktop (RDP) utility allows you to connect to a computer on a network and access all of your programs, files, and network resources as if you were sitting in front of that computer. Remote desktop is often used by security professionals to administer servers, and fix problems on client computers without having to be in front of them. In fact, they could be in another country.

You cannot use Remote Desktop Connection to connect to computers running Windows 7 Starter, Windows 7 Home Basic, and Windows 7 Home Premium. In other words, only Windows 7 Professional, Ultimate, and Enterprise editions allow a computer to connect to them via RDP. All versions of Windows 7 have the Remote Desktop client software that allows them to make outgoing connections.

To use Remote Desktop and Remote Assistance, you have to use TCP port 3389. Therefore, it needs to be opened using the Windows Firewall and any other firewalls between your computer and the remote host. Additional requirements include:

- You must have permission to connect to the remote computer.
- The remote computer must be turned on or have Wake on LAN enabled.
- Both computers must be connected to a network.
- The remote computer must be configured to accept incoming connections (see next section). By default this is turned off.

Enabling Remote Desktop Connections:

Follow these steps to enable the remote desktop connection in Windows 7:

1. Click *Start*, then right-click the Computer and select *properties*.
2. Click the *Remote settings* option in the window.
3. Enable *Allow connections from computers running any version of Remote Desktop* in the System Properties dialogue box.
4. Click *Apply* and the remote desktop connections feature will be enabled on your Windows 7 computer.

Note: When you enable Remote Desktop, Windows Firewall automatically updates rules to allow Remote Desktop connections to be made to the computer. If you reset Windows Firewall to its default settings, the firewall will no longer allow connections. Simply disable and then re-enable Remote Desktop to correct this problem.

Establishing a Remote Desktop Connection:

1. Click *Start* and then click *All Programs* and then click *Accessories*.
2. Click the *Remote Desktop Connection* option. The Remote Desktop dialogue box is displayed; specify the IP address or hostname of the remote machine to which you want to connect.
3. Click *Connect* and if the computer is running and remote connections are enabled on it, a connection will be made.
4. Enter the the username and password for that computer.

If a user other than yourself is logged into the remote machine, they will be presented with an alert that someone is trying to establish a remote desktop connection with the computer. They can choose to accept the connection or not.

Configuring Remote Desktop:

To configure remote access, follow these steps:

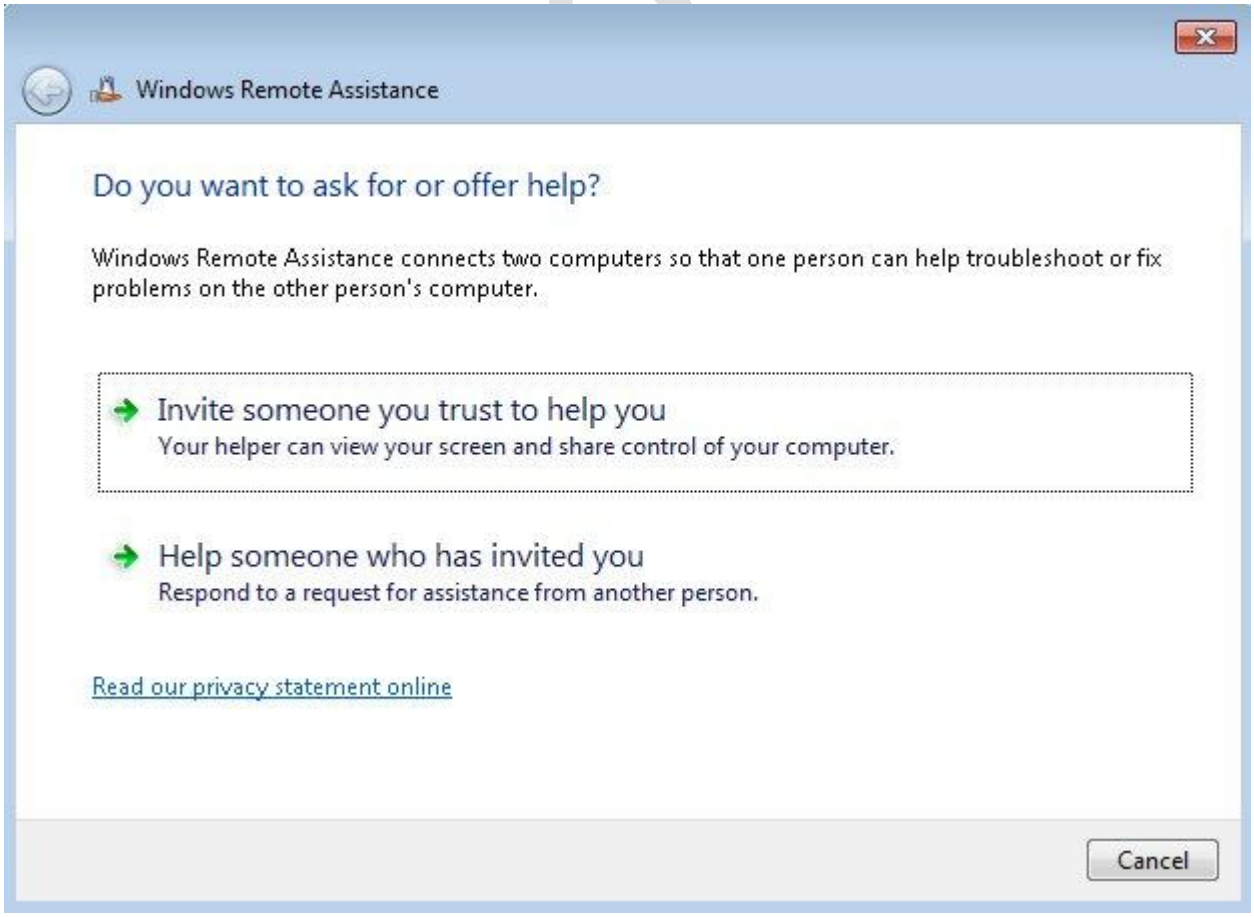
1. In the Control Panel, first click *System And Security*, and then click *System*.
2. Click *Remote Settings* in the left pane and the System Properties dialog box to the Remote tab opens.
3. If you want to disable the Remote Desktop, select *Don't Allow Connections To This Computer*, then click *OK* and skip the remaining steps.
4. To enable Remote Desktop, choose either of the two options:
    - Select *Allow Connections From Computers Running Any Version Of Remote Desktop*. This allows connections from any version of Windows.
    - Select *Allow Connections Only From Computers Running Remote Desktop With Network Level Authentication*. This allows connections only from Windows 7 or later computers and computers with secure network authentication.
5. Click *Select Users* to open the Remote Desktop Users dialog box. To grant Remote Desktop access to any user, click *Add*. This opens the *Select Users* dialog box. In the Select Users dialog box, click *Locations* to select the computer or domain in which the users are located with whom you want to work. Type the name of a user and enter the object names to the selected fields, and then click *Check Names*. If matches are found, then you can select the account you want to use and then click *OK*. If no matches are found, update the name you entered and search again.
6. To revoke remote access permissions for any user account, select the account and then click *Remove*.
7. Click *OK* when you have finished.

Remote Assistance:

Since Windows XP, Remote Assistance has provided a handy way to get or give a helping hand from a distance. The main difference between Remote Desktop and Remote Assistance is that with Remote Assistance, the remote user must request a connection, and when connected, both the local user and the remote user can see what is happening on the screen at the same time. Windows Remote Assistance is enabled by default on computers running Windows 7.

In previous versions of Windows, the primary way to initiate a Remote Assistance connection was by creating an "invitation" file with info on how to find and connect to your system, and sending it the person you are requesting help from via e-mail. You can still use invitation files in Windows 7, and if your helper is running Vista or XP, you'll have to. However, if both parties have Windows 7, a new feature called Easy Connect can simplify the connection process by eliminating e-mail as a middleman.

To request remote assistance in Windows 7, search for *assistance* from the Start menu, then click *Windows Remote Assistance*.



After you click *Invite someone you trust to help you*, you'll see *Easy Connect* along with the two e-mail-based invitation options. Choose *Easy Connect*, and then you should see a Windows Remote Assistance window displaying the 12-character password needed for access to your computer. This automatic password generation is another new Windows 7 feature, and it occurs whether you use Easy Connect or invitations. It forces you to use a strong password to increase security over that in Vista or XP.

If Easy Connect is grayed out, one of the following reasons may be the cause.

- Both computers aren't running Windows 7. In order to use Easy Connect with Remote Assistance, both of the computers must be running Windows 7.
- Access to the Internet is limited. If access to the Internet is limited on either computer, Easy Connect is disabled. Internet access might be limited if you're on a corporate network.
- Your router doesn't support Easy Connect. Easy Connect uses the Peer Name Resolution Protocol (PNRP) to transfer the Remote Assistance invitation over the Internet. One possible issue is that your router doesn't support UPnP, or doesn't have it enabled. You may also want to try enabling port 3540 (UDP) on your router. You can check your router by using the Internet Connectivity Evaluation Tool on the Microsoft website. If you're running Windows Server, you need to install the Peer Name Resolution Protocol.

Once connected and with the remote user's permission, you can "remote control" their computer like you would with Remote Desktop, only the user will be able to see what you are doing.

After you've successfully established a Remote Assistance session with someone via Easy Connect, connecting to that person in the future will be even easier. The next time you run Remote Assistance you'll see a list of people you've previously connected to. Select a name and the Windows Remote Assistance window will launch, and when your helper connects to you, you'll be connected without having to see or enter a password because the one from your last session is cached. This subsequent connect feature only works when the helper is using the same computer they were on initially.

Windows Remote Management Service:

The Windows Remote Management service allows you to execute commands on a remote computer, either from the command prompt using WinRS or from Windows PowerShell. Before you can use WinRS or Windows PowerShell for remote management tasks, it is necessary to configure the target computer using the WinRM command. To configure the target computer, run the command *WinRM quickconfig* from a command prompt.

You can use Windows Remote Management service (WinRS) to execute command-line utilities or scripts on a remote computer. To use WinRS, open a command prompt and prefix the command that you want to run on the remote computer with the *WinRS –r:[RemoteComputerName]* command. For example, to execute the Ipconfig command on a computer named *Naomi*, issue the command:

WinRS –r:Naomi ipconfig

If the computer is on the local network, you can use its NetBIOS name. If the computer is on a remote network, you may need to specify its fully qualified domain name (FQDN). It is also possible to specify credentials to be used on the remote computer, for example, to run the command net accounts, which displays information about a computer's password policy on a computer named Naomi.7-seconds.pdxoffice using the *NaomiS* user account,

issue the following command:

WinRS –r:http://Naomi.7-seconds.pdxoffice –u:NaomiS net accounts

If you do not specify a password using the –p:password option, you are prompted to enter a password after you execute the command. You can configure WinRS options through Group Policy in the *Computer Configuration\Administrative Templates\Windows Components\Windows Remote Shell* node.

PowerShell:

Windows PowerShell utilities give you the ability to remotely configure and administer a Windows 7 machine. Windows PowerShell is a command-line scripting utility that allows you to remotely execute commands on a Windows 7 machine. Windows PowerShell is a command line utility that was specifically designed for system administrators to allow for remote administration. One of the advantages of Windows PowerShell is that it introduced the concept of a cmdlet. A cmdlet is a command that is built into Windows PowerShell. There are more than 100 built-in cmdlets, and you can build your own cmdlets and allow others to use them as well.

Another advantage of Windows PowerShell is that it allows you to gain access to a file system on a computer. Windows PowerShell also allows you to access the Registry, digital certificate stores, and other data stores.

The following features are new with PowerShell in Windows 7:

- **New cmdlets** - Windows PowerShell includes over 100 new cmdlets, like Get-Hotfix, Send-MailMessage, Get-ComputerRestorePoint, New-WebServiceProxy, Debug-Process, Add-Computer, Rename-Computer, Reset-ComputerMachinePassword, and Get-Random.
- **Remote management** - You can run commands on one computer or more computers with a single command. You can establish an interactive session with a single computer, and computers can receive remote commands from multiple computers.
- **PowerShell Integrated Scripting Environment (ISE)** - Windows PowerShell ISE is a graphical user interface for Windows PowerShell with which you can run commands, and write, edit, run, test, and debug scripts in the same window. It offers eight independent execution environments and includes a inbuilt debugger, multiline editing, selective execution, syntax colors, line and column numbers, and context-sensitive Help.
- **Background jobs** - With Windows PowerShell background jobs, you can run commands asynchronously in the background and can continue to work in your session. You can run background jobs on a local or remote computer, and can store the results locally or remotely.
- **Debugger** - The Windows PowerShell debugger can help you to debug functions and scripts. You can step through code , set and remove breakpoints, check the values of variables, and display a call-stack trace.
- **Modules** - Windows PowerShell modules allow you to organize your Windows PowerShell scripts and functions into independent, self-contained units. You can package your cmdlets, scripts, functions, and other files into modules that can be distributed to other users. Modules are easier to install and use as compared to Windows PowerShell snap-ins. Modules can include any type of file, like audio files, images, Help files, and icons. Modules run in a separate session so as to avoid name conflicts.
- **Transactions** - Windows PowerShell now also supports transactions, through which you can manage a set of commands as a logical unit. A transaction can be committed, or it can be completely undone to undo the changes and the affected data is not changed by the transaction.
- **Events** Windows PowerShell includes a new event infrastructure with which you can create events, subscribe to system and application events, then you can listen, forward, and act on the events synchronously and asynchronously.

- **The Advanced functions** - Advanced functions are similar to cmdlets, but they are written in the Windows PowerShell scripting language instead of in C#.
- **Script internationalization** - Scripts and functions display messages and Help text to users in various languages.

Using Windows PowerShell:

1. Click *Start*, then click *All Programs* and then click *Accessories*.
2. Click *Windows PowerShell* and then again click *Windows PowerShell* to access it. Windows PowerShell Integrated Scripting Environment (ISE) is a new host application which allows you to run commands and write, test, and debug scripts in a friendly, syntax-colored. It can be accesses by clicking *Windows PowerShell ISE*.
3. When the Windows PowerShell utility starts, type *Help* and press *Enter*. This will show you the Windows PowerShell syntax and some of the commands included with Windows PowerShell. You can type *Help* * at the Windows command prompt. This will show you all of the cmdlet commands that you can use.

Following are few Windows PowerShellcmdlets:

Clear-History	Deletes entries from the command history
Invoke-command	Runs commands on local or remote computers
Start-job	Starts a Windows PowerShell background job
Stop-job	Stops a Windows PowerShell background job
Remove-job	Deletes a Windows PowerShell background job
Import-Module	Adds modules to the current session
Receive-job	Gets the results of a Windows PowerShell background job
Format-table	Shows the results in a table format
Out-file	Sends the job results to a file
Get-Date	Gets the date and time
Set-Date	Sets the system time and date on a computer

Get-event	Gets an event in the event queue
New-event	Creates a new event
Trace-command	Configures and starts a trace of a command on a machine.

70-680 Study Guide - Configure Shared Resources

Introduction:

Historically, when it came to Windows networks, there were 2 basic types to consider. Company networks typically have a server and a domain environment, while small office and home networks use a peer-to-peer type network called a workgroup in Windows. Windows 7 adds Homegroups to make workgroup sharing easier. Let's look at a description of each type:

- **Workgroups**
  - All computers are peers which means no computer has control over another computer.
  - Each computer has a set of user accounts. To log on to any computer in the workgroup, you must have an account on that computer, or know the username and password of an account on that computer.
  - There are typically no more than twenty computers. 10 or less is ideal.
  - A workgroup is not protected by a password.
  - All computers must be on the same local network or subnet.
  - Management of user accounts, securing resources, and providing access to shared resources is very difficult with workgroups.
- **Homegroups**
  - Computers on a home or small office network must belong to a workgroup, but they can also belong to a homegroup. A homegroup makes it easier to share documents and printers with peers.
  - A homegroup is protected with a password, but you only need to type the password once when adding a computer to the homegroup.
- **Domains**
  - Must have at least 1 server. Network administrators use servers to control the security and permissions for all computers on the domain. Domain users must provide a password or other credentials each time they access the domain.
  - If you have a user account on the domain, you can log on to any computer on the domain without needing a local account on that computer.

- There can be thousands of client computers in a domain.
- The computers can be on different local networks.
- Domain users can join an existing Homegroup, but cannot create one.

When setting up your computer on a network in the Network and Sharing Center, you will choose whether your computer is part of a workgroup or a domain. Homegroups are configured here after joining a network.

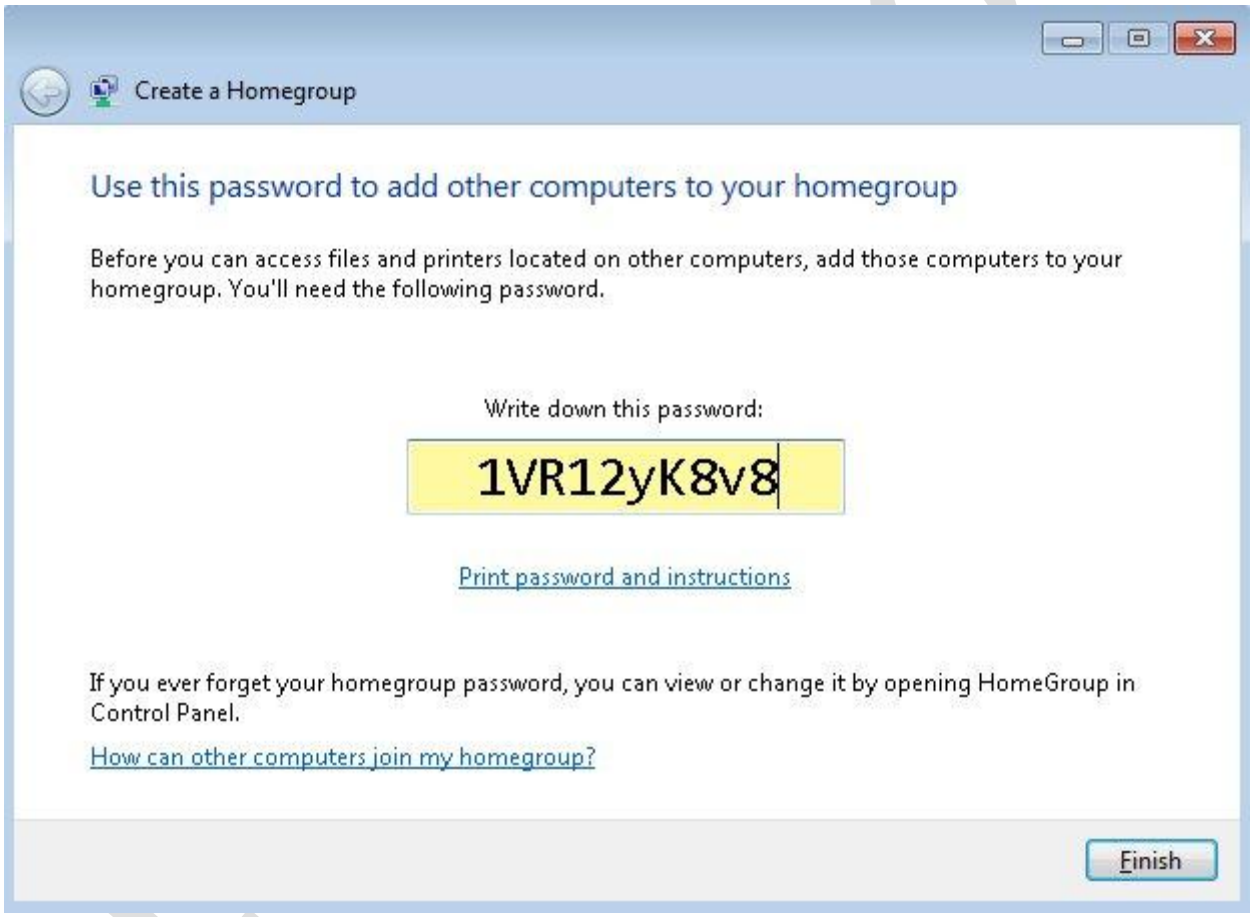
Homegroups:

HomeGroup is a feature of Windows 7, and Home Premium or better is required to create a HomeGroup, however, all versions of Windows 7 can join one. To create a Homegroup, follow these steps:

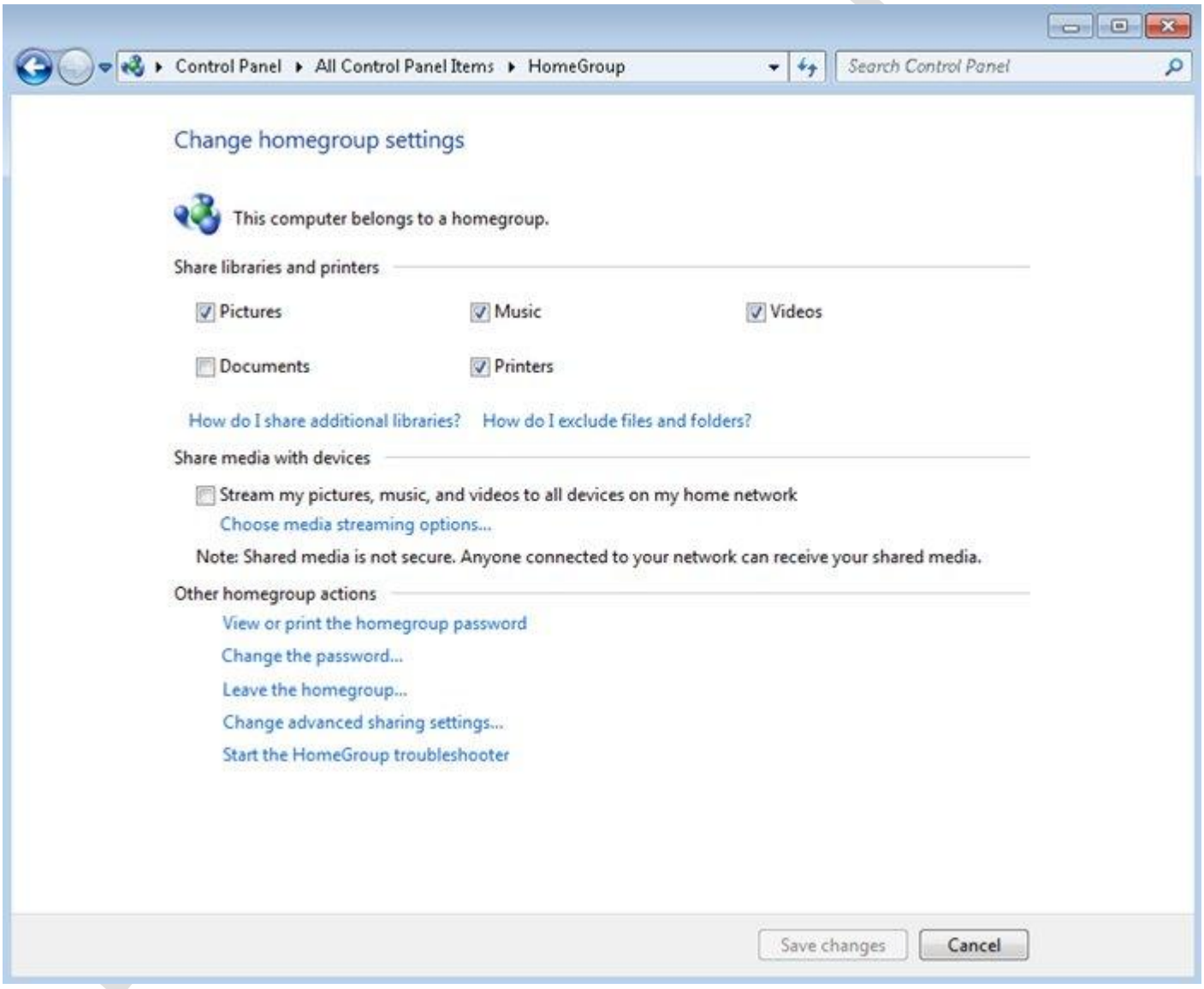
1. From the Network and Sharing Center, click *Choose homegroup and sharing options*.

2. Click *Create a homegroup*. Select the items you wish to share and click *Next*.

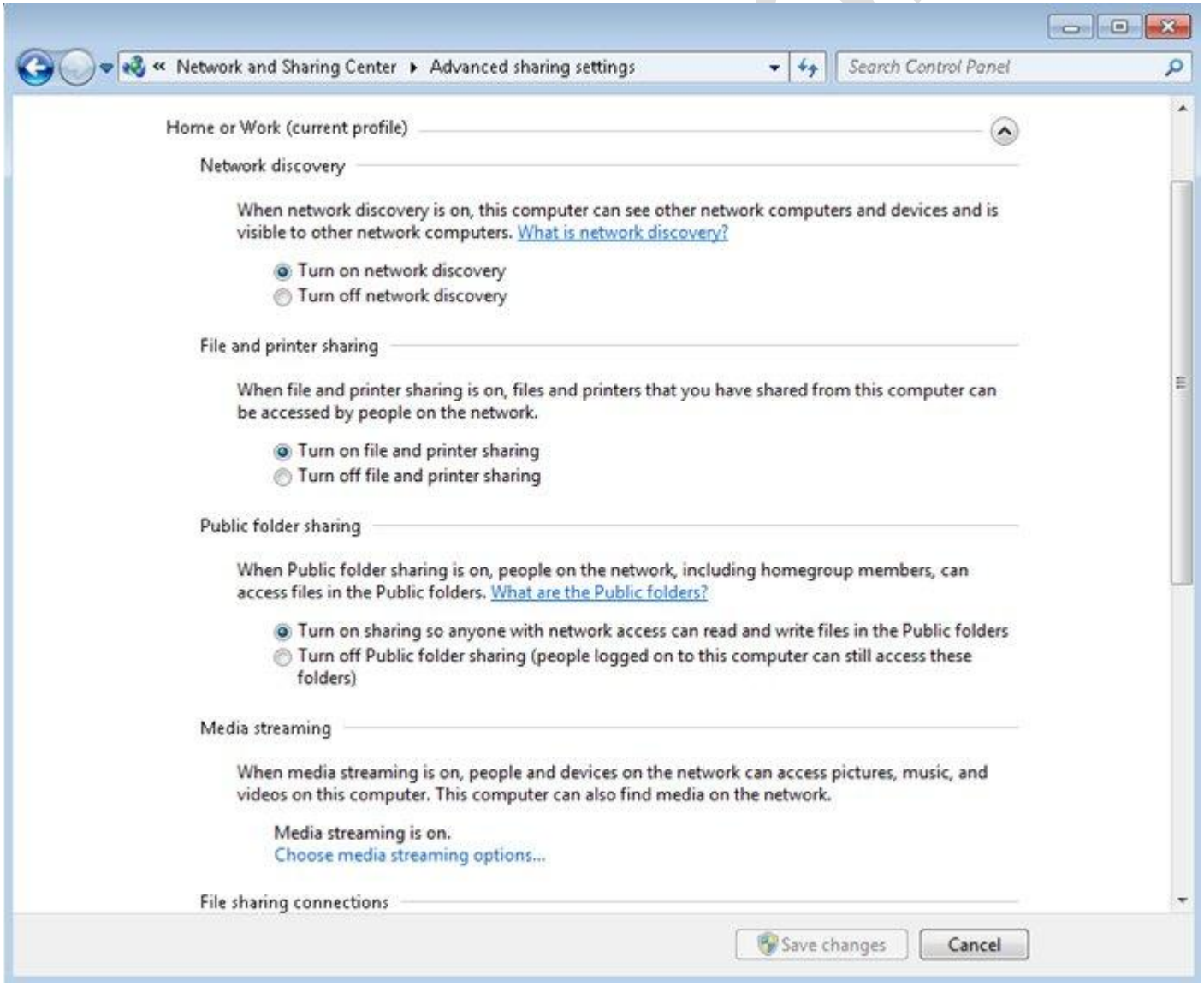
3. On the next screen, Windows will assign a password to your homegroup which can be changed later. Write down the password which will be needed by others whom you want to allow access to your group. Click *Finish*.



4. After completing the wizard, you will see the *Change homegroup settings* window. Here you can change the types of files that are shared, change the password, allow streaming of shared media, leave the homegroup, and modify advanced settings.



5. Clicking on *Change advanced sharing settings* will bring up the screen below. Here you can customize sharing settings for each network profile. This screen can also be reached by clicking on the *Change advanced sharing settings* link in the left pane of the Network and Sharing Center.



Joining a homegroup is simple. From the Network and Sharing Center, click on the *Homegroup* link in the lower left pane. On the next screen, any available homegroups on your networks will show and you can click the *join now* button. You must have the homegroup's password to join and your computer's network location must be set to Home.

In some cases, you might want to prevent access to certain files or folders within your shared Libraries or share folders outside of your Libraries. To do that, right-click the folder, and then do one of the following:

- To share the folder with nobody, click Share with, and then click *Nobody*.
- To share the file or folder with specific people, click *Share with* in the toolbar, click *Specific people*, select each person with whom you want to share with the file or folder, and then click *Add*. Click *Share* to close the File Sharing dialog box. Sharing with specific people only works if they've linked their profiles to an online ID.
- To share the file or folder with the entire homegroup, click *Share with* in the toolbar, and then click either *HomeGroup (Read)* or *HomeGroup (Read/Write)*.

Shared Folders:

Shared folders allow you to share data stored on your computer with other users on your network. You can share individual folders by right-clicking the folder you wish to share, choosing *Properties*, and then clicking the *Share* tab of the folder's properties.

This window provides two different sharing options: Share and Advanced Sharing. You can use shared folders when you cannot use HomeGroups, such as when you want to share resources on a Work network.

Clicking *Share* brings up the File Sharing dialogue box. You can use this window to set share permissions for local user accounts, the Everyone group, or the HomeGroup.

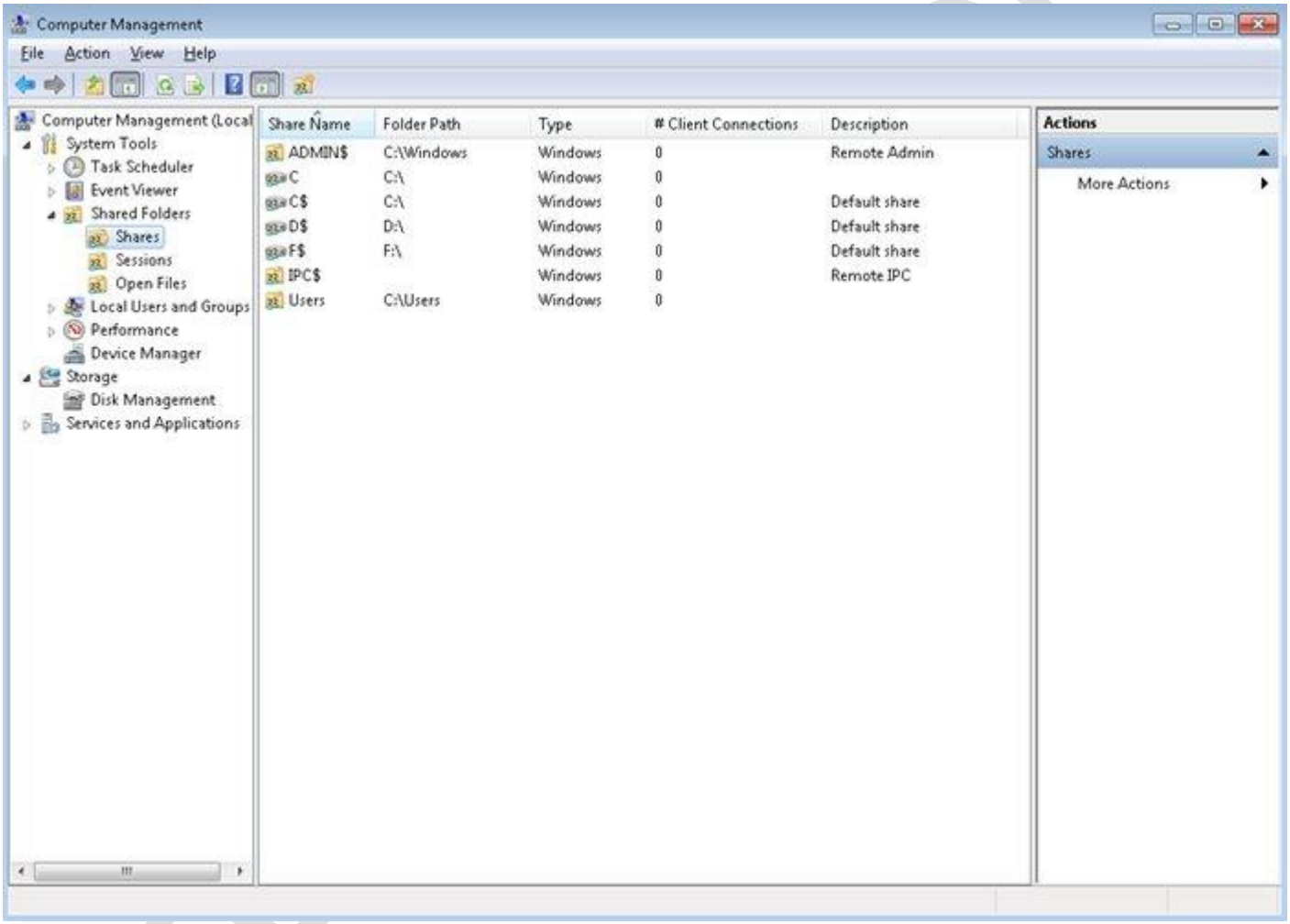
If you click *Advanced Sharing*, you can specify the name of the shared folder. A shared folder can be shared several times with different share names and permissions. To configure the permissions for the Shared folder, click the *Permissions* button.

But before you can configure the permissions, you must first understand how they work. This will be covered in the "Configure file and folder access" section of the guide.

Managing Shares:

You can manage all shared folders on a client running Windows 7 centrally using the Shared Folders node of the Computer Management console. The Shares node, shown below, displays all shared folders on the computer. The Sessions node provides details on which remote users currently are connected to shared folders, where they are connecting from and how long they have been connected. The Open Files node displays the folders and files

that remote users are accessing. You can edit the properties of an existing share by right-clicking it within this console and selecting *properties*. You can create a shared folder by right-clicking the Shares node and then clicking *New Share*. This starts the Create a Shared Folder Wizard.

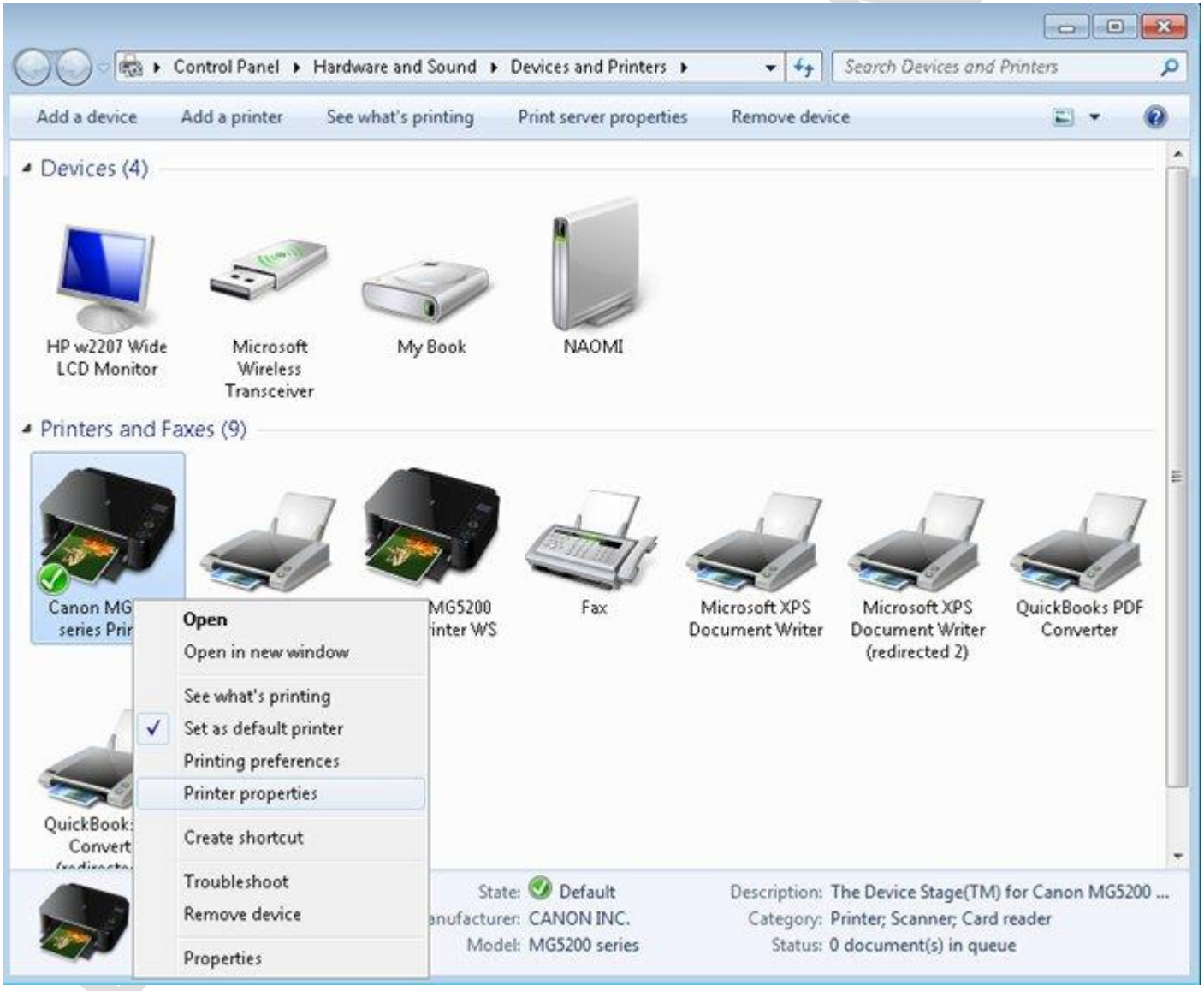


Sharing Printers:

You can connect a print device (printer, plotter, copy machine, or similar device) directly to your Windows 7 computer such as with a USB connection, or indirectly through a network. You can then print to the printer from the locally connected computer, or you can share the printer so that other users and network applications can print to the printer over the network. When setting up the printer, you will add either a local printer or a network printer depending on which of the scenarios above applies.

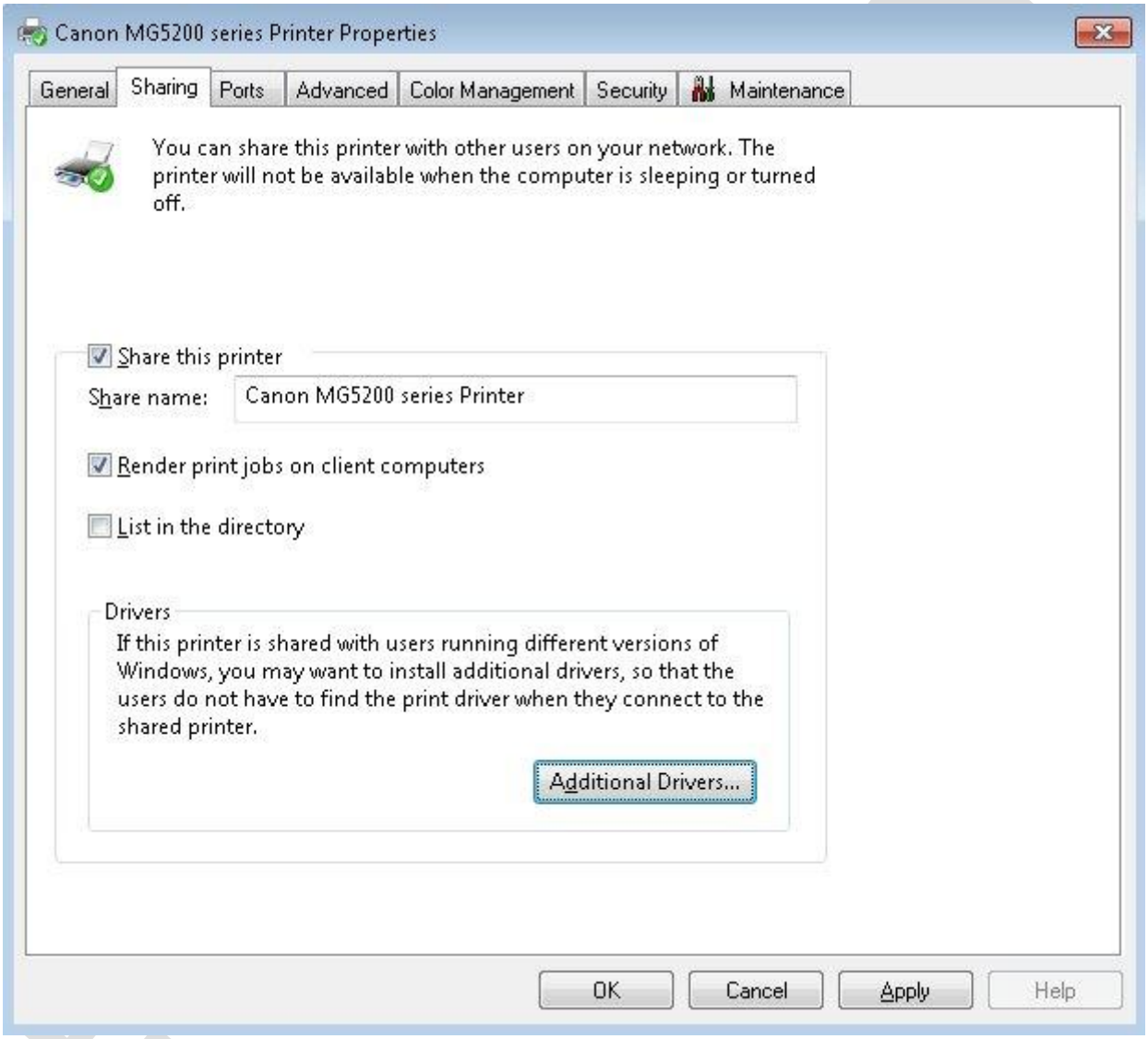
If you wish to share a printer, follow these steps:

1. Click *Start* and select *Devices and Printers*.
2. Right click on the printer you wish to share and select *Printer Properties*.

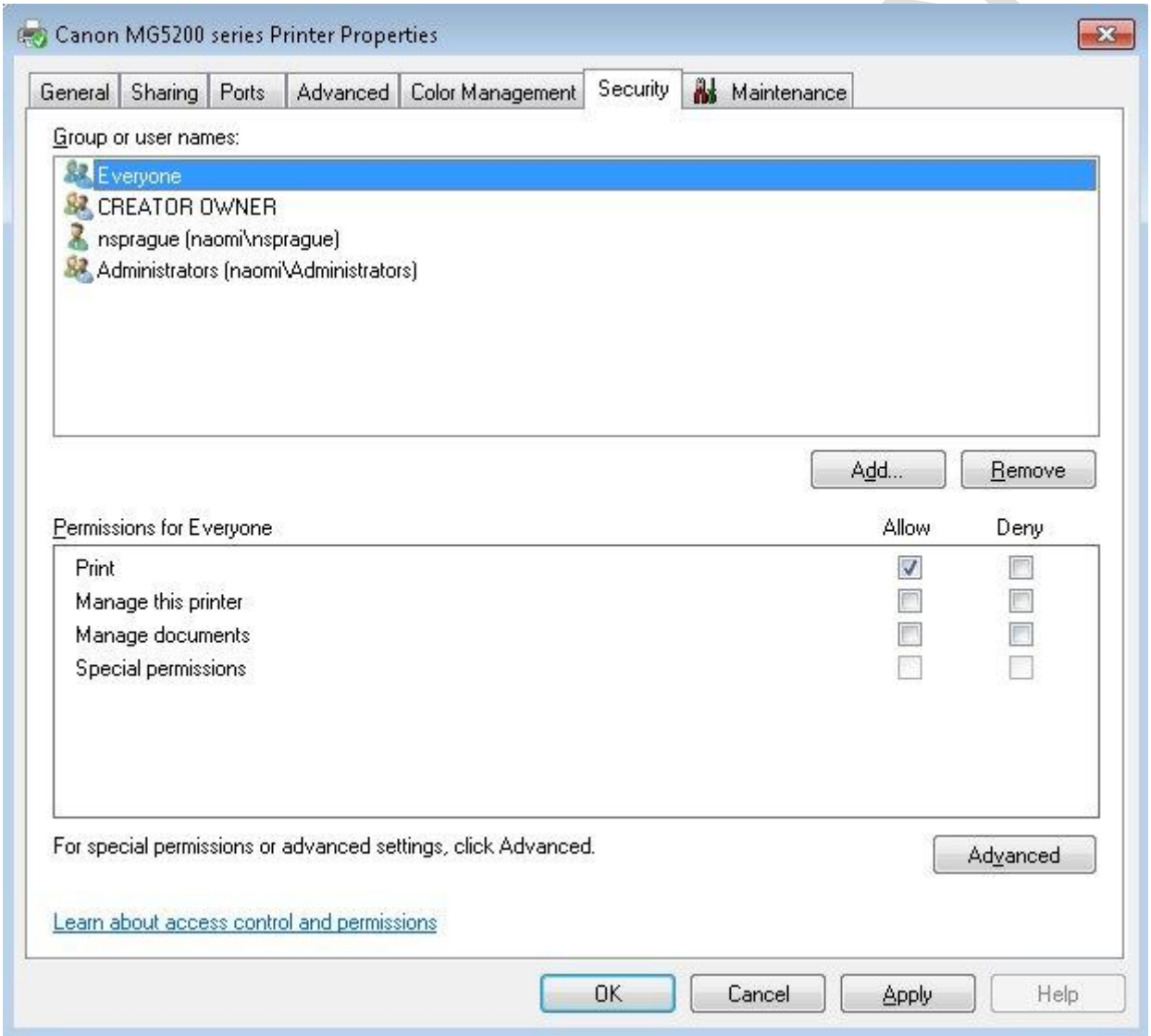


3. Next, click on the *Sharing* tab and check the *Share this Printer* checkbox. You can name the share so that others can easily find it. If you are in a domain environment, you can also publish the printer in Active Directory if you choose the *List in the directory* option. Click on the *Additional Drivers* button to see which drivers are installed. If the users who will be connecting to this printer are using a different operating system, you can check the box next to the driver for their OS so they do not have to find and install the driver when they connect. If the driver does not show here, you can download additional

drivers from the manufacturer or get them off the installation disk that came with the printer.



4. To set permissions for the printer, click on the *Security* tab.



When you share a printer, the Everyone group is assigned the Print permission by default, as shown in Figure 8-16. This means that all members of the HomeGroup or any user that is a member of the domain in a domain environment can send print jobs to the printer. If several people use the printer, you may wish to assign one of the other available permissions to allow better printer management. The available permissions are:

- **Print** - This permission allows a user to print to the printer and rearrange their own documents that have been submitted to the printer.

- **Manage This Printer** - Users with this permission can pause and restart the printer, change spooler settings, adjust printer permissions, change printer properties, and share a printer.
- **Manage Documents** - This permission allows users or groups to pause, resume, restart, cancel, or reorder the documents submitted by users that are currently in the print queue.

You can connect to a shared printer by going to the *Devices and Printers* control panel and clicking *Add a Printer*. Select *Add a network, wireless or Bluetooth printer*. A window comes up showing the available printers on the network. Note that if the printer or the computer it is connected to is turned off or sleeping, the printer will not show in the list. If the printer you wish to connect to is not on the list, click *The printer I want isn't listed*. Here you can browse the network for the printer, enter the share name and path to connect, or enter an IP address or hostname if you have that information.

Note that printers can also be shared using Homegroups.

70-680 Study Guide - Configure File and Folder Access

Encrypting File System (EFS):

Windows 7 includes the encrypting file system (EFS), which allows users to encrypt and decrypt files that are stored on an NTFS volume. This technology is only available in the Professional, Enterprise, and Ultimate editions of Windows 7. By using EFS, folders and files are kept secure against intruders who might gain unauthorized physical access to the device, for example, by stealing a computer or a removable drive.

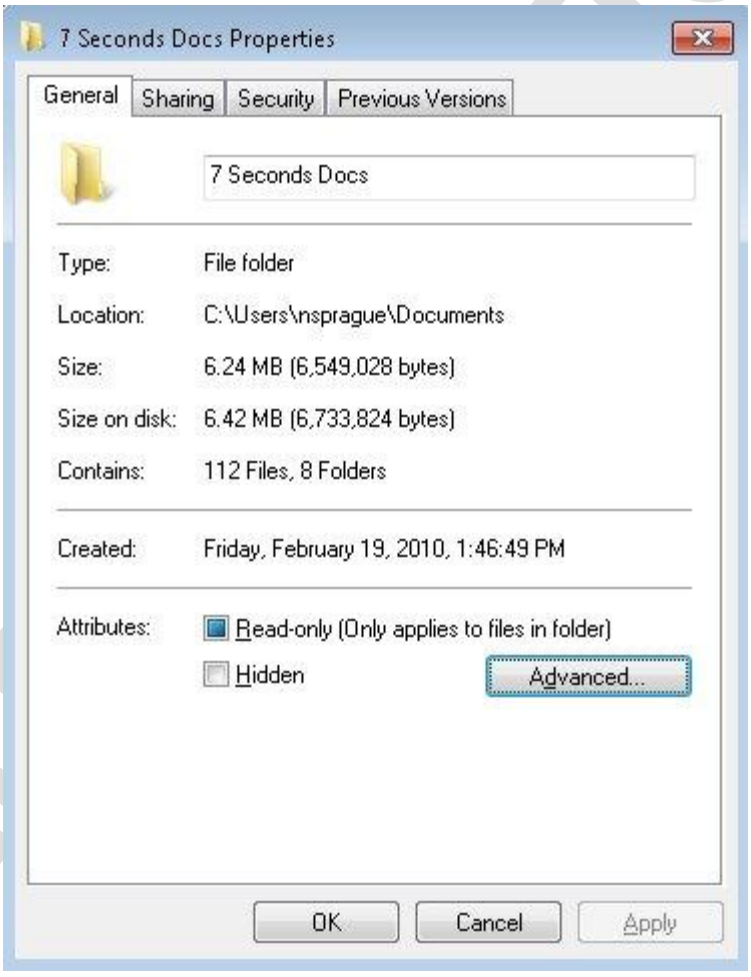
EFS uses a process known as public key encryption. In public key encryption, a user has 2 keys: a public key, also known as a certificate, and a private key. The public key is kept in the computer's store and accessible to everyone. Users can use the public key to encrypt data. The private key is kept in the user's private certificate store and can only be used by the user. The private key decrypts data which has been encrypted using the public key. The first time a user encrypts a file on a computer running Windows 7, the computer creates an EFS certificate and private key. This allows you to even encrypt data on an external drive, flash drive, etc. EFS encryption works so that even if a user has read access to a file on a flash drive, for example, they cannot actually open the file unless they have the appropriate encryption certificate.

Files and folders on a drive can only be encrypted if the drive is formatted with the NTFS file system. Also, a file or folder cannot be both encrypted and compressed at the same time. If a file or folder is compressed and you encrypt it, the compression will be lost. If you COPY an encrypted file to a compressed folder, the file will remain compressed - not encrypted. If you MOVE a compressed file to an encrypted folder, the file will decompress and

become encrypted. If you copy an encrypted file or folder to a FAT32 volume, Windows 7 decrypts the file when it is copied.

You can encrypt a file with EFS using the following steps:

1. Right-click the folder or file you want to encrypt and then click *Properties*.
2. Click the *General* tab and then click *Advanced*.



3. Select the *Encrypt contents to secure data* checkbox and then click *OK*.

Encrypted file icons are colored green in Windows Explorer. To unencrypt files and folders, simply follow the instructions above, but uncheck the *Encrypt contents to secure data* checkbox.

If the encrypted file needs to be shared with another user on the same computer, they need to export their EFS certificate. You would then import it and add the certificate to the shared file.

The first time you encrypt a folder or file, you should back up your encryption certificate. If your certificate and key are lost or damaged, and you do not have a backup, you won't be able to access the folders/files that you have encrypted. Read Back up Encrypting File System (EFS) certificate for instructions on this.

To recover encrypted files with lost or damaged keys, you use a special EFS certificate. To use this special certificate, you have to create the recovery certificate, install it, and then update other EFS certificates with the recovery certificate. To do this, follow these steps:

1. Click *Start* and enter *cmd* into the search box to open a command prompt.
2. If you are using removable media such as a disk or flash drive (recommended) to store your certificate, plug it in now.
3. Navigate to the directory on the drive where you want to store the recovery certificate by typing drive letter and then pressing *Enter*.

4. Type *cipher /r: [filename]* (where filename is the name that you want to give to the recovery certificate) and then press *Enter*. If you are prompted for an administrator password or confirmation, type the password or provide confirmation. The recovery certificate will be save to the location you specified.

Permissions:

In the last section of this guide, sharing was discussed and the topic of permissions came up several times. Below we will explain permissions in more detail. Read the following carefully and note the distinctions between FILE and FOLDER.

NTFS File Permissions:
NTFS file permissions are used to control the access that a user, group, or application has to folders and files. They are referred to as NTFS permissions because a drive must be formatted with NTFS in order to utilize these permissions. NTFS file permissions are used to control the access that a user, group, or application has to files. This first table displays the available permissions for files.

Full Control	Read, write, modify, execute, change attributes, permissions, and take ownership of the file.
Modify	Read, write, modify, execute, and change the file's attributes.
Read & Execute	Display the file's data, attributes, owner, and permissions, and run the file (if it's a program or has a program associated with it for which you have the necessary permissions).
Read	Display the file's data, attributes, owner, and permissions.
Write	Write to the file, append to the file, and read or change its attributes.

Windows 7 has the option of denying a user or users a particular permission. For example, if you wanted to make sure that Bob is unable to read any files, then simply deny him read permissions. Permissions are cumulative, except for Deny, which overrides everything. By cumulative, we mean that a user's effective permissions are the result of combining the user's assigned permissions and the permissions assigned to any groups that the user is a member of. For example, if Bob is assigned Read access to a file, and the "sales" group that Bob is a member of has Write permissions assigned, Bob's effective permissions is are Read and Write for that file.

NTFS Folder Permissions:
NTFS Folder permissions determine the access that is granted to a folder and the files and subfolders within that folder. These permissions can be assigned to a user or group. The following table displays the various permissions for folders.

Full Control	Read, write, modify, and execute files in the folder, change attributes, permissions, and take

	ownership of the folder or files within.
Modify	Read, write, modify, and execute files in the folder, and change attributes of the folder or files within.
Read & Execute	Display the folder's contents and display the data, attributes, owner, and permissions for files within the folder, and run files within the folder (if they're programs or have a program associated with them for which you have the necessary permissions).
List Folder Contents	Display the folder's contents and display the data, attributes, owner, and permissions for files within the folder, and run files within the folder (if they're programs or have a program associated with them for which you have the necessary permissions).
Read	Display the file's data, attributes, owner, and permissions.
Write	Write to the file, append to the file, and read or change its attributes.

The Read & Execute and List Folder Contents folder permissions appear to be exactly the same, however, they are inherited differently, thus are different permissions. Files can inherit the Read & Execute permissions but can't inherit the List Folder Contents permission. Folders can inherit both.

File permissions override folder permissions. For example, let's say that Bob has read access to a file called file.txt which is located in a folder that he has no access to. In this case, the file will be invisible to the Bob and since he cannot list the folder contents, he would have to access the file using the UNC path or the logical file path.

Special Access File Permissions:
Windows 2000 & 2003 also support special access permissions which are made by combining other permissions. The following tables will show special access permissions and the recipes to make them.

File Special Permissions	Full Control	Modify	Read & Execute	Read	Write
Traverse Folder/Execute File	X	X	X		
List Folder/Read Data	X	X	X	X	
Read Attributes	X	X	X	X	
Read Extended Attributes	X	X	X	X	
Create Files/Write Data	X	X			X

Create Folders/Append Data	X		X				X					
Write Attributes	X		X				X					
Write Extended Attributes	X		X				X					
Delete Subfolders and Files	X											
Delete	X		X									
Read Permissions	X		X		X		X		X			
Change Permissions	X											
Take Ownership	X											
Synchronize	X		X		X		X		X			

Special Access Folder Permissions:
Below are the special access permissions for folders.

Folder Special Permissions	**Full Control**		**Modify**		**Read & Execute**		**List Folder Contents**		**Read**		**Write**	
Traverse Folder/Execute File	X		X		X		X					
List Folder/Read Data	X		X		X		X		X			
Read Attributes	X		X		X		X		X			
Read Extended Attributes	X		X		X		X		X			
Create Files/Write Data	X		X								X	
Create Folders/Append Data	x		x								X	
Write Attributes	X		X								X	
Write Extended Attributes	X		X								X	
Delete Subfolders And Files	X											
Delete	X		X									
Read Permissions	X		X		X		X		X		X	
Change Permissions	X											

Take Ownership	X						
Synchronize	X	X	X	X	X	X	

Remember that file permissions override the permissions of its parent folder. Anytime a new file is created, the file will inherit permissions from the target folder.

Share Permissions:
Share level permissions only apply when a file or folder is being accessed via the network and do not apply to a user logged into the machine locally. The following are the different share-level permissions:

Read View files and subdirectories. Execute applications. No changes can be made.

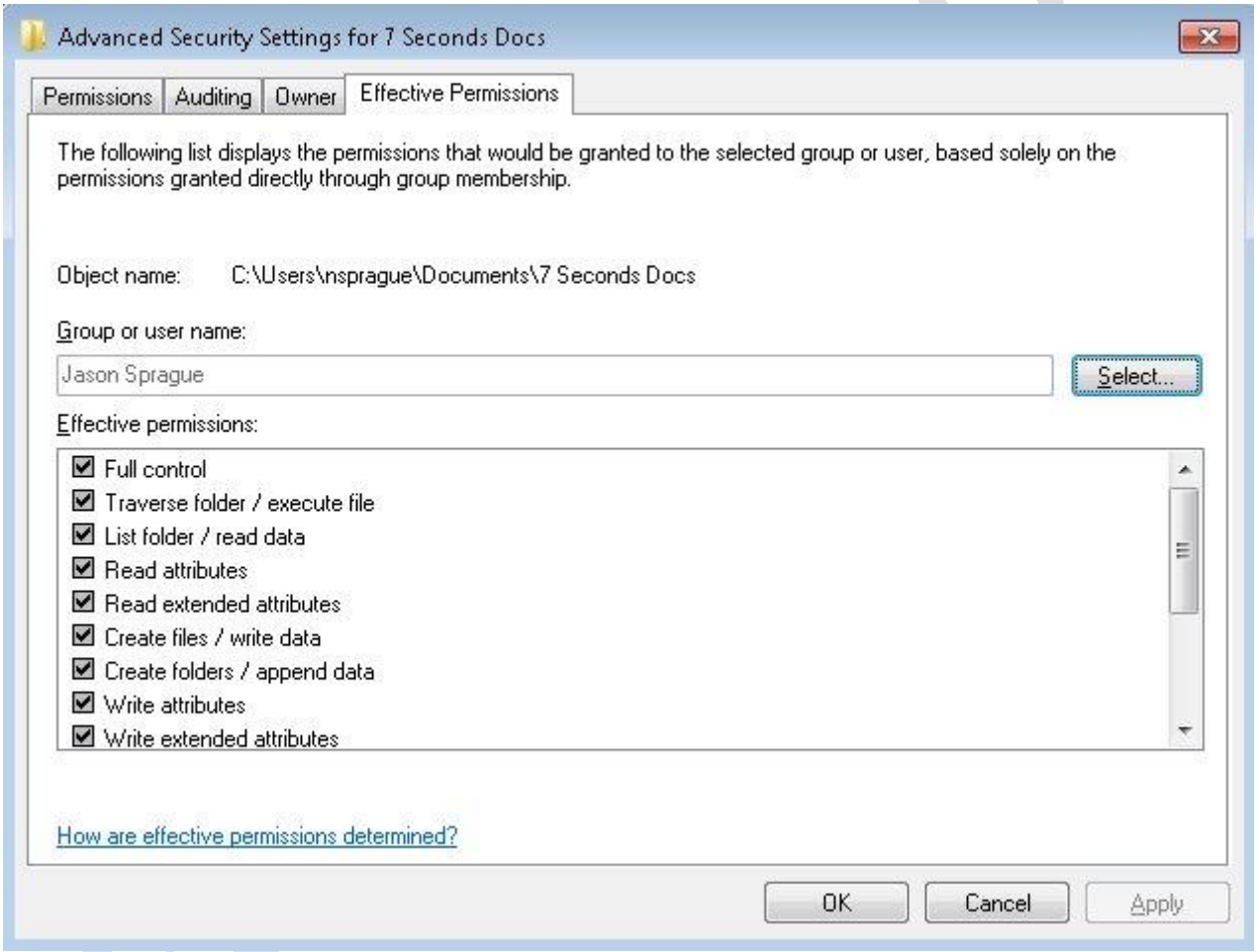
Change Includes read permissions and the ability to add, delete or change files or subdirectories

Full Control Can perform any and all functions on all files and folders within the share.

The Deny permission can also be applied to shares. The Deny permission overrides all others. When folders on FAT and FAT32 volumes are shared, only the share level permissions apply as these systems do not support file and directory (NTFS) permissions. When folders on NTFS volumes are shared, the effective permission of the user will be the most restrictive of the NTFS and share permissions. This means that if Bob is trying to access a file called *mystuff* located on *myshare* and he has share permissions of read and file permissions of full control, his effective permissions would be read. Conversely, if his share permissions are full control and his file permissions are read, he will still only have read permissions to *mystuff*.

Effective Permissions:
Determining effective permissions can get confusing, especially on enterprise networks. In Windows 7, there is help. To view effective permissions, follow these steps:

1. Right click on the file or folder that you wish to find the effective permissions for and click *Properties*.
2. Click on the *Security* tab and then the *Advanced* button.
3. In the new window, click the *Effective Permissions* tab. Type in a group or user to check.



This feature lists the permissions that would be granted to the selected group or user based solely on the permissions granted directly through group membership. It does not take into account share permissions.

Copying, Moving, and Inheritance:

The next table shows what happens to files when they are copied or moved within or across NTFS partitions.

Moving within a partition	Does not create a new file - simply updates location in directory. File keeps its original permissions.
Moving across a partition	Creates a new file and deletes the old one. Inherits the target folders permissions.
Copying within a partition	Creates a new file which inherits permissions of target folder.

70-680 Study Guide - Configure User Account Control (UAC)

User Account Control (UAC):

If you logged on with a user account that was a member of the local administrators group in previous versions of Microsoft Windows, such as Windows XP, you automatically had administrator-level access at all times. This would not present a problem on its own, however, administrators would login with their admin account even when they weren't performing admin tasks. The problem with this is that any program run by a user logged on with an administrative account runs with the rights and privileges of that user. This created a security risk which is addressed with UAC.

User Account Control (UAC) is a security feature in Windows 7. It provides the users with notification of all the system-level changes that an application makes onto the system. If you configure UAC to notify the changes its popups ask users for their confirmation when software makes changes, that can harm your computer and therefore it adds another layer of security to Windows. It improves the security in Microsoft Windows by enforcing standard user privileges on application software, until it is authorized by the administrator to increase or elevate the user privileges. In this way, only the trusted applications receive administrative privileges, which implies that a user account may have administrator privileges assigned to it, but applications that the user runs do not inherit those privileges unless they are approved or the user explicitly authorizes them. Windows Vista only offers you two types of UAC settings: on and off, but in Windows 7, you can choose from a wide range of settings. Windows 7 provides you with four UAC settings, which are:

- **Always notify** – You can select this UAC setting if you want to get notified whenever a program tries to install or make changes to your computer system. This option can also be selected if you want to be notified when you make changes to the Windows settings. This is the most secure setting.
- **Notify me only when programs try to make changes to my computer** – You can select this option when you need notifications only when programs attempt to make changes in your windows settings.

When you select this option you don't get notifications when you yourself make some changes in the windows settings.

- **Notify me only when programs try to make changes to my computer (do not dim my desktop)** - You can select this option when you need notifications only when programs attempt to make changes in your windows settings and your desktop will not be dimmed with this option. When you select this option you don't get notifications when you yourself make some changes in the windows .
- **Never notify** – It disable the User Access Control. You can select this option when you don't want to receive any sort of notification whenever you or any of system programs makes any change in the windows settings. This is the least secure setting.

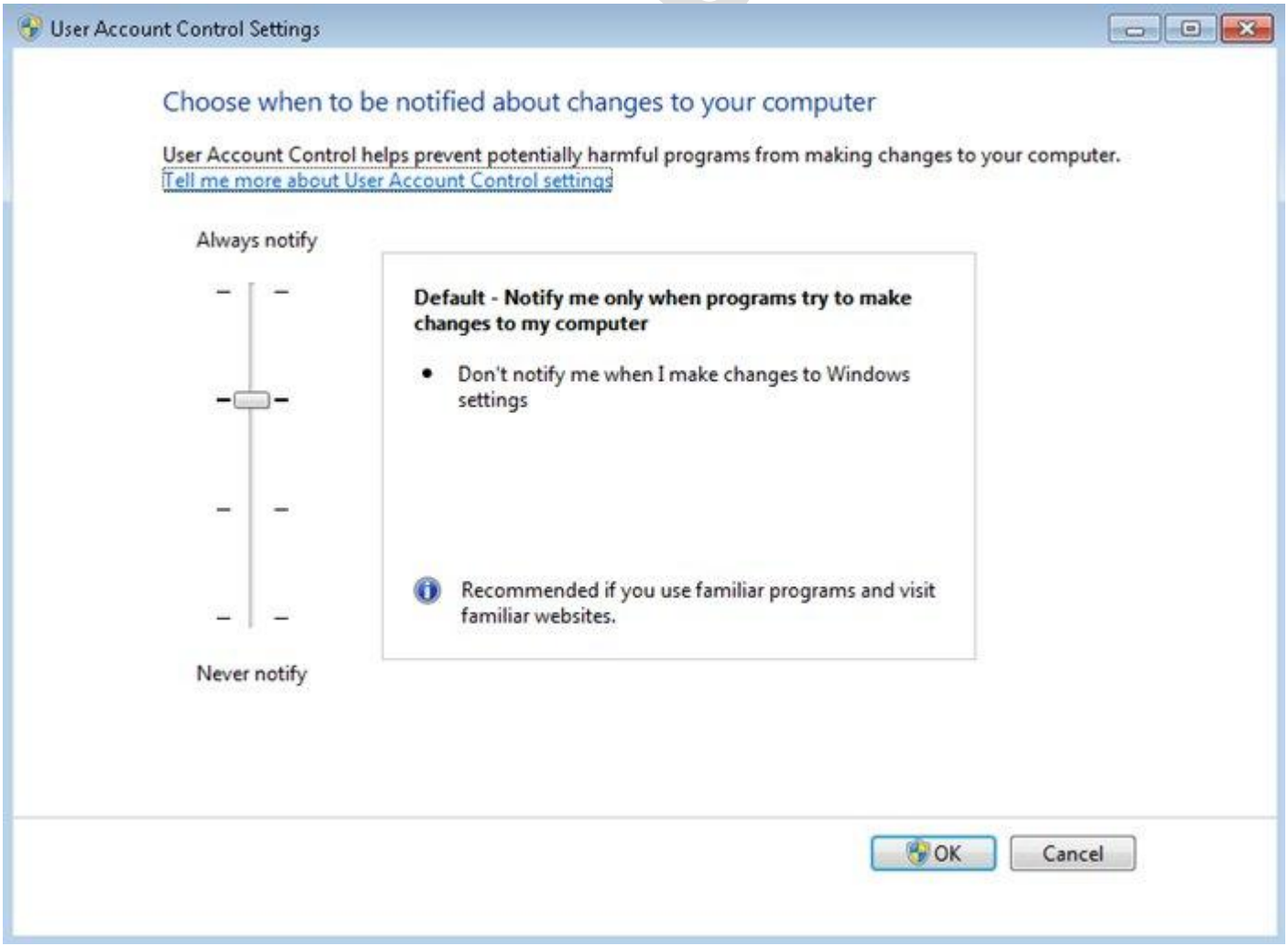
Secure Desktop:

Secure Desktop ensures that malware is unable to alter the display of the UAC prompt as a method of tricking you into allowing administrative access. When you configure UAC to use the Secure Desktop, the desktop is unavailable when a UAC prompt is triggered. You must respond to the UAC prompt before you can interact with the computer. The secure desktop actually makes a bitmap copy of the current screen which is why if you have a video running when the secure desktop comes up, the video will appear to freeze. If you do not respond to a UAC prompt on a Secure Desktop after 150 seconds, Windows will automatically deny the request and return to the standard desktop.

Configuring User Account Control (UAC):

Use the following steps to configure UAC.

1. Click *Start* and type *UAC* in the search box.
2. Click *Change User Account Control Settings*.
3. This loads User Account Control Settings panel. On this screen you can adjust the notifications using the slider in the left pane. You can select from the following UAC settings:
    - Always notify me
    - Default
    - Default (Without Dimming)
    - Never notify



4. Select the appropriate setting and then click *OK*. The computer must be restarted for changes to take effect.

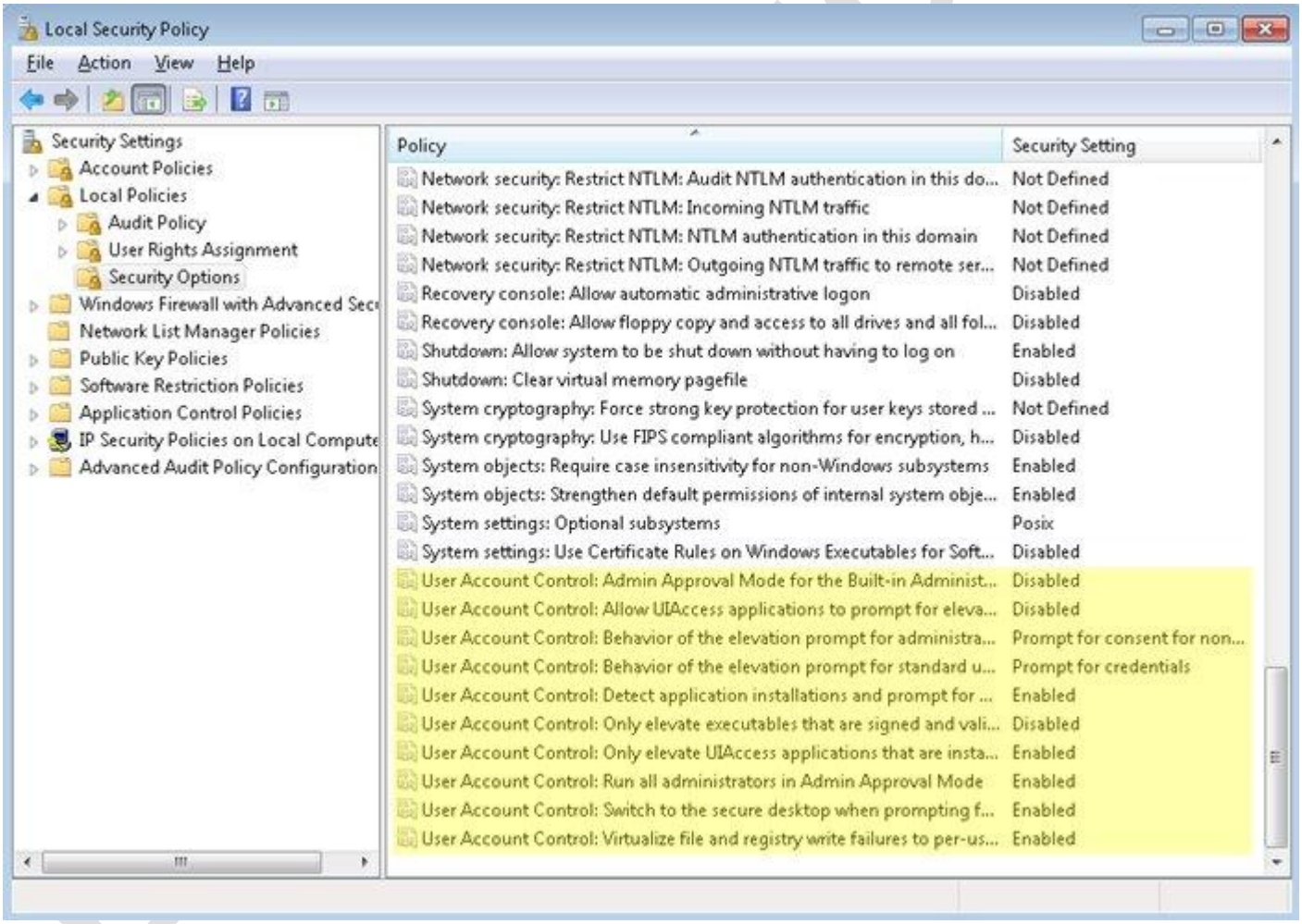
Typically, only a user with administrative rights will get UAC warnings because it is disabled by default for standard users.

Configuring UAC With Local and Group Policies:

Besides changing the notification behavior of UAC, you can also control the behavior of the UAC by using local or group policies. Local policies are managed from each local computer while group policies are managed as part of Active Directory.

Follow these steps to change UAC settings:

1. Click *Start*, type *secpol.msc* in the Search programs and files box, and press *Enter*.
2. From the Local Security Policy tree, click *Local Policies* and then double-click *Security Options*
3. The UAC policies are at the bottom of the list. To modify a setting, simply double-click on it and make the necessary changes.



Below are the policies that can be modified and what they do.

Policy	**Description**
Use Admin Approval Mode for the built-in	This policy setting controls the behavior of Admin Approval Mode for the built-in Administrator account. The options are:

Administrator account	• Enabled: The built-in Administrator account uses Admin Approval Mode. By default, any operation that requires elevation of privilege will prompt the user to approve the operation. • Disabled: (Default) The built-in Administrator account runs all applications with full administrative privilege.
Allow UIAccess applications to prompt for elevation without using the secure desktop	This policy setting controls whether User Interface Accessibility (UIAccess or UIA) programs can automatically disable the secure desktop for elevation prompts used by a standard user. • Enabled: UIA programs, including Windows Remote Assistance, automatically disable the secure desktop for elevation prompts. If you do not disable the "User Account Control: Switch to the secure desktop when prompting for elevation" policy setting, the prompts appear on the interactive user's desktop instead of the secure desktop. • Disabled: (Default) The secure desktop can be disabled only by the user of the interactive desktop or by disabling the "User Account Control: Switch to the secure desktop when prompting for elevation" policy setting.
Behavior of the elevation prompt for administrators in Admin Approval Mode	This policy setting controls the behavior of the elevation prompt for administrators. The options are: • Elevate without prompting: Allows privileged accounts to perform an operation that requires elevation without requiring consent or credentials. Note: Use this option only in the most constrained environments. • Prompt for credentials on the secure desktop: When an operation requires elevation of privilege, the user is prompted on the secure desktop to enter a privileged user name and password. If the user enters valid credentials, the operation continues with the user's highest available privilege. • Prompt for consent on the secure desktop: When an operation requires elevation of privilege, the user is prompted on the secure desktop to select either Permit or Deny. If the user selects Permit, the operation continues with the user's highest available privilege. • Prompt for credentials: When an operation requires elevation of privilege, the user is prompted to enter an administrative user name and password. If the user enters valid credentials, the operation continues with the applicable privilege.

	• Prompt for consent: When an operation requires elevation of privilege, the user is prompted to select either Permit or Deny. If the user selects Permit, the operation continues with the user's highest available privilege. • Prompt for consent for non-Windows binaries: (Default) When an operation for a non-Microsoft application requires elevation of privilege, the user is prompted on the secure desktop to select either Permit or Deny. If the user selects Permit, the operation continues with the user's highest available privilege.
Behavior of the elevation prompt for standard users	This policy setting controls the behavior of the elevation prompt for standard users. The options are: • Prompt for credentials: When an operation requires elevation of privilege, the user is prompted to enter an administrative user name and password. If the user enters valid credentials, the operation continues with the applicable privilege. • Automatically deny elevation requests: When an operation requires elevation of privilege, a configurable access denied error message is displayed. An enterprise that is running desktops as standard user may choose this setting to reduce help desk calls. • Prompt for credentials on the secure desktop: (Default) When an operation requires elevation of privilege, the user is prompted on the secure desktop to enter a different user name and password. If the user enters valid credentials, the operation continues with the applicable privilege.
Detect application installations and prompt for elevation	This policy setting controls the behavior of application installation detection for the computer. The options are: • Enabled: (Default for home) When an application installation package is detected that requires elevation of privilege, the user is prompted to enter an administrative user name and password. If the user enters valid credentials, the operation continues with the applicable privilege. • Disabled: (Default for enterprise) Application installation packages are not detected and prompted for elevation. Enterprises that are running standard user desktops and use delegated installation technologies such as Group Policy Software Installation or Systems Management Server (SMS) should disable this policy setting. In this case, installer detection is unnecessary.
Only elevate executable files that are signed and validated	This policy setting enforces public key infrastructure (PKI) signature checks for any interactive applications that request elevation of privilege. Enterprise administrators can control which applications are allowed to run by adding certificates to the Trusted Publishers certificate store on local computers. The options are:

- Enabled: Enforces the PKI certification path validation for a given executable file before it is permitted to run.
- Disabled: (Default) Does not enforce PKI certification path validation before a given executable file is permitted to run.

This policy setting controls whether applications that request to run with a User Interface Accessibility (UIAccess) integrity level must reside in a secure location in the file system. Secure locations are limited to the following:

- …\Program Files\, including subfolders
- …\Windows\system32\
- …\Program Files (x86)\, including subfolders for 64-bit versions of Windows

Only elevate UIAccess applications that are installed in secure locations

Note: Windows enforces a public key infrastructure (PKI) signature check on any interactive application that requests to run with a UIAccess integrity level regardless of the state of this security setting. The options are:

- Enabled: (Default) If an application resides in a secure location in the file system, it runs only with UIAccess integrity.
- Disabled: An application runs with UIAccess integrity even if it does not reside in a secure location in the file system.

This policy setting controls the behavior of all User Account Control (UAC) policy settings for the computer. If you change this policy setting, you must restart your computer. The options are:

Run all administrators in Admin Approval Mode

- Enabled: (Default) Admin Approval Mode is enabled. This policy must be enabled and related UAC policy settings must also be set appropriately to allow the built-in Administrator account and all other users who are members of the Administrators group to run in Admin Approval Mode.
- Disabled: Admin Approval Mode and all related UAC policy settings are disabled. Note: If this policy setting is disabled, the Security Center notifies you that the overall security of the operating system has been reduced.

Switch to the secure desktop when prompting

This policy setting controls whether the elevation request prompt is displayed on the interactive user's desktop or the secure desktop. The options are:

for elevation

- Enabled: (Default) All elevation requests go to the secure desktop regardless of prompt behavior policy settings for administrators and standard users.
- Disabled: All elevation requests go to the interactive user's desktop. Prompt behavior policy settings for administrators and standard users are used.

Virtualize file and registry write failures to per-user locations

This policy setting controls whether application write failures are redirected to defined registry and file system locations. This policy setting mitigates applications that run as administrator and write run-time application data to %ProgramFiles%, %Windir%, %Windir%\system32, or HKLM\Software. The options are:

- Enabled: (Default) Application write failures are redirected at run time to defined user locations for both the file system and registry.
- Disabled: Applications that write data to protected locations fail.

70-680 Study Guide - Configure Authentication and Authorization

User Accounts:

Windows 7 workstations can be configured as a member of a workgroup or as a member of a domain. When a workstation is configured in a workgroup, user access and security are configured on the workstation itself. Each computer maintains its own security database, which includes its own local user accounts and user groups. If a user on one computer needs to access resources on other computers, a user account has to be created on each computer, or they have to login with an existing account on that computer. The user and group information is not shared with other computers. By default, if the computer is not part of a domain, local users are created without passwords.

A domain, on the other hand, uses one database known as Active Directory, which is stored on one or more domain controller servers. This provides the ability to share its common security and user and group account information for all computers within the domain. When a user logs onto the domain, they can access resources throughout the domain with the same logon (single sign-on). The domain allows for centralized network

administration of all users, groups, and resources on the network. A user account enables a user to log on to a computer or domain with an identity that can be authenticated and authorized for access to the resources of the computer or domain. Because the user account is meant to be assigned to one and only one user, it enables you to assign rights and permissions to a single user and gives you the ability to track what users are doing.

When you install Windows 7, the operating system installs default user accounts which are managed using the User Accounts control panel.

- **Administrator** - The Administrator account is a predefined account that provides complete access to files, directories, services, and other facilities on the computer. You cannot delete this account. The built-in administrator account is disabled by default in Windows 7 on new installations. If Windows 7 determines during an upgrade from Windows Vista that the built-in administrator is the only active local administrator account, Windows 7 leaves the account enabled and places the account in Admin Approval Mode. The built-in administrator by default, cannot log on to the computer in safe mode.
- **Guest** - The Guest account is designed for users who need one-time or occasional access. Although guests have only limited system privileges, you should be very careful about using this account because it opens the system to potential security problems. The risk is so great that the account is initially disabled when you install Windows 7.

When you create additional accounts, you can choose between two options:

- Standard user
- Administrator

These account types give the user a different level of control. 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. 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 (i.e. system files), or change settings on the computer that affect other users.

The administrator account provides the most control over the computer, and should be used only when necessary. The administrator account lets you make changes that affect other users. Administrators can change security settings, install software and hardware, and access all files on the computer. Administrators can also make changes to other local user accounts.

When you set up Windows, you are required to create an administrator account that allows you to set up your computer and install any programs that you want to use. After you have finished setting up your computer, it is recommended for security reasons to create a standard account for regular use.

User Groups:

The Windows 7 built-in groups that you can add users to in order to assign them rights are as follows:

- **Administrators** - Members of this group have unrestricted access to the client.
- **Backup Operators** - Members of this group are able to override file and folder access restrictions for the purpose of backing up data.
- **Cryptographic Operators** - Members of this group are able to perform cryptographic operations. This policy is used only when Windows 7 is deployed in a special configuration called common criteria mode.

In this mode administrators are able to read and write all settings except those related to the cryptography of IPsec policy.

- **Distributed COM Users** - Members of this group are able to manipulate Distributed COM objects on this computer.
- **Event Log Readers** - Members of this group can read data stored in the event logs.
- **Network Configuration Operators** - Members of this group can change Transmission Control Protocol/Internet Protocol (TCP/IP) address settings.
- **Performance Log Users** - These users can schedule the logging of performance counters, enable trace providers, and collect event traces.
- **Performance Monitor Users** - These users can access performance counter data locally and remotely.
- **Power Users** - This group is included for backward compatibility.
- **Remote Desktop Users** - Members of this group are able to log on remotely through remote desktop.
- **Replicator** - This group is used to support file replication in domain environment.

Configuring Authentication:

User authentication is a method of identifying the user and verifying that the user is allowed to access some restricted service. After the user has been established as authenticated user, user's authorization determine the user's rights to access resources in different modes, depending on the user rights assigned to that user. For example, depending on the user authorization a user can access a file, a folder, a service or an application with full rights or partial rights.

Configuring authentication methods:

1. Click *Start* and type *Firewall* in the search box.
2. Select *Windows Firewall with Advanced Security* from the search results.
3. On Windows Firewall with Advanced Security page, click *Windows Firewall Properties*.
4. On the *IPsec Settings* tab, click *Customize*.
5. In the Authentication Method section, select the type of authentication which you want to use From the given list:
    - **Default** - This option enables the authentication method currently defined by the local administrator in Windows Firewall with Advanced Security or by Group Policy as the default.
    - **Computer and User using KerberosV5** - This option configures your computer to use and require authentication of both the computer and the currently logged-on user by using their domain credentials. This authentication method can work only with other computers that can use Authenticated IP (AuthIP), including Windows 7, Windows Vista, Windows Server 2008, and Windows Server 2008 R2. User-based authentication using Kerberos V5 isn't supported by IKE v1.
    - **Computer (using Kerberos V5)** - This option configures your computer to use and require authentication of the computer by using its domain credentials. This option works with other computers that can use IKE v1, and also supports earlier versions of Windows.
    - **User (using Kerberos V5)** - This option configures your computer to use and require authentication of the currently logged-on user by using his or her domain credentials. This authentication method works only with other computers that are capable of using AuthIP, including Windows 7, Windows Vista, Windows Server 2008, and Windows Server 2008 R2. User-based authentication using Kerberos V5 isn't supported by IKE v1.
    - **Computer certificate from this certification authority** - This option requires you to enter the identification of a certification authority (CA), and configures the computer to use and require authentication by using a certificate which is issued by the selected CA. You can also select Accept only health certificates, then only certificates that include the system health authentication enhanced key usage (EKU) provided in a Network Access Protection (NAP) infrastructure can be used for this rule.

- **Advanced** - You can click Customize to specify a custom combination of authentication methods. You can specify a combination of both a First authentication method and a Second authentication method. The first authentication method can be one of the following:
  - **Computer (Kerberos V5)** - This option configures your computer to use and require authentication of the computer by using its domain credentials. This option works with other computers that can use IKE v1, and also supports earlier versions of Windows.
  - **Computer (NTLMv2)** - This option configures your computer to use and require authentication of the computer by using its domain credentials. This option works only with other computers that are capable of using AuthIP, including Windows 7, Windows Vista, Windows Server 2008, and Windows Server 2008. IKE v1 does not support user-based authentication using Kerberos V5.
  - **Computer certificate from this certification authority (CA)** - This option requires you to enter the identification of a certification authority (CA), and configures the computer to use and require authentication by using a certificate which is issued by the selected CA. You can also select Accept only health certificates, and then certificates issued by a NAP server can be used.
  - **Preshared key (not recommended)** - This method requires you to enter a preshared key which configures your computer to authenticate by exchanging the preshared keys. The authentication succeeds only if they match. This method is not recommended by microsoft, and is included only for backward compatibility and testing purposes.

  When you select First authentication is optional, then the connection can succeed even if the authentication attempt specified in this column fails. The second authentication method can be one of the following:

  - **User (Kerberos V5)**
  - **User (NTLMv2)**
  - **User health certificate from this certification authority (CA)** - This option requires you to enter the identification of a CA and configures your computer to use and require user-based authentication by using a certificate which is issued by the specified CA. You can also select Enable certificate to account mapping, which enables certificate association with a user in Active Directory for the purpose of granting or denying the access to specified users or user groups.
  - **Computer health certificate from this certification authority (CA)** - This option requires you to enter the identification of a certification authority (CA), and configures the computer to use and require authentication by using a certificate which is issued by the selected CA. You can also select Accept only health certificates, then only certificates that include the system health authentication enhanced key usage (EKU) provided in a Network Access Protection (NAP) infrastructure can be used for this rule.

6. Click *OK* on dialog boxes to save your changes and return to the Group Policy Management Editor.

Multifactor Authentication:

Multi-Factor Authentication (MFA) is an additional layer of security that offers enhanced control over your AWS Account settings and the AWS services and resources that have been subscribed for your account. It is an optional feature that requires a valid six-digit, single-use code from an authentication device, in addition to your standard AWS credentials, before access is granted.

MFA uses an authentication device that generates random, six-digit authentication codes continuously. Once you enable AWS MFA, whenever somebody tries to sign in to AWS to access your AWS Account settings on the AWS Portal or to use the AWS Management Console to access the AWS services and resources that are subscribed to

your account, access is granted only after the correct user name and password and the precise code from your authentication device are provided. This multi-factor authentication provides even greater protection for your AWS Account settings and the AWS services and resources that are subscribed to your account, including extra protection of sensitive information such as your AWS access identifiers and critical actions like changing your AWS infrastructure service subscriptions.

Smart Cards with PIV:

Windows 7 provides support for smart card–related Plug and Play and the Personal Identity Verification (PIV).It implies that users of Windows 7 can use smart cards from vendors who have published their drivers through Windows Update without needing special middlewares. These drivers can be downloaded in the similar way as drivers for other devices in Windows. When a PIV-compliant smart card is inserted into a smart card reader, Windows tries to download the driver from Windows Update. If an appropriate driver is not accessed through Windows Update, a PIV-compliant minidriver that is included with Windows 7 operating system is used for the card.

Network administrators, who want to enhance the security of the organization's portable computers used by remote users, can use this service. It has very simplified deployment made possible by smart card Plug and Play PIV support. Users can use smart cards to perform critical business tasks in a secure manner.

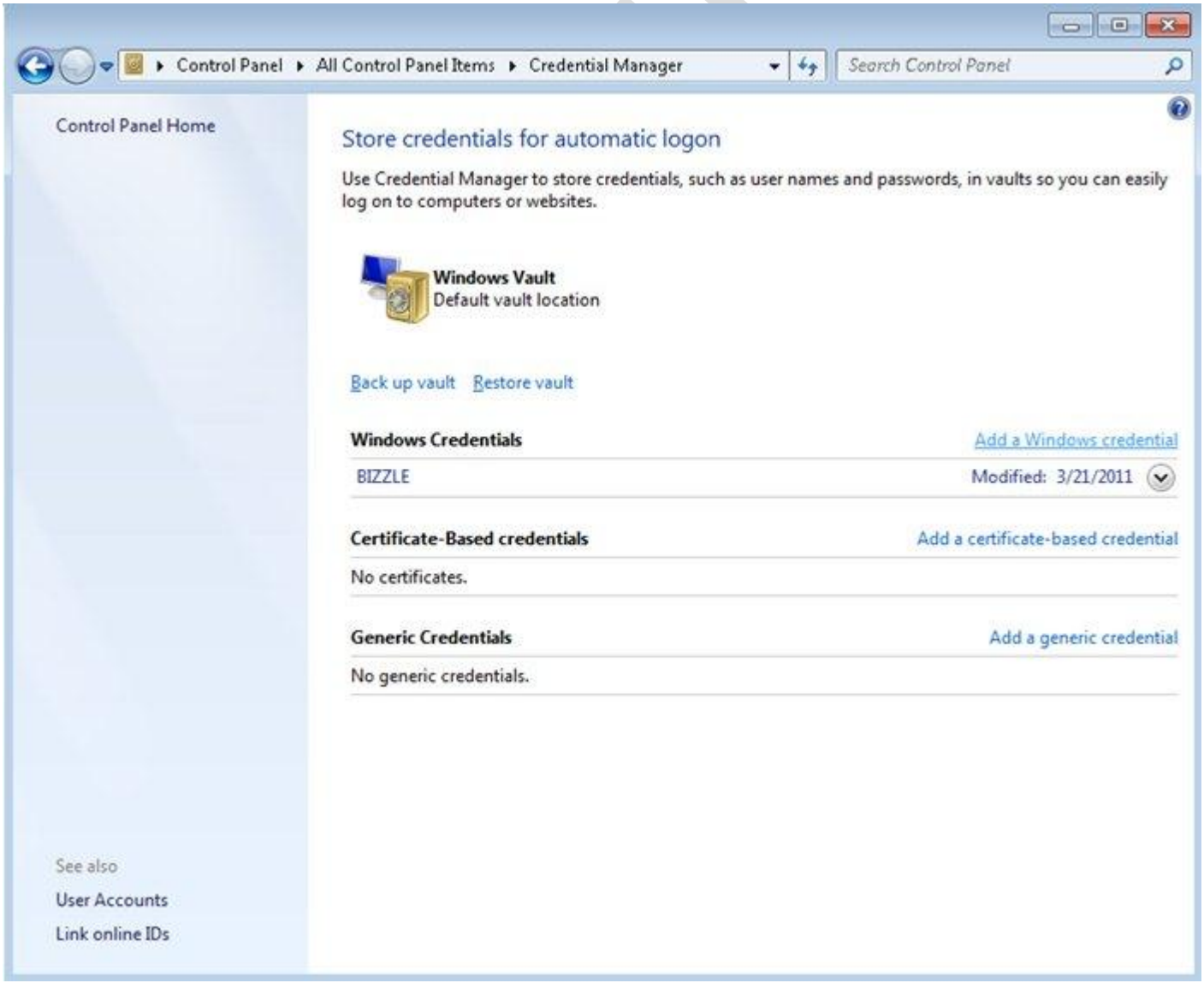
The smart card with PIV in Windows 7 have following features:

- **Encrypting drives with BitLocker Drive Encryption** - In the Windows 7 operating system, users can choose to encrypt their removable media with BitLocker and then they can use the smart cards to unlock the drive. Windows can retrieve the correct minidriver for the smart card and allows the operation to complete.
- **Smart card domain logon using the PKINIT protocol** - In Windows 7, the appropriate minidriver for a smart card is retrieved automatically, enabling a new smart card to authenticate to the domain without requiring the user to install or configure additional middleware or drivers.
- **E-mail and Document signing** - Windows 7 users can retrieve the correct minidriver for a smart card at run time automatically to sign an e-mail or document. XML Paper Specification (XPS) documents can also be signed without the need for additional software.
- **Use with business applications** - In Windows 7, any application that uses Cryptography Next Generation (CNG) or CryptoAPI to enable the applications to use certificates can use Windows to retrieve the correct minidriver for a smart card at run time so that no additional middleware is required.

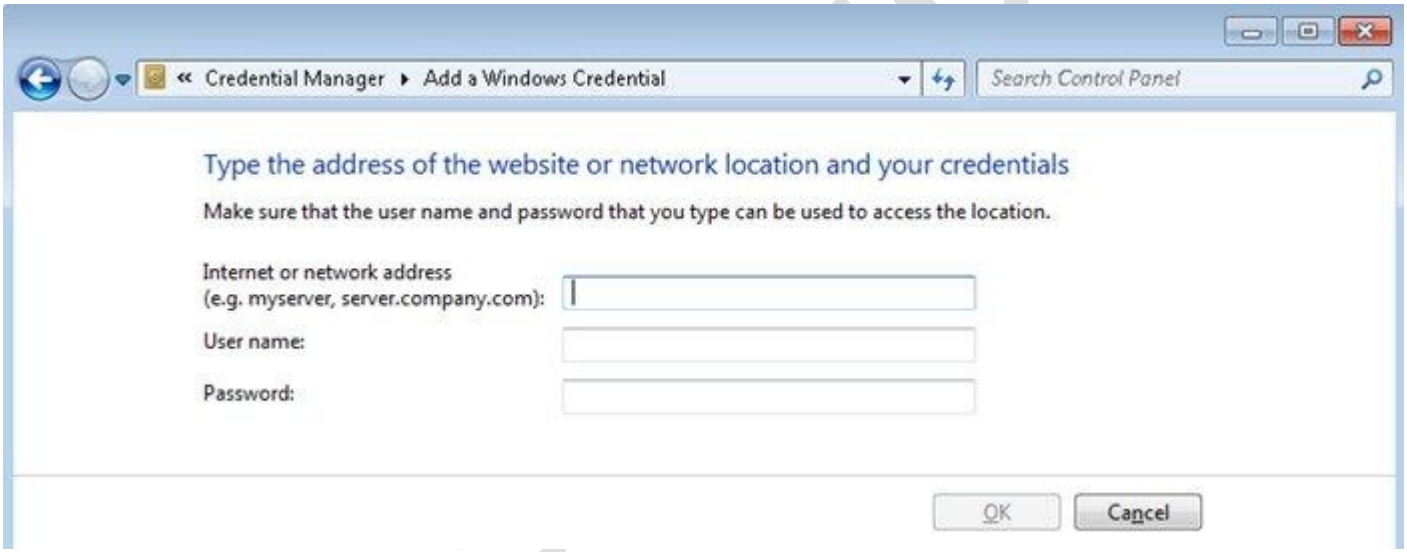
Credential Manager in Windows 7:

Credential Manager allows you to store credentials, such as user names and passwords that are used to log on to websites or on other computers on the network. When you store your credentials, Windows automatically logs you on to websites or other computers. Credentials are saved in vaults by Windows. Follow these steps to manage your credentials in windows 7:

1. Click the *Start* and then click *Control Panel*.
2. Type *Credential manager* in the Control Panel's search Window, then click *Credential Manager* from the search window.



3. Click on *Add a Windows credential*. In the Resource box, type the URL of the website or the name of the computer on the network or that you want to access. Next, type the user name and password that you want to use for that computer or website, and then click *OK*. You can also perform actions like Edit/Remove the credential from the vault at any time.



To add a certificate based credential, follow these steps:

1. Open the Credential Manager by following the steps above.
2. Click *Add a certificate-based credential* and then click *Open the Certificate Manager* to view the Current User Certificates.
3. Enter the internet or network address, then click *Select Certificate*, and then click *OK*.

Windows Vault contains credentials for websites and programs. It can be backed up by following these steps:

1. Open the Credential Manager in the control panel.
2. Click *Back up vault* to make a backup of all the stored credentials.
3. Browse to the location to store Windows Vault backup and then click *Next*. Press *CTRL+ALT+DELETE* to continue your backup.
4. Provide a password to protect the backup file. Type the Password in the box and Click *Next*.

To restore the vault, follow these steps:

1. Open the Credential Manager in the control panel.
2. Click the *Restore Vault* link in the Credential Manager window.
3. Browse to the location for the Backup vault file to restore then click *Next*.

4. Press *CTRL+ALT+DELETE* to continue restoring your logon credentials.
5. Enter the password for the backup file in the box and click *Next*.
6. Click *Finish*.

Although Credential Manager can be used to back up some forms of digital certificates, it cannot be used to back up and restore the self-signed Encrypting File System (EFS) certificates

70-680 Study Guide - Configure BranchCache

Introduction to BranchCache:

BranchCache is a feature of Microsoft Windows 7 which can be utilized for businesses that operate from multiple office locations. BranchCache provides a file caching service for professional network administrators which works by enabling Windows servers to automatically retrieve and distribute the local copies of files which are being accessed remotely by Windows 7 clients.

BranchCache can help increase network responsiveness of centralized applications, when they are accessed from remote offices, and users in those offices can experience as if they are working on their local area network. BranchCache also helps in reducing WAN utilization. When you enable BranchCache, a copy of data accessed from intranet Web and file servers is cached locally in the branch office. When another client on the same network requests that file, the client downloads it from the local cache without downloading the same content from the WAN link.

Your system must meet the following requirements to use BranchCache:

- Client computers must use Windows 7, with the BranchCache feature enabled on it.
- Web servers and File servers must use Windows Server 2008 R2, with the BranchCache feature enabled on it.

BranchCache can operate in one of two modes:

- **Distributed Cache** uses peer to peer architecture. Distributed Cache is beneficial for branch offices that do not have a local server.
- **Hosted Cache** uses a client/server architecture, Client computers cache contents to a computer on the local network running Windows Server 2008, which is known as the Hosted Cache. Other clients who need the same content can retrieve it directly from the Hosted Cache. The Hosted Cache computer can run Windows Server 2008 and can also host other applications.

Hosted Cache Mode:

The Hosted Cache is a repository of data which has been downloaded from BranchCache enabled servers in the branch office by BranchCache enabled clients. Hosted Cache mode does not need a dedicated server. The BranchCache feature can be enabled on any server with Windows Server 2008 R2, which is located in a branch.vBranchCache can be set up as a virtual workload and run on a server simultaneously with other workloads, such as File and Print.

Hosted Cache mode uses the following process to cache and retrieve data:

1. The Windows 7 client connects to the content server and requests a file in the similar way when files are retrieved without BranchCache.
2. The content server authorizes and authenticates the client. If the process of authentication and authorization is successful, it returns content metadata over the same channel from which data would have been sent.
3. The client uses the hashes in the metadata for searching the file. As this is the first time any client has retrieved the file, therefore it is not already cached on the local network and the client retrieves the file directly from the content server.
4. The client establishes a Secure Sockets Layer (SSL) connection with the Hosted Cache server, and also offers the content identifiers over this encrypted channel.
5. The Hosted Cache server connects to the client and retrieves the set of those blocks that it does not have cached.
6. When another Windows 7 client requests the same file from the content server. The content server again authorizes the user and sends content identifiers.
7. The client uses these identifiers for requesting the data from the Hosted Cache server. The Hosted Cache server encrypts the data and then sends it to the client. The data is encrypted with a key that is derived from the hashes sent by the content server with the content metadata.
8. The client decrypts the data, and ensures that it is identical to the block hashes that the content server provided with the content metadata. It ensures that the content has not been modified.

Distributed Cache Mode:

In this mode, Windows 7 clients retrieve the cache contents by the WAN, then send that content directly to other authorized Windows 7 clients whenever requested. Distributed Cache mode is best for branch offices with less than 50 users.

The first client to retrieve content from a content server by using the WAN becomes the source for that content in the branch for other clients requesting the same content. When another client requests the same content, it downloads only the content metadata from the content server and sends a request for the segment hashes on the local network to determine if some other client already has the cached data. Then the second client retrieves the content locally from the client that has the content data.

This process is similar to the process used by the Hosted Cache mode, but the requests for cached content are sent to the local network and a Hosted Cache server is not required.

Distributed Cache mode uses the following process to cache and retrieve data:

1. The Windows 7 client connects to the content server and requests a file in the similar way when files are retrieved without BranchCache.

2. The content server authorizes and authenticates the client, and the server sends an identifier that is client used by client to search for the file on the local network. Whenever any client attempts to retrieve the file for the first time, it is not cached on the local network. So, the client retrieves the file directly from the content server and caches it.
3. When another client requests the same file from the content server, then it authenticates and authorizes the user in the similar way it would have done if BranchCache was not being used. If the process of authentication and authorization is successful, it returns content metadata over the same channel that data would normally have been sent.
4. The other client sends a request on the local network for the required file by using the Web Services Discovery (WS-Discovery) multicast protocol.
5. The client that cached the file earlier sends the file to the requesting client. The data is encrypted with a key which is derived from the hashes sent by the content server with the content metadata.
6. The client decrypts the data by computing the hashes on the blocks received from the first client, and ensures that it is similar to the block hashes provided with content metadata by the content server. It ensures that the content has not been modified.

BranchCache improves the performance of applications that use one of the following protocols:

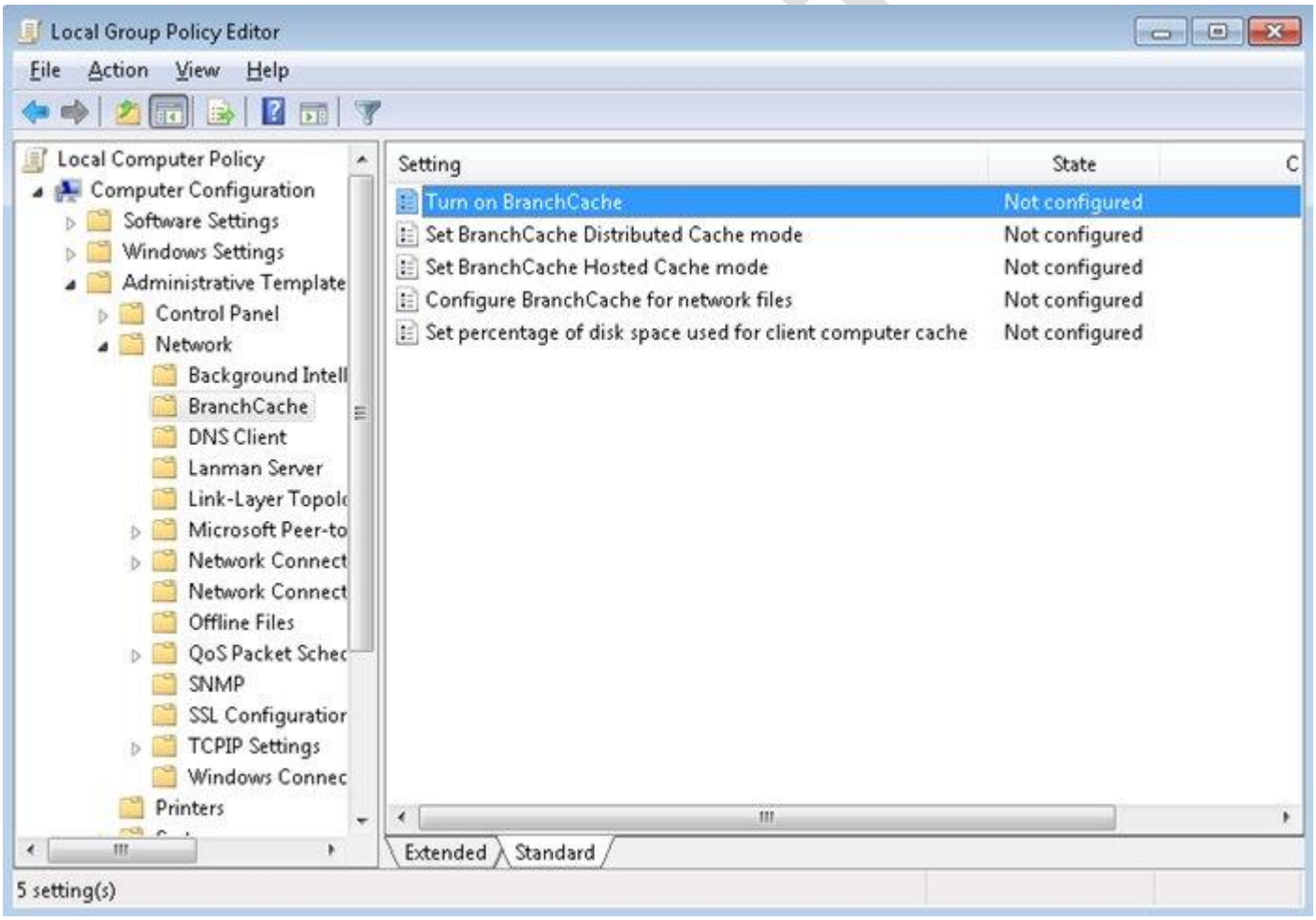
- HTTPS and HTTP. The protocols used by Web browsers and many other applications, such as Internet Explorer or Windows Media, among others.
- SMB (including signed SMB traffic). The protocol used for shared folders.

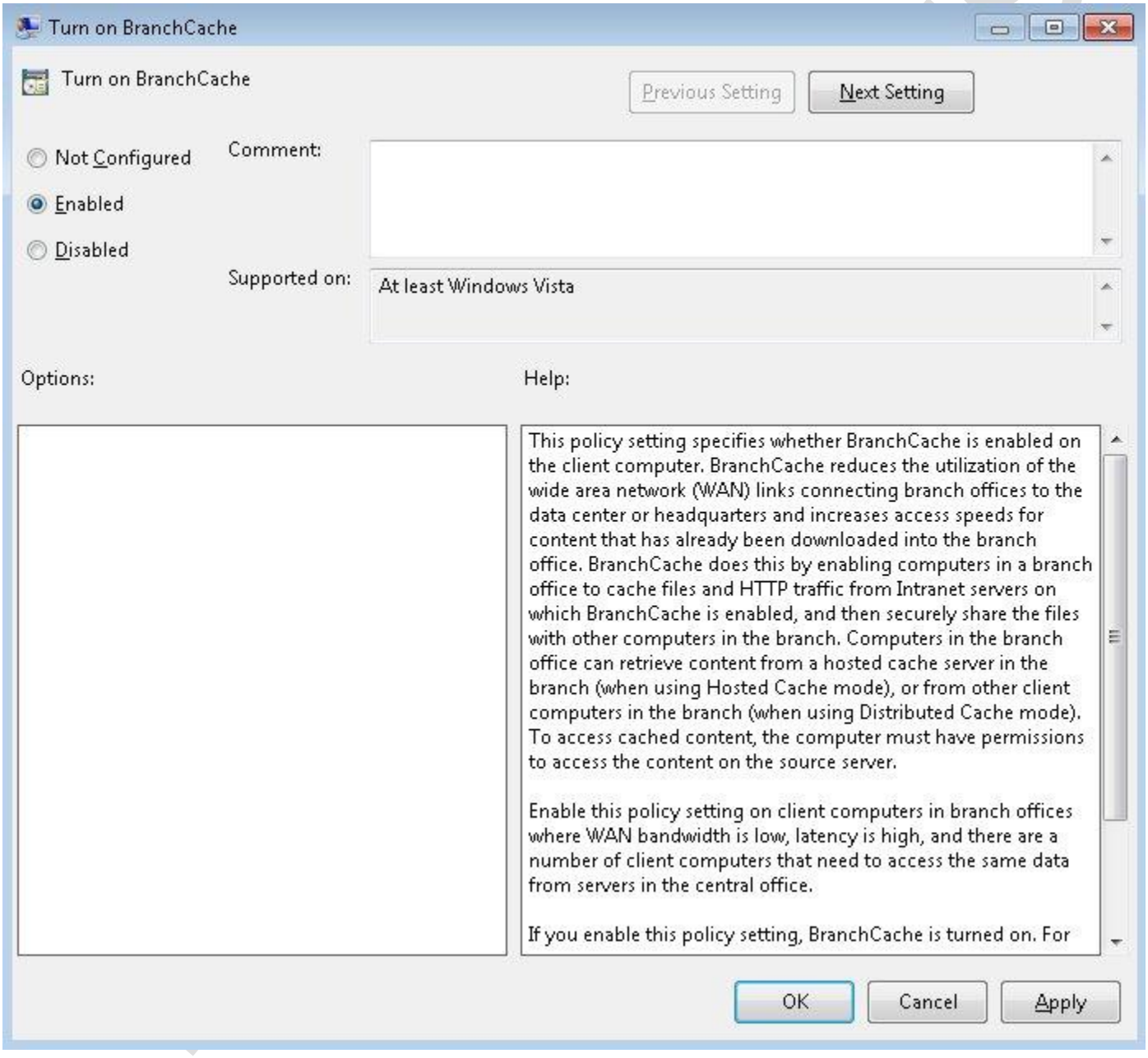
BranchCache only retrieves data from a server when the client requests it. As it is a passive cache, it does not increase WAN utilization. BranchCache only caches read requests and does not interferes with a user saving a file.

BranchCache Client Configuration:

On the Windows 7 Client you need to configure the GPO by editing the settings in the MMC. Follow these steps to configure Branchcache on Windows 7 Computer:

1. Click *Start*, and type *Group Policy* in the search box then click *Edit Group Policy*.
2. Click *Administrative Templates* in the *Computer Configuration* section in the left pane.
3. Click *Network*, and then click *Branch Cache*.
4. You can enable various options in the Branch cache, by double clicking the option and selecting *enable*.





If you are using Distributed Cache, enable *Turn on BranchCache* and then turn on *Set BranchCache Distributed Cache Mode*. If you are using hosted cache mode you will need to enable *Turn on BranchCache* and enable *Set BranchCache Hosted Cache mode*. Optionally, you can also set other values using this set of GPOs, like latency values or setting a percentage of your disk space dedicated to this cache. When you use Group Policy or local computer policy settings to enable BranchCache, the correct firewall exceptions are automatically created to allow BranchCache traffic.

Importing the BranchCache Certificate on Client Computers:

You can use the following steps to import the BranchCache certificate into the Trusted Root Certification Authorities certificate store for the local computer on each BranchCache client computer. To perform these steps you should be a member of the Administrators group:

1. Click *Start* and in the search box type *mmc*.
2. Click *File*, and then click *Add/Remove Snapin*. The Add or Remove Snapins dialog box opens, click *Certificates*, and then click *Add*.
3. In the Certificates snap-in page, click *Computer account*, and then click *Next*.
4. In Select Computer, ensure that Local computer is selected, click *Finish* and then click *OK*. The Certificates snap-in is now added to the MMC.
5. In the MMC, double-click *Certificates (Local Computer)*, and then double-click *Trusted Root Certification Authorities*.
6. Click Certificates.
7. In the *Action* menu, click *All Tasks*, and then click *Import*. The Certificate Import Wizard is opened.
8. Click *Next*. click *Browse* in the File to import. In the Open dialog box, go to the folder location where you saved the BranchCache.cer file. Select the file and then click *Open*.
9. On the Certificate Import page, click *Next*.
10. In Certificate Store, ensure that *Trusted Root Certification Authorities* is selected, and then click *Next*.
11. Click *Finish*. An information dialog box opens and displays the message *The import was successful*. Click *OK*.

70-680 Study Guide - Configure BitLocker and BitLocker To Go

Introduction to BitLocker and BitLocker To Go:

The BitLocker feature of Windows 7 is available only in Ultimate and Enterprise edition of Windows 7. This feature enhances the security of the data on your computer by encrypting the entire drive which contains your data and Windows. Once you turn on BitLocker service on a drive, any file that you save on that drive is encrypted automatically. This means that if a computer is stolen, the data cannot be recovered unless the thief also has the password to the system. This helps companies keep sensitive data from falling into the wrong hands when a computer is stolen, and also makes hard drive disposal much easier.

BitLocker To Go is also a security enhancement mechanism offered by Windows 7 which gives the lockdown treatment to easily-misplaced portable storage devices like external hard drives and USB flash drives.

BitLocker Drive Encryption can use a Trusted Platform Module (TPM) to validate the integrity of a computer's

boot manager and boot files at startup, and to guarantee that a computer's hard disk has not been tampered with while the operating system was offline. To encrypt the drive on which you have installed Windows, BitLocker stores its own encryption and decryption key in a hardware device that is separate from your hard disk. Therefore to use BitLocker service on your computer, it must have one of the following:

- For BitLocker to use the system integrity check provided by a TPM, the computer must have a TPM version 1.2. If your computer does not have a TPM, enabling BitLocker will require you to save a startup key on a removable device such as a USB flash drive.
- A computer with a TPM must also have a Trusted Computing Group (TCG)-compliant BIOS. The BIOS establishes a chain of trust for pre-operating system startup and must include support for TCG-specified Static Root of Trust Measurement. A computer without a TPM does not require a TCG-compliant BIOS.
- The system BIOS (for TPM and non-TPM computers) must support the USB mass storage device class, including reading small files on a USB flash drive in the pre-operating system environment.

In order to enable BitLocker Drive Encryption on the operating system drive, your computer's hard disk must meet the following requirements:

- Your computer's hard disk must have at least two partitions: the operating system partition and the active system partition. The operating system partition is that partition where you have installed Windows and it will be encrypted. The active system partition is left unencrypted so that the computer can be started, and this partition must be at least 100 MB in size. In Windows 7, by default, the system partition is not assigned a drive letter and is hidden from the user. If your computer does not have a separate, active partition, the required partition is created during BitLocker setup.
- Both the partitions, the operating system and active system partitions must be formatted with the NTFS file system.
- The BIOS must be compatible with the TPM or should support USB devices during computer startup.

BitLocker can encrypt the computer's data drives and removable data drives like external hard drives and USB flash drives. For encryption, a data drive must be formatted by using the FAT, FAT16, FAT32, or NTFS file system and must be at least 64 MB in size.

BitLocker is similar to EFS, but there are some important differences as shown in the table below:

BitLocker	**EFS**
Encrypts all files on the drive that Windows is installed on.	Encrypts selected files on any drive.
BitLocker is either on or off for all users or groups.	Encrypts files associated with the user account that configured EFS. If a computer has multiple users, each can encrypt their own files.
Uses the Trusted Platform Module (TPM), a special chip in some computers that supports advanced security features.	Does not require or use any special hardware.
You must be an administrator to turn BitLocker encryption on or off after it is enabled.	You do not have to be an administrator to use EFS.

BitLocker Modes:

- **TPM-only mode** - In this mode, the user is unaware that BitLocker is in effect and they do not have to provide a password, PIN, or startup key to start the computer. TPM-only mode is the least secure implementation of BitLocker because it does not require additional authentication.
- **TPM with startup key** - This mode requires that a USB device hosting a preconfigured startup key be available to the computer before the computer can boot into Microsoft Windows. If the device hosting the startup key is not available at boot time, the computer automatically enters recovery mode. This mode also provides boot environment protection via the TPM.
- **TPM with PIN** - In this mode, the user must enter a PIN before the computer boots. You can configure Group Policy so that it is possible to enter a password containing numbers, letters, and symbols rather than a simple PIN number. If you do not enter the correct PIN or password at boot time, the computer automatically enters recovery mode. This mode also provides boot environment protection through the TPM.
- **TPM with PIN and startup key** - This is the most secure option. You can configure this option through Group Policy. When you enable this option, a user must enter a startup PIN and have the device hosting the startup key connected before the computer will boot into Windows 7. This mode also provides boot environment protection through the TPM.
- **Without TPM** - This mode provides hard disk encryption but does not provide boot environment protection. This mode is used on computers without TPM chips. You can configure BitLocker to work on a computer that does not have a TPM chip by configuring the Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives\Require Additional Authentication At Startup policy. When you configure BitLocker to work without a TPM chip, you need to boot with a startup key on a USB storage device.

Do I have TPM Hardware:

Before configuring BitLocker, you will want to know if your computer has TPM hardware. To find out, follow these steps:

1. Click the *Start* button, then *Control Panel*.
2. Click *Security*, and then click *BitLocker Drive Encryption*. (If you do not see BitLoker Drive Encryption as an option, the most likely reason is that you are not running the Ultimate or Enterprise edition of Windows 7).
3. If the *TPM administration* link appears in the left pane, your computer has the TPM security hardware. If the link is not there, you will need a removable USB device such as a flash drive to turn on BitLocker and store the BitLocker startup key.

If the TPM Administration link is available, clicking on it will allow you to store TPM recovery information in Active Directory Domain Services (AD DS), clear the TPM, reset the TPM lockout, and enable or disable the TPM.

Configuring BitLocker:

Follow these steps to configure BitLocker:

1. Open the BitLocker Drive Encryption control panel following the instructions in the section directly above. This screen presents a list of all the drive partitions under Help protect your files and folders by

encrypting your drives. You can choose the drive that you want to encrypt with BitLocker. Let's suppose you choose drive D.
2. Select the *Turn On BitLocker* link next to the volume description of drive D.
3. Select the method you want to use to unlock your protected drive. You can choose between password unlocking, unlocking using a smart card or you can also select to unlock automatically. Let's suppose you choose to unlock with password. Then select *Use a password to unlock this drive* checkbox, enter the password and click *Next*.
4. On the *How do you want to store your recovery key* page, select an appropriate option. If you select *print the key*, you can take out the printout. If you select to store it on a file you'll get the key in a file with xps extension. Selecting the option to *store the key on a USB drive*, you need to insert the drive and will get the key on that. Click *Next*.
5. On Encrypt the drive page, click *Start Encrypting*. It encrypts your drive.
6. You can now manage your encrypted drive from BitLocker Drive Encryption page, mentioned in Step no. 2. For drive D, you'll observe certain options next to your BitLocker controlled drive: *Turn Off BitLocker* and *Manage BitLocker*. You can change or remove the password, or can also change the method to unlock the encrypted drive to Smart Card unlocking.

If you selected *Use a password to unlock this drive*, when you try to access your drive, you will receive a password prompt to unlock the drive. If you selected the smart card option, you will be prompted to insert the smart card.

Configuring BitLocker To Go:

1. Connect the USB drive for which you want to enable BitLocker Encryption.
2. Click *Start*, then click *Control Panel*.
3. Click *System and Security*, then click *BitLocker Drive Encryption*. This screen presents a list of all the drive partitions and the connected USB flash drive under Help protect your files and folders by encrypting your drives.
4. Click the *Turn On BitLocker* link option next to the volume description for the USB drive. It starts the initialization process of BitLocker Drive Encryption.
5. Select the method you want to use to unlock your protected drive. You can choose between password unlocking or unlock using a smart card. Lets suppose you choose to unlock with password. Then select *Use a password to unlock this drive* checkbox, enter the password and click *Next*.
6. On How do you want to store your recovery key page, select an appropriate option. If you select print the key, you can take out the printout. If you select to store it on a file you'll get the key in a file with xps extension, and prompts you for the location to save the file. Click *Next*.
7. On Encrypt the drive page, click *Start Encrypting*. It encrypts your drive.
8. You can now manage your encrypted drive from BitLocker Drive Encryption page, mentioned in Step no. 3. For your encrypted USB flash drive, you'll observe certain options next to your BitLocker controlled drive: Turn Off BitLocker and Manage BitLocker. You can change or remove the password, or can also change the method to unlock the encrypted drive to Smart Card unlocking.

BitLocker Data Recovery Agents:

Data Recovery Agents are special user accounts that can be used to recover encrypted data. You can configure such an account to recover BitLocker-protected drives if the recovery password or keys are lost. Data Recovery Agents can be used across an entire organization, meaning that you can recover all BitLocker-encrypted volumes using a single account rather than having to recover a specific volume's recovery password or key.

Before a data recovery agent can be configured for a drive, you must add the data recovery agent to Public Key Policies\BitLocker Drive Encryption in either the Group Policy Management Console (GPMC) or the Local Group Policy Editor. You must also enable and configure the Provide the unique identifiers for your organization policy setting to associate a unique identifier to a new drive that is enabled with BitLocker. An identification field is a string that is used to uniquely identify a business unit or organization. Identification fields are required for management of data recovery agents on BitLocker-protected drives. BitLocker will only manage and update data recovery agents when an identification field is present on a drive and is identical to the value configured on the computer.

To assign a BitLocker identification field to a BitLocker-protected drive follow given steps:

1. Log on as an administrator to the computer where you want to assign the identification field.
2. Click *Start*, type *cmd* in the Search programs and files box.
3. At the command prompt, type the following command, replacing [drive letter] with the BitLocker-protected drive's identifier (for example, E:): *manage-bde -SetIdentifier [drive letter]*
4. The Manage-bde command-line tool will set the identification field to the value specified in the Provide the unique identifiers for your organization Group Policy setting.
5. After the value has been set, Manage-bde will display a message informing you that the drive identifier has been set.

To configure an identification field:

1. Click *BitLocker Drive Encryption* in the GPMC or Local Group Policy Editor under *Computer Configuration\Administrative Templates\Windows Components*, to show the policy settings.
2. Double-click the *Provide the unique identifiers for your organization* policy setting in the details pane.
3. Click *Enable*. In BitLocker Identification Field, enter the identification field for your organization. This would be the identifier configured in the steps above.
4. Click *OK* to apply and close the policy setting.

To configure a data recovery agent:

1. Open GPMC or the Local Group Policy Editor.
2. In the console tree under Computer Configuration\Windows Settings\Security Settings\Public Key Policies, right-click *BitLocker Drive Encryption*.
3. Click *Add Data Recovery Agent* to start the Add Recovery Agent Wizard. Click *Next*.
4. On the Select Recovery Agents page, click *Browse Folders*, and select a.cer file to use as a data recovery agent. After the file is selected, it will be imported and will appear in the Recovery agents list in the wizard. Multiple data recovery agents can be specified. After you have specified all the data recovery agents that you want to use, click *Next*.
5. The Completing the Add Recovery Agent page of the wizard displays a list of the data recovery agents that will be added to the Group Policy. Click *Finish* to confirm the data recovery agents, and close the wizard.

70-680 Study Guide - Configure DirectAccess

Introduction to DirectAccess:

DirectAccess is a new feature in the Windows 7 and Windows Server 2008 operating systems that provides users the connectivity to their corporate network any time they have Internet access. When DirectAccess is enabled, requests for corporate resources such as e-mail servers, shared folders, or intranet Web sites etc are securely directed to the corporate network, without requiring the users to connect to a virtual private network (VPN). DirectAccess provides increased productivity by offering the same connectivity experience both inside and outside of the office. Without DirectAccess, mobile computers can only be managed when users connect to a VPN or are physically inside the office. With DirectAccess you can now manage the mobile computers by updating Group Policy settings and distributing software updates any time the mobile computer has Internet connectivity, even when the user is not logged on. By using technologies such as Internet Protocol version 6 (IPv6) and Internet Protocol security (IPsec), DirectAccess provides secure and flexible network infrastructure for enterprises. Following are the security and performance capabilities of the direct access:

- **Better authentication:** DirectAccess authenticates the computer and enables it to connect to the intranet before the user logs on and can also authenticate the user and supports two-factor authentication using smart cards.
- **Encryption:** DirectAccess uses IPsec to provide encryption for communications over the Internet.
- **Better access control:** Computer support professionals can configure the intranet resources differently for users. It allows individual users or a group of users access and use specific applications, servers or even subnets.
- **Simplification and Cost Reduction:** DirectAccess separates intranet from Internet traffic, which reduces unnecessary traffic on the corporate network, as it sends only the traffic destined for the corporate network through the DirectAccess server.

DirectAccess resolves the limitations of VPNs by automatically establishing a bi-directional connection from the client computers to the corporate network. DirectAccess uses two technologies: Internet Protocol security (IPsec) and Internet Protocol version 6 (IPv6).

DirectAccess uses IPsec for providing encryption for communications across the Internet. Clients can establish an IPsec tunnel for the IPv6 traffic to the DirectAccess server, which works as a gateway to the intranet.

DirectAccess clients uses the following process to connect to intranet resources:

- A computer running Windows 7 Enterprise or Windows 7 Ultimate operating system detects that it is connected to a network.
- The DirectAccess client computer attempts to connect to an intranet website specified during DirectAccess configuration.
- The DirectAccess client computer connects to the DirectAccess server using IPv6 and IPsec. If a native IPv6 network is not available then the client uses 6to4 or Teredo to send IPv4-encapsulated IPv6 traffic.
- If a firewall or proxy server prevents the client computer that is using 6to4 or Teredo from reaching the DirectAccess server, the client automatically attempts to connect by using the Internet Protocol over Secure Hypertext Transfer Protocol (IP-HTTPS) protocol. IP-HTTPS uses a Secure Sockets Layer (SSL) connection to encapsulate IPv6 traffic.

- As part of establishing the IPsec session for the tunnel to reach the intranet DNS server and domain controller, the DirectAccess client and server authenticate each other using computer certificates for authentication.
- If Network Access Protection (NAP) is enabled and configured for health validation, then DirectAccess client obtains a health certificate from the Health Registration Authority (HRA) that is located on the Internet before connecting to the DirectAccess server. The HRA then forwards the DirectAccess client's health status information to a NAP health policy server. The NAP health policy server processes the policies that are defined within the Network Policy Server (NPS) and determines whether the client satisfies the system health requirements. If it satisfies, the HRA obtains a health certificate for the DirectAccess client. When the DirectAccess client establishes the connection with DirectAccess server, it submits its health certificate for authentication.
- When the user logs on, the DirectAccess client establishes the second IPsec tunnel to access the resources of the intranet. The DirectAccess client and server authenticate each other using a combination of computer and user credentials.
- The DirectAccess server forwards traffic to and from the DirectAccess client and the intranet resources to which the user has been granted access.

DirectAccess clients get their configuration through Group Policy. This Group Policy is filtered so that it only applies to computers that are members of specific DirectAccess security groups. The policies that apply through this filtering are located in the Computer Configuration\Administrative Templates\TCPIP Settings\IPv6 Transition Technologies node.

DirectAccess Requirements:

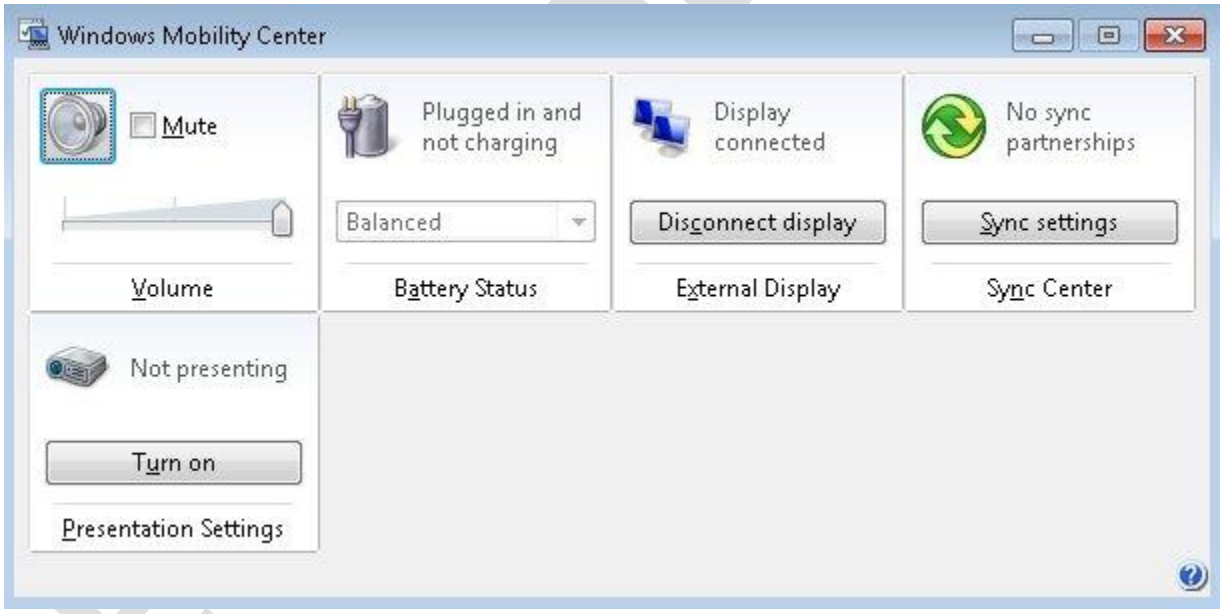
DirectAccess requires the following:

- One or more DirectAccess servers running Windows Server 2008 R2 with two network adapters: one of them should be directly connected to the Internet and other should be connected to the intranet. DirectAccess servers should be a member of an AD DS domain.
- On the DirectAccess server, there should be two consecutive public IPv4 addresses assigned to the network adapter that is connected to the Internet.
- DirectAccess client computers running Windows 7 Enterprise or Windows 7 Ultimate. DirectAccess clients should be members of an AD DS domain.
- At least one domain controller and DNS server should be running Windows Server 2008 SP2 or Windows Server 2008 R2.
- A public key infrastructure (PKI) should be there to issue computer certificates, smart card certificates for smart card authentication, and health certificates for NAP.
- DirectAccess with UAG provides a built-in NAT64, but DirectAccess without UAG, an optional NAT64 device can be used to provide access to IPv4-only resources for DirectAccess clients.

70-680 Study Guide - Configure Mobility Options

Windows Mobility Center:

Windows Mobility Center is a component that centralizes important information to mobile computing. Mobility center enables you to access various settings like speaker volume, wireless network connection status, and display brightness in a quick and efficient manner. The Windows Mobility Center feature is available on laptops, notebooks, and tablet PCs by default. It is not available on desktop computers unless you enable it manually. But this feature is not available in the Windows 7 Starter edition. Presentation settings in Windows Mobility Center are not available in Windows 7 Home Premium edition and are only available in Windows 7 Ultimate, Professional, and Enterprise editions.



Configuring Windows Mobility Center Options:

1. Click *Start*, and then click *Control Panel*.
2. Click *Windows Mobility Center*, and if you cannot locate this link in Control panel, then type *Windows Mobility Center* in the search box of control panel. Then click the link *Windows Mobility Center*.

Windows Mobility Center displays the commonly used settings, such as brightness, volume, battery status, and wireless network status. Different tiles containing these settings are displayed depending on your system, and

your laptop manufacturer. If a setting doesn't appear, the possible reason may be that the required hardware, such as a wireless network adapter, or driver is missing or turned off. For example, if the Turn wireless on button is not available, you might have to use the hardware switch on your computer to first turn on the wireless adapter.

Following are some settings that you find in Mobility Center but all the settings might not be available on all laptops:

- **Brightness** - You can move the slider to temporarily adjust the brightness of your display. To adjust the display brightness settings for your power plan, you need to click the icon to open Power Options.
- **Volume** - You can move the slider to adjust the speaker volume of your laptop, or select Mute check box to turn off the volume temporarily.
- **Battery Status** - This displays how much charge remains on your battery or you can also change or select a power plan from the list for your computer.
- **Wireless Network** - This displays the status of your wireless network connection or it can be used to turn your wireless network adapter on or off.
- **Screen Rotation** - This changes the orientation of your PC screen from portrait to landscape, or vice versa.
- **External Display** - This can be used when you want to connect an external monitor to your laptop, or customize the display settings.
- **Sync Center** - It displays the status of an in-progress file sync, you can start a new sync, setup a sync partnership, or can also change your settings in Sync Center.
- **Presentation Settings** - With this setting you can connect your laptop to a projector. Click Turn on to display a presentation from your computer. With this option laptop stays awake, and system notifications are turned off.

Offline Files:

Using offline files, provides access to files stored in shared network folders even when the network copies are unavailable. This can be done by choosing the network files you want to make available offline, which automatically creates a copy of the network files on your computer. These copies of network files that are stored on your computer are called offline files. Windows will automatically sync your offline files when connected to the network, and open the local copies of the files whenever the network versions are unavailable. In a nutshell, offline files provide access to files on a network share when they are unavailable, provide faster access when you have a slow network connection, and allow you to work with files when away from the network.

By default, offline files are enabled on the following versions of Windows 7: Windows 7 Professional, Windows 7 Enterprise, and Windows 7 Ultimate.

Syncing Offline Files:

This process is automated, however, below is more information about the process:

- If you are working offline and make changes to offline files from a network folder, Windows will automatically sync any changes you made to the files the next time you connect to that network folder.
- If you are working offline while someone else changes files in a shared network folder, Windows will sync those changes with the offline files on your computer the next time you connect to that network folder. If you have also changed the files since you last connected to the network folder, a sync conflict

will occur and Windows will ask you which version you want to keep. You can resolve these and other sync conflicts by using Sync Center.

- If Windows encounters a problem when trying to sync offline files between your computer and a network folder (for example, if the network folder you are trying to sync with is unavailable), a sync error will occur.

You can manually sync files - more on this below.

Configuring Offline Files:

To turn offline files off and on, as well as configure other options, follow these steps:

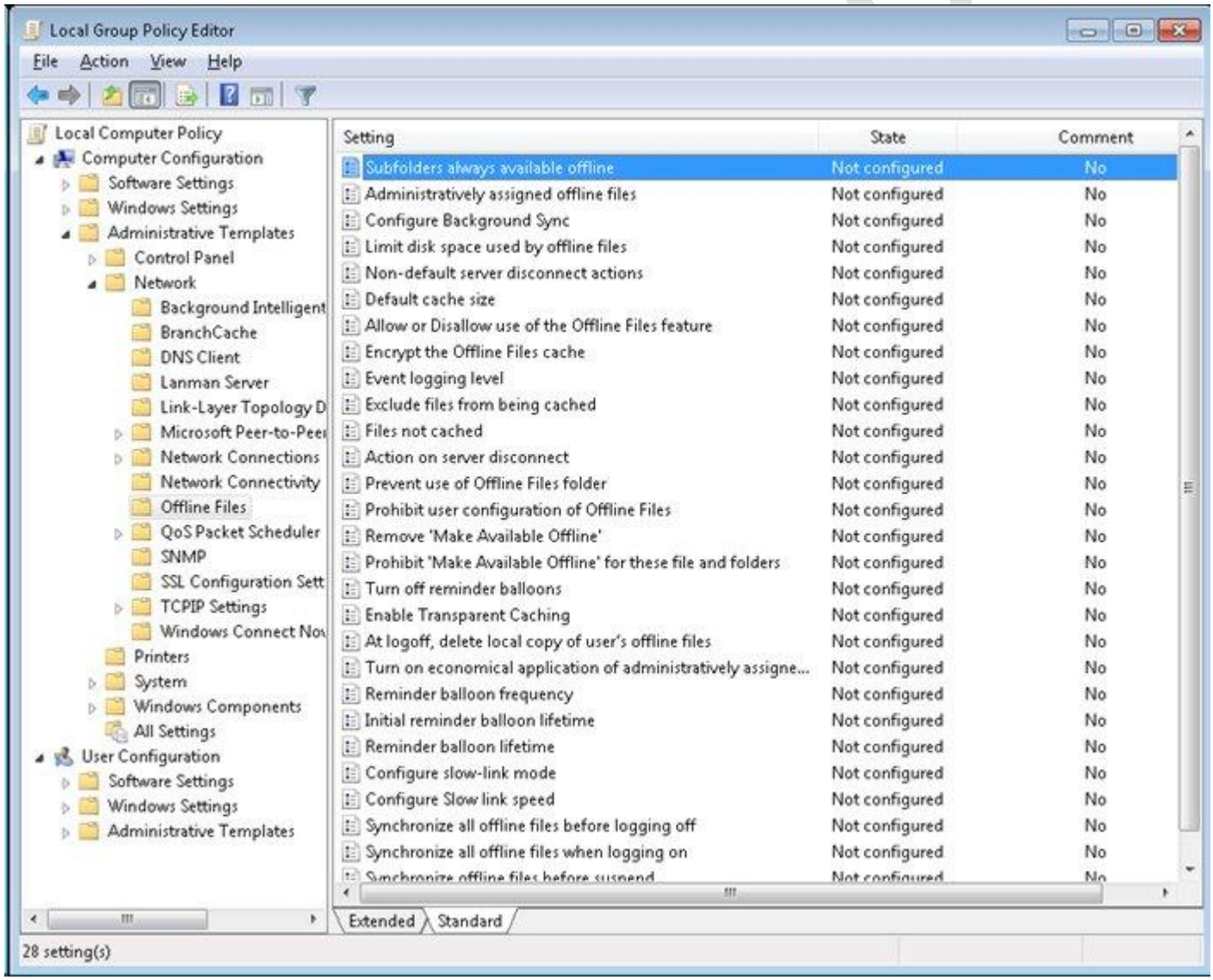
1. Click *Start* and enter *Offline Files* into the search box.
2. Click *Manage Offline Files* and you will see the window shown below.

3. The following describes the various tabs and options available.
    - **General** - Turn offline files on and off, open the Sync Center, and view offline files.
    - **Disk Usage** - Allows you to view and configure the amount of disk space used by offline files, as well as delete them.
    - **Encryption** - This encrypts your files with EFS. This can help safeguard your files in case your computer is ever lost or stolen.
    - **Network** - This tab allows allows you to use offline files if a slow connection is discovered and the amount of time between checks. Enabled by default.

A user can make a file available offline by right-clicking the file and then clicking the *Always Available Offline* option.

Configuring Offline Files With Group Policy:

You configure Offline Files through Offline Files policies, located in the *Computer Configuration\Administrative Templates\Network\Offline Files* node of a Group Policy Object. There are 28 policies that can be configured here.



The following tables explains the group policy settings available for offline files. Note: the bolded titles are the ones you will most likely need to know for the exam.

Group Policy Setting	Description
Subfolders always available offline	Makes subfolders available offline whenever their parent folder is made available offline.
Administratively assigned offline files	Allows the administrator to specify files and folders available offline to users of the computer. To assign a file or folder, click Show and then click Add. In the Type the name of the item to be added box, type the fully qualified UNC path.
Configure Background Sync	This machine-specific policy is in effect when a network folder is determined to be in “slow-link” mode. For network folders in "slow-link" mode, a sync will be initiated in the background on a regular basis, according to the sync interval and variance settings configured here.
Limit disk space used by offline files	This policy limits the amount of the computer's disk space that can be used to store offline files.
Nondefault server disconnect actions	Determines how computers respond when they are disconnected from particular Offline Files servers. Administrators can enter the name of each server and specify whether users can work offline when disconnected from that server.
Default cache size	Limits percentage of a computer’s disk space that can be used to store automatically cached offline files. Does not affect disk space available for manually cached offline files.
Allow or Disallow use of the Offline Files feature	Determines whether Offline Files is enabled. Offline Files is enabled by default on Windows XP Professional–based client computers and is disabled by default on servers.
Encrypt the Offline Files cache	Determines whether offline files are encrypted in the cache on the local computer. Encrypting the offline cache enhances security on the local computer.
Event logging level	Determines which events the Offline Files feature records in the Event Log.
Exclude files from being cached	This policy enables administrators to exclude certain file types (by file extension) from being made available offline.
Files not cached	Allows you to exclude certain types of files from automatic and manual caching for offline use.
Action on server disconnect	Determines whether network files remain available if the computer is suddenly disconnected from the server hosting the files.
Prevent use of Offline Files folder	Disables the View Files button on the Offline Files tab. As a result, users cannot use the Offline Files folder to view or open copies of network files stored on their computer. Does not prevent users from working offline or from saving local copies of files available offline. Does not prevent them from using other programs, such as Windows Explorer, to view their offline files.
Prohibit user	Prevents users from enabling, disabling, or changing the configuration of Offline

configuration of Offline Files	Files. Administrators can configure other settings as they require, and then enable this setting to prevent users from making any changes, thus locking in a standard configuration.
Remove Make Available Offline	Prevents users from making network files and folders available offline. Removes the Make Available Offline option from the File menu and from all shortcut menus in Windows Explorer. Does not prevent the system from saving local copies of files that reside on network shares designated for automatic caching.
Prohibit "Make Available Offline" for these files and folders	Allows the administrator to specify files or folders that you do not want available offline. To assign a file or folder, click Show and then click Add. In the Type the name of the item to be added box, type the fully qualified UNC path.
Turn off reminder balloons	Reminder balloons appear above the Offline Files icon in the notification area to notify users when they have lost the connection to a networked file and are working on a local copy of the file. This setting hides or displays reminder balloons.
Enable transparent caching	Transparent Caching optimizes bandwidth consumption on WAN links and provides near local read response times for mobile users and branch office workers that are accessing network files and folders that are not explicitly made available offline. The greatest benefits of Transparent Caching are realized when BranchCache is deployed.
At logoff, delete local copy of user's offline files	Deletes local copies of the user's offline files when the user logs off. Caution: Files are not synchronized before they are deleted. Any changes to local files since the last synchronization are lost.
Turn on economical application of administratively assigned offline files	If you enable or do not configure this policy setting, only new files and folders in administratively assigned folders are synchronized at logon. Files and folders that are already available offline are skipped and are synchronized later. If you disable this policy setting, all administratively assigned folders are synchronized at logon.
Reminder balloon frequency	Determines how often reminder balloon updates appear (in minutes).
Initial reminder balloon lifetime	Determines how long the first reminder balloon for a network status change is displayed (in seconds).
Reminder balloon lifetime	Determines how long updated reminder balloons are displayed.
Configure slow link mode	This policy setting enables computers to use the slow-link mode of Offline Files (it is enabled by default for computers running Windows 7. This policy also controls when client computers running Windows 7 or Windows Server 2008 R2 transition to the slow-link mode.
Configure slow link speed	Configures the threshold value at which the Offline Files component considers a network connection to be slow, to prevent excessive synchronization traffic.
Synchronize all offline files before logging off	Determines whether offline files are fully synchronized when users log off.

Synchronize all offline files when logging on	Determines whether offline files are fully synchronized when users log on.
Synchronize all offline files before a suspend	Determines whether offline files are fully synchronized before a4:17 PM 6/26/2011 computer (such as a portable computer) enters suspend mode.

Resolving Sync Conflicts:

Sync conflicts can occur when changes are made to a file available offline both on the file server and within the local cache. For example, Bob makes a file called sales.doc available offline. Bob then makes changes to the file on his laptop while at home (offline file). Meanwhile, Joe works on sales.doc at the office. When Bob reconnects his laptop to the network, Sync Center notifies him that there is a sync conflict.

Windows 7 offers the Sync Center control panel for resolving these conflicts. To do this, click on *View Sync Conflicts* in the left pane of the Sync Center. This will display a list of files that have experienced a conflict. Click on *Resolve* and you will be presented with the following options:

- Keep the local version The version of the file that is stored on the local computer will be kept. This version overwrites the changed version of the file on the file share.
- Keep the server version The version of the file that is stored on the file share is kept, and the changes made to the local version are lost.
- Keep both versions The version on the local computer is renamed and then saved to the file share. The version of the file on the file share keeps the original name.

Power Management:

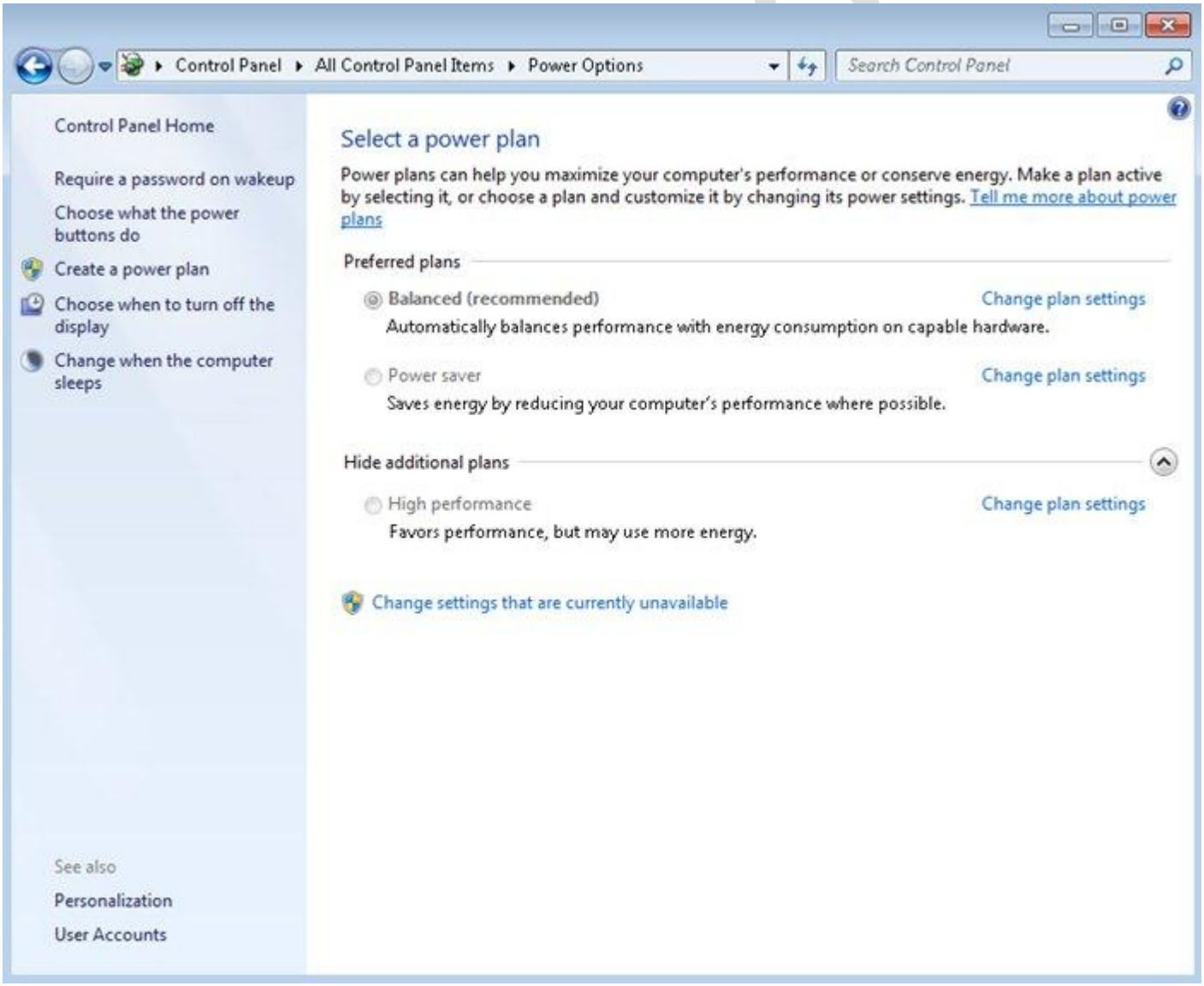
A power plan (formerly known as a power scheme in earlier versions of Windows) is a collection of hardware and system settings that manages how your computer uses and conserves power. You can use power plans to save energy, maximize system performance, or balance energy conservation with performance.

Windows 7 includes three default power plans as follows:

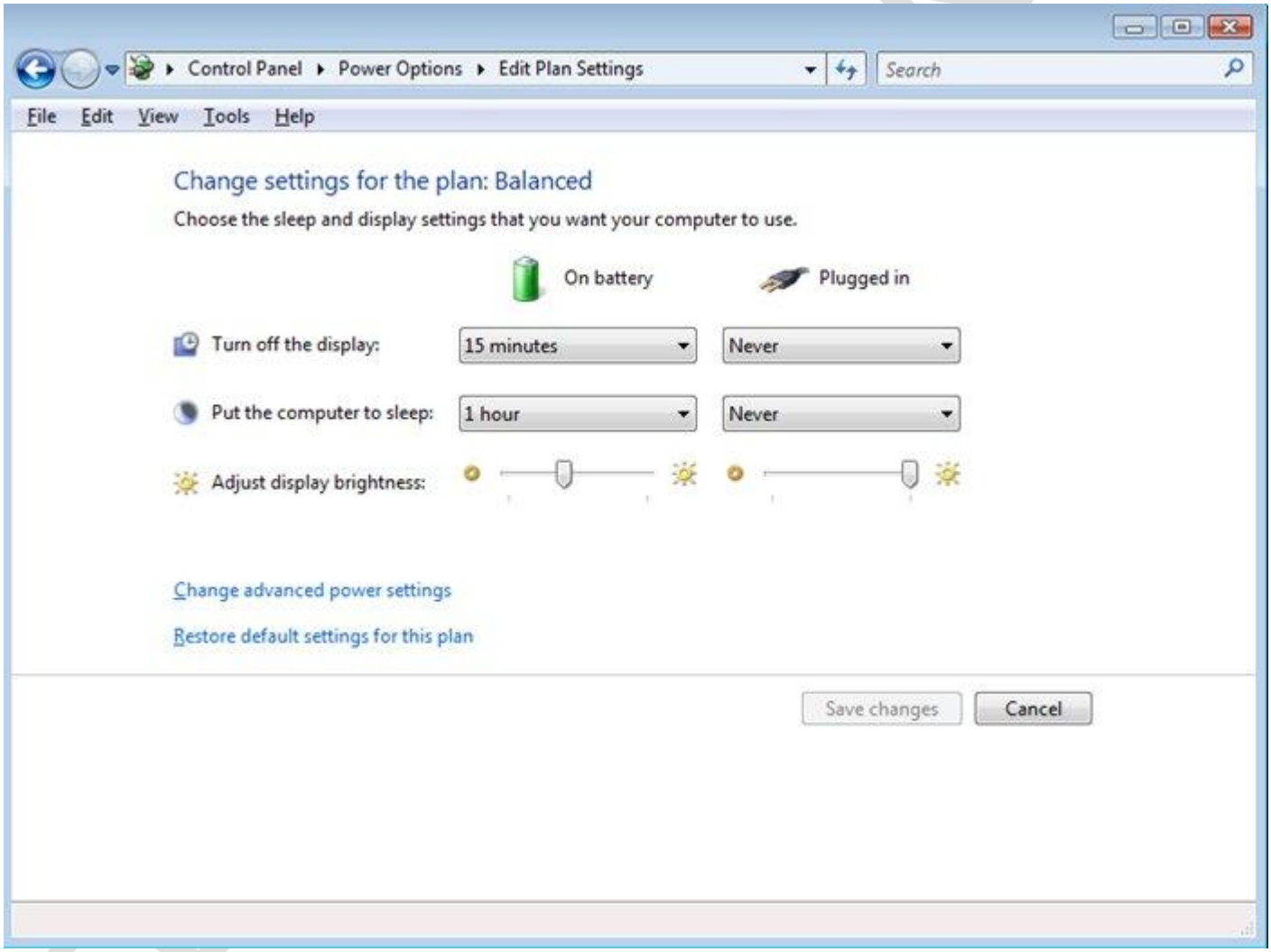
- **Balanced** - Offers full performance when you need it and saves power during periods of inactivity.
- **Power saver** - Saves power by reducing system performance. This plan can help mobile PC users get the most from a single battery charge.
- **High performance** - Maximizes system performance and responsiveness. Mobile PC users might notice that their battery doesn't last as long when using this plan.

To modify one of the existing plans follow the steps below:

1. Click the *Start* button, then *Control Panel*, and then *System and Security*. Next click *Power Options*.
2. Click *Change plan settings* next to the plan that you want to change.



3. Choose the display and sleep settings that you want to use when your computer is running on battery and when it's plugged in.



4. To change additional power settings, click *Change advanced power settings*. This will allow you to change settings for specific hardware.

You can also create a new plan following these steps:

1. Click the *Start* button, then *Control Panel*, and then *System and Security*. Next click *Power Options*.
2. Click *Create a plan* in the left pane.
3. Select the plan that is the closest to the type of plan that you want to create. Type a name for the plan and then click *Next*.
4. Choose the display and sleep settings that you want to use when your computer is running on battery and when it's plugged in and then click *Create*.

To further configure your new plan, follow the steps above for modifying an existing plan.

Sleep and Hibernate:

Sleep is a power-saving state that allows a computer to quickly resume full-power operation (typically within several seconds) when you want to start working again. Putting your computer into the sleep state is like pausing a DVD player: The computer immediately stops what it's doing and is ready to start again when you want to resume working.

Hibernation is a power-saving state designed primarily for laptops. While sleep puts your work and settings in memory and draws a small amount of power, hibernation puts your open documents and programs on your hard disk, and then turns off your computer. Of all the power-saving states in Windows, hibernation uses the least amount of power. On a laptop, use hibernation when you know that you won't use your laptop for an extended period and won't have an opportunity to charge the battery during that time.

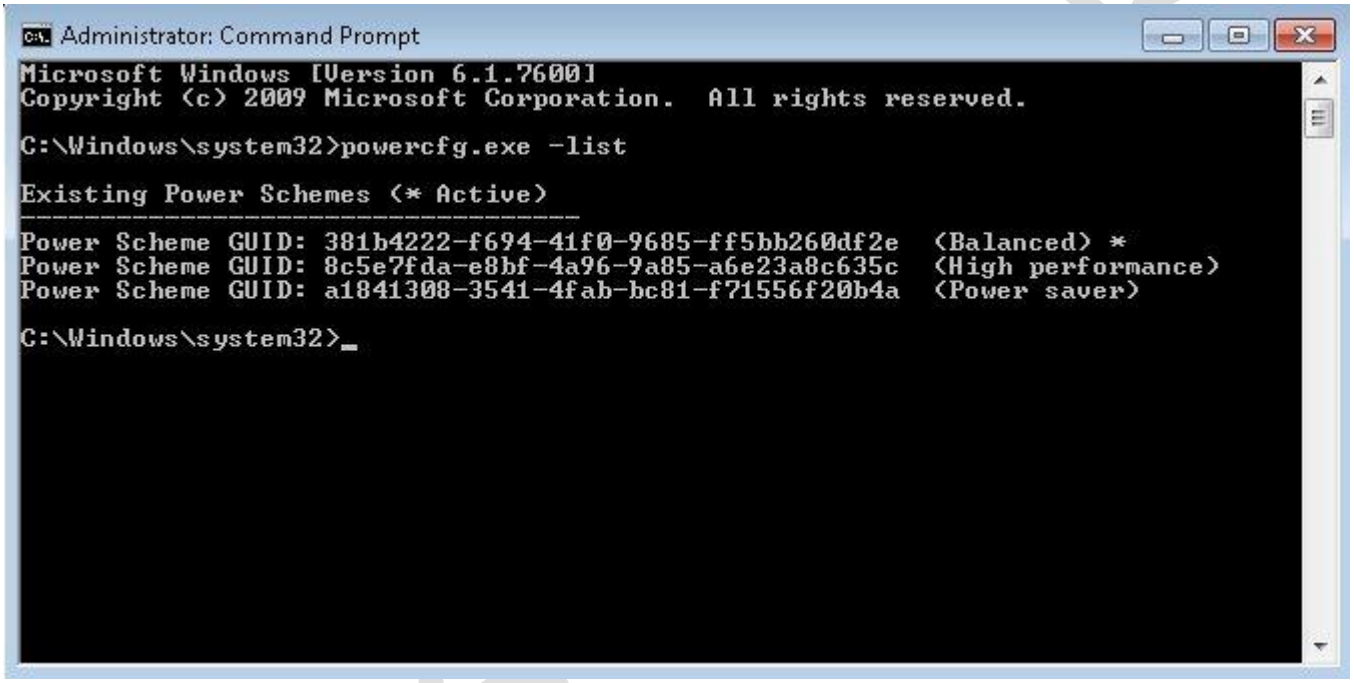
Hybrid sleep is designed primarily for desktop computers. Hybrid sleep is a combination of sleep and hibernate—it puts any open documents and programs in memory and on your hard disk, and then puts your computer into a low-power state so that you can quickly resume your work. That way, if a power failure occurs, Windows can restore your work from your hard disk. When hybrid sleep is turned on, putting your computer into sleep automatically puts your computer into hybrid sleep. Hybrid sleep is typically turned on by default.

These settings can also be configured from the Power Options control panel.

Exporting Power Plans:

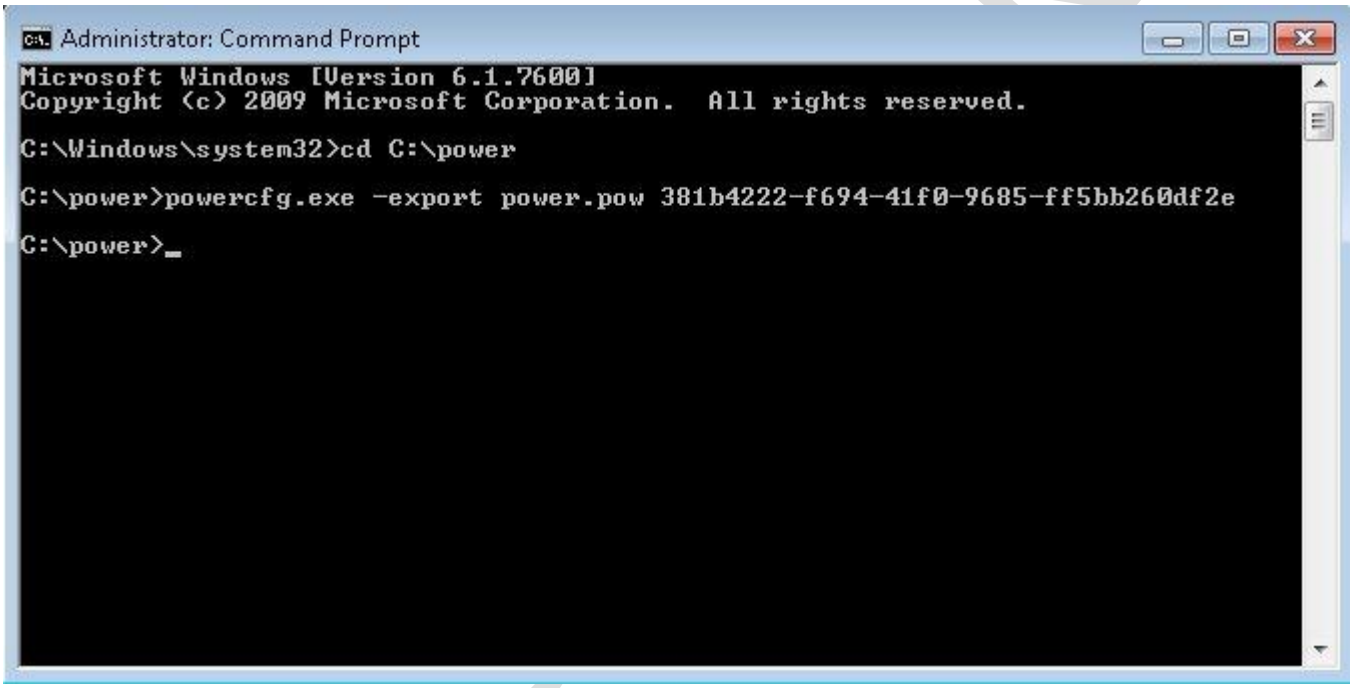
Powercfg.exe is a command line utility that can perform most of the power configuration tasks covered above. It can also do a couple of things that can't be done through the GUI such as exporting a power plan to be migrated to another computer. To do this, follow these steps:

1. At an elevated command prompt, type *powercfg.exe –list*. Record the GUID assigned to the plan you wish to export as you will need it later.



2. Create a directory to save the exported configuration. In this example, we are using *C:\power*. Change into this directory by typing *cd C:\power*.

3. Enter the command *powercfg.exe –export [filename].pow [GUID]*, where [filename] is the name of the exported file to be saved and [GUID] is the GUID of the power plan you are trying to export.



4. In this case, the file power.pow was saved to our C:\power folder. This file can be migrated to another computer and imported using the following command: *powercfg.exe -import [path to file]\power.pow*.

70-680 Study Guide - Configure Remote Connections

Introduction to VPNs:

A VPN is a network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network. A VPN works by using the shared public infrastructure while maintaining privacy through security procedures and tunneling protocols such as the Layer Two Tunneling Protocol (L2TP) or PPTP. In effect, the protocols, by encrypting data at the sending end and decrypting it at the receiving end, send the data through a "tunnel" that cannot be "entered" by data that is not properly encrypted.

Although not every edition of Windows 7 supports DirectAccess, every edition of Windows 7 supports VPN using the PPTP, L2TP/IPsec, SSTP, and IKEv2 protocols which are discussed below:

- **Point-to-Point Tunneling Protocol (PPTP)** - Based on PPP, the Point to Point Tunneling Protocol (PPTP) provides for the secure transfer of data from a remote client to a private server by creating a multi-protocol Virtual Private Network(VPN) which encapsulates PPP packets into IP datagrams. PPTP is considered to have weak encryption and authentication, therefore, IPsec is typically preferred.
- **Layer 2 Tunneling Protocol (L2TP) / IP security (IPsec):** - L2TP is the next-generation tunneling protocol partially based on PPTP. To provide encryption, L2TP acts as a data link layer (layer 2 of the OSI model) protocol for tunneling network traffic between two peers over an existing network (usually the Internet). It is common to carry Point-to-Point Protocol (PPP) sessions within an L2TP tunnel. L2TP does not provide confidentiality or strong authentication by itself. IPsec is often used to secure L2TP packets by providing confidentiality, authentication and integrity. The combination of these two protocols is generally known as L2TP/IPsec. IPSec ensures confidentiality, integrity, and authenticity of data communications across a public network. IPSEC is made of two different protocols: AH and ESP. AH (Authentication header) is responsible for authenticity and integrity, while ESP (Encapsulating Security payload) encrypts the payload.
- **Secure Socket Tunneling Protocol (SSTP)** - A tunneling protocol that uses the HTTPS protocol over TCP port 443 to pass traffic through firewalls and Web proxies that might block PPTP and L2TP/IPsec traffic. SSTP provides a mechanism to encapsulate PPP traffic over the Secure Sockets Layer (SSL) channel of the HTTPS protocol. The use of PPP allows support for strong authentication methods, such as EAPTLS. SSL provides transport-level security with enhanced key negotiation, encryption, and integrity checking.
- **Internet Key Exchange (IKEv2)** - IKEv2 is a tunneling protocol that uses the IPsec Tunnel Mode protocol over UDP port 500. An IKEv2 VPN is useful when the client moves from one wireless hotspot to another or when it switches from a wireless to a wired connection. The use of IKEv2 and IPsec provide strong authentication and encryption methods. Windows 7 is the first Microsoft operating system to support this protocol.

By default, the VPN type is set to Automatic. You can configure a connection to use a specific VPN protocol, but if you do this, Windows 7 does not try to use other VPN protocols if the protocol you select is not available. When a VPN connection type is set to Automatic, Windows 7 attempts to make a connection using the most secure protocol.

VPN Authentication Protocols:

Remote access in Windows 7 supports the authentication protocols listed in the following table. They are listed in order of increasing security.

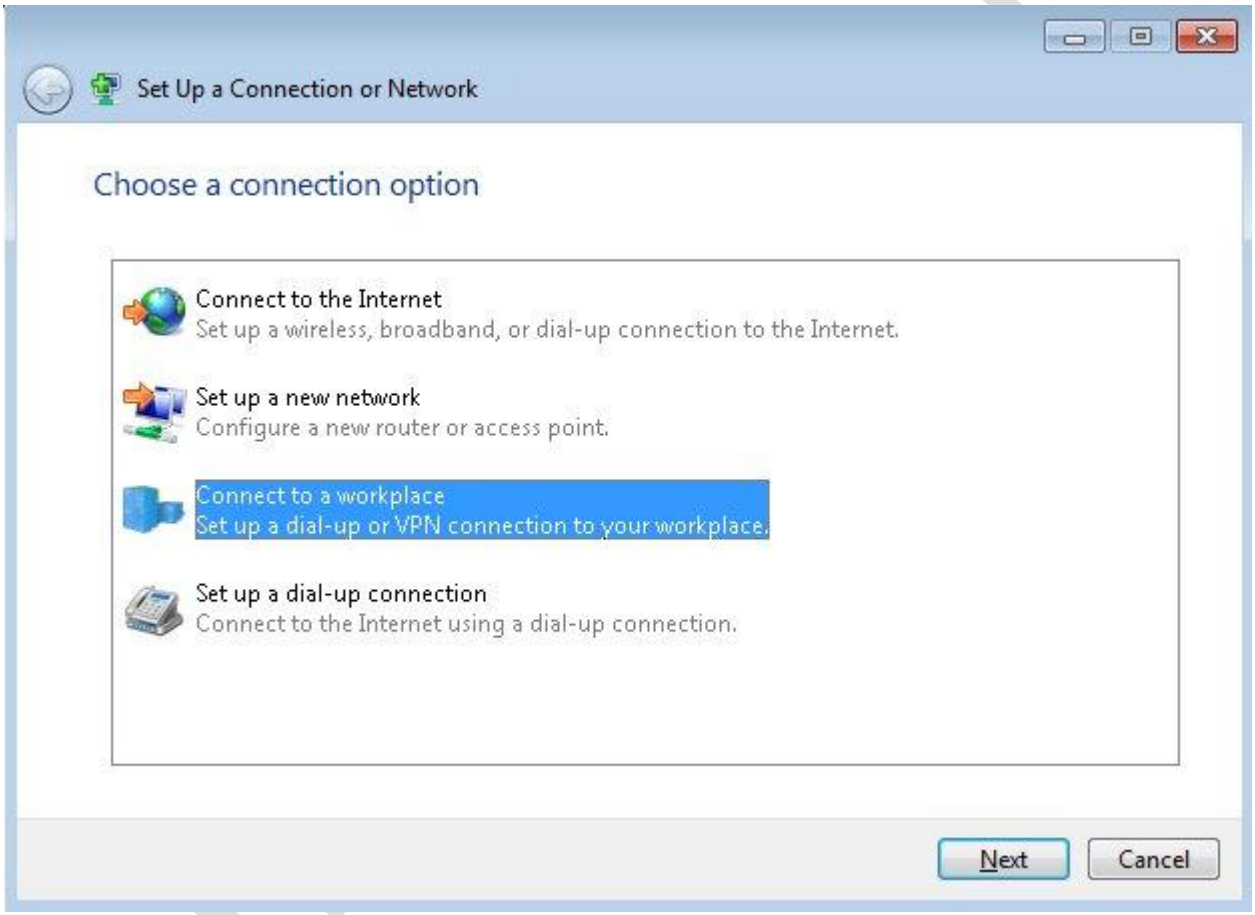
Protocol	Description
PAP	This protocol uses plaintext passwords. Typically used if the remote access client and remote access server cannot negotiate a more secure form of validation. PAP is the least secure authentication protocol. It does not protect against replay attacks, remote client impersonation, or remote server impersonation. PAP is not enabled by default for Windows 7 and is not supported by remote access servers running Windows Server 2008.
CHAP	CHAP uses a 3-way handshake in which the authentication agent sends the client program a key to be used to encrypt the user name and password. CHAP uses the Message Digest 5 (MD5) hashing scheme to encrypt the response. CHAP is an improvement over PAP, in that the password is not sent over the PPP link. CHAP requires a plaintext version of the password to validate the challenge response. CHAP does not protect against remote server impersonation. Although remote access servers running Windows Server 2008 do not support this protocol, it is enabled by default for Windows 7 VPN connections for legacy VPN connections.
MS-CHAP v2	Supports two-way mutual authentication. The remote access client receives verification that the remote access server that it is dialing in to has access to the user's password. MS-CHAP v2 provides stronger security than CHAP.
EAP-MS-CHAPv2	Allows for arbitrary authentication of a remote access connection through the use of authentication schemes, known as EAP types. EAP offers the strongest security by providing the most flexibility in authentication variations. This protocol requires the installation of a computer certificate on the VPN server.

Just like the VPN protocols, by default, Windows first tries to use the most secure authentication protocol that is enabled, and then falls back to less secure protocols if the more secure ones are unavailable.

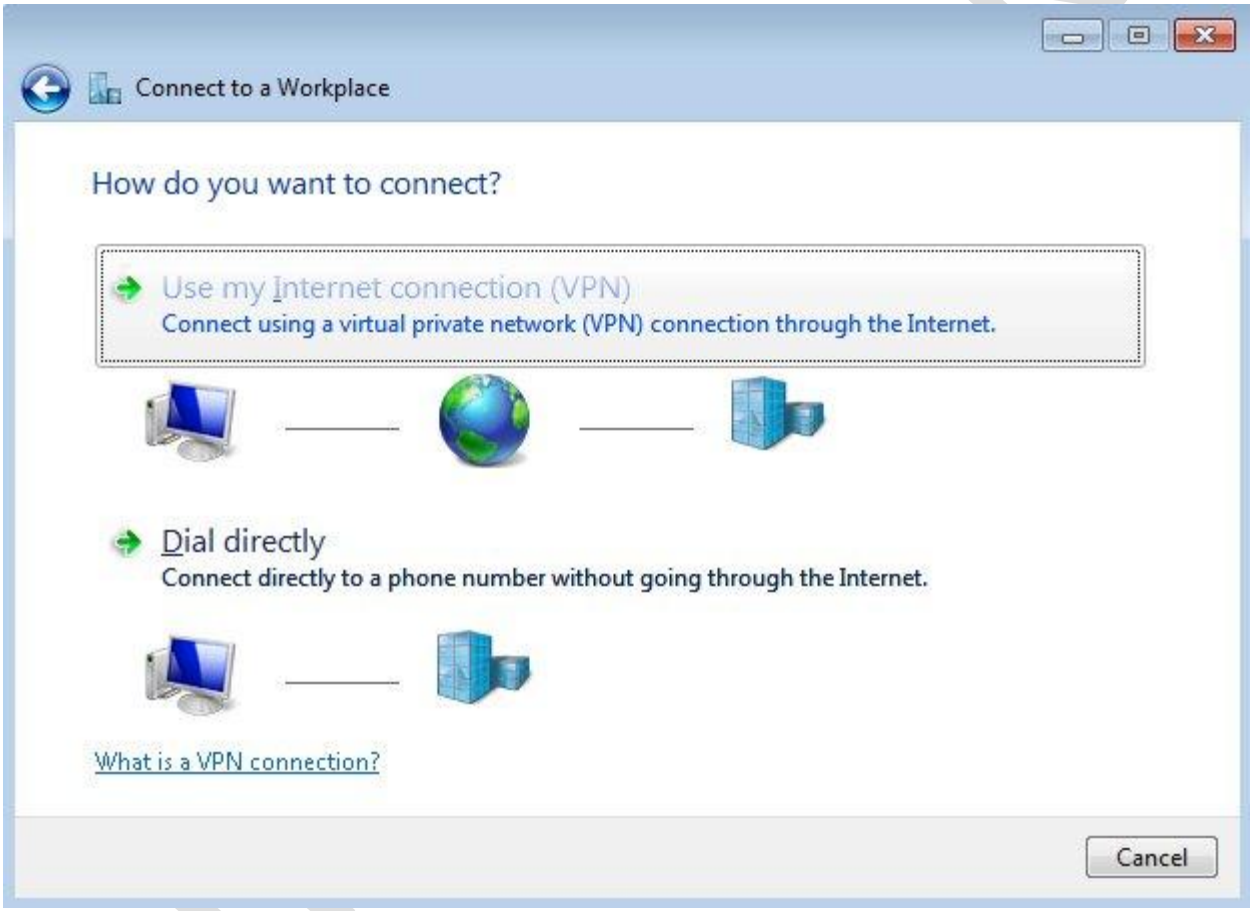
Configuring a VPN Connection:

When configuring a VPN, you need to know the IP address or fully qualified domain name (FQDN) of the remote access server to which you are connecting. The steps for creating the VPN connection to a Windows Server 2008 computer are as follows:

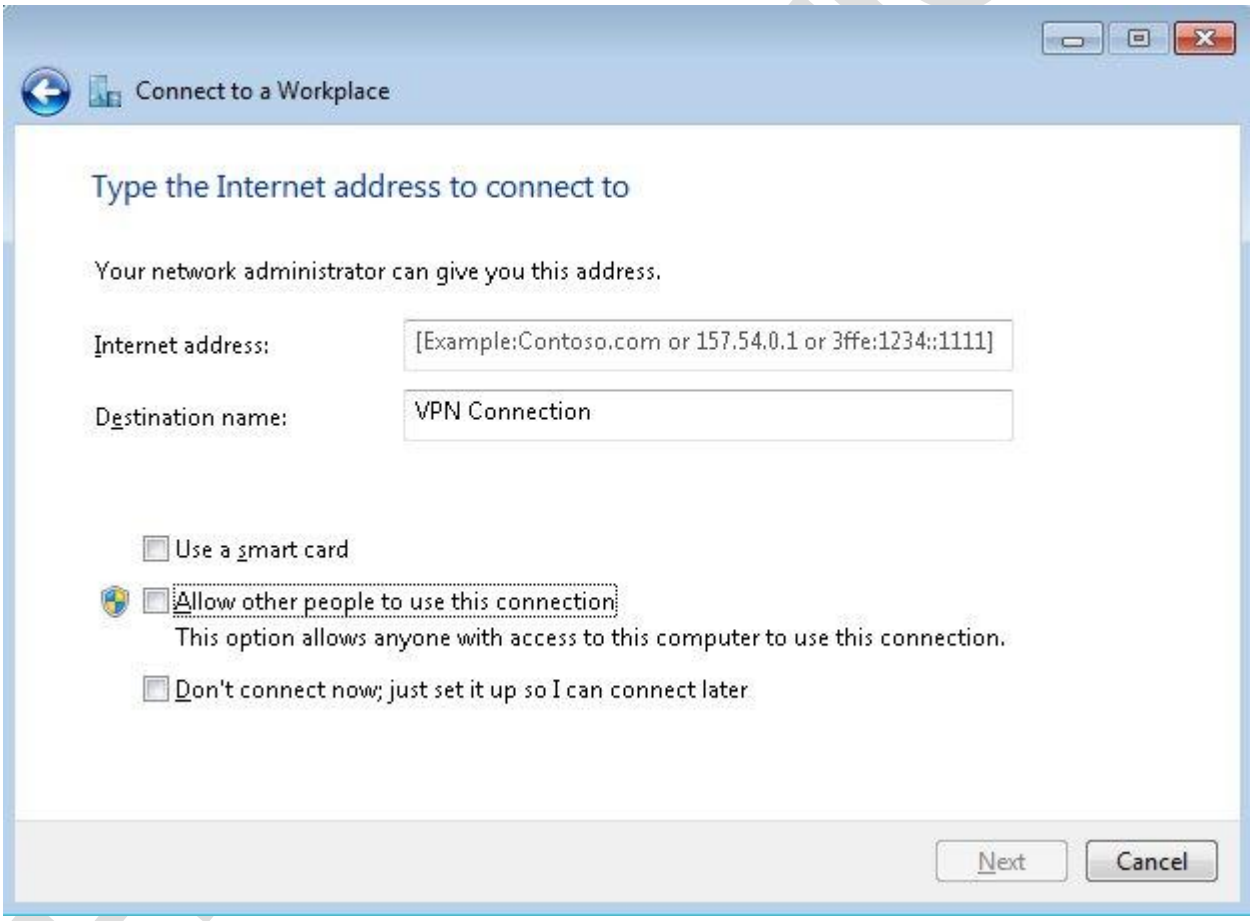
1. Open the Control Panel, select *Network and Internet* then *Network and Sharing Center*.
2. Click *Set up a new connection*.
3. Click *Connect to a workplace* and then click *Next*.



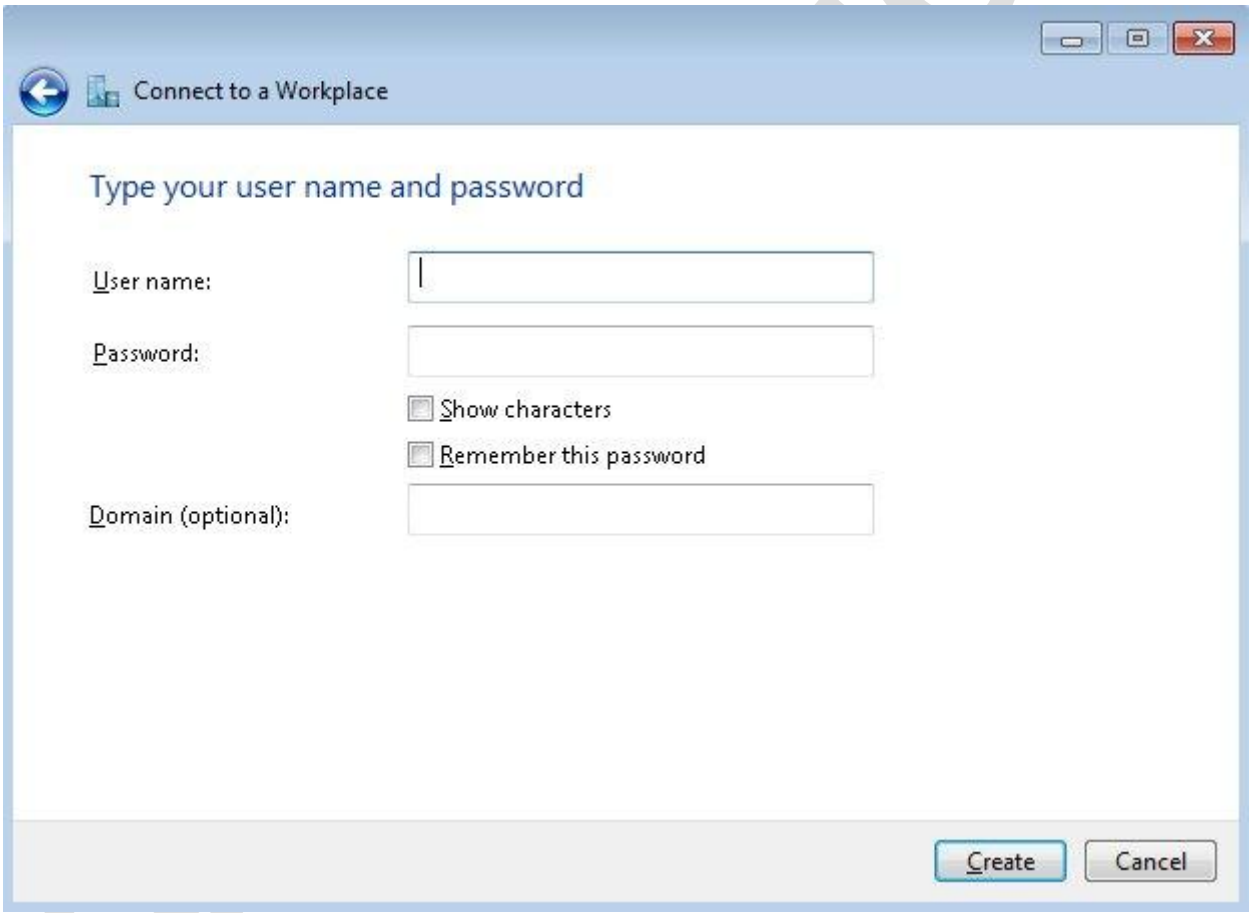
4. Select *Use my Internet connection (VPN)*.



5. Enter the hostname or IP Address for the VPN Server and enter a name for the connection. You can also configure the option to use a smart card for authentication, allow other people to use your VPN connection, and instruct the wizard not to connect you to the VPN now.

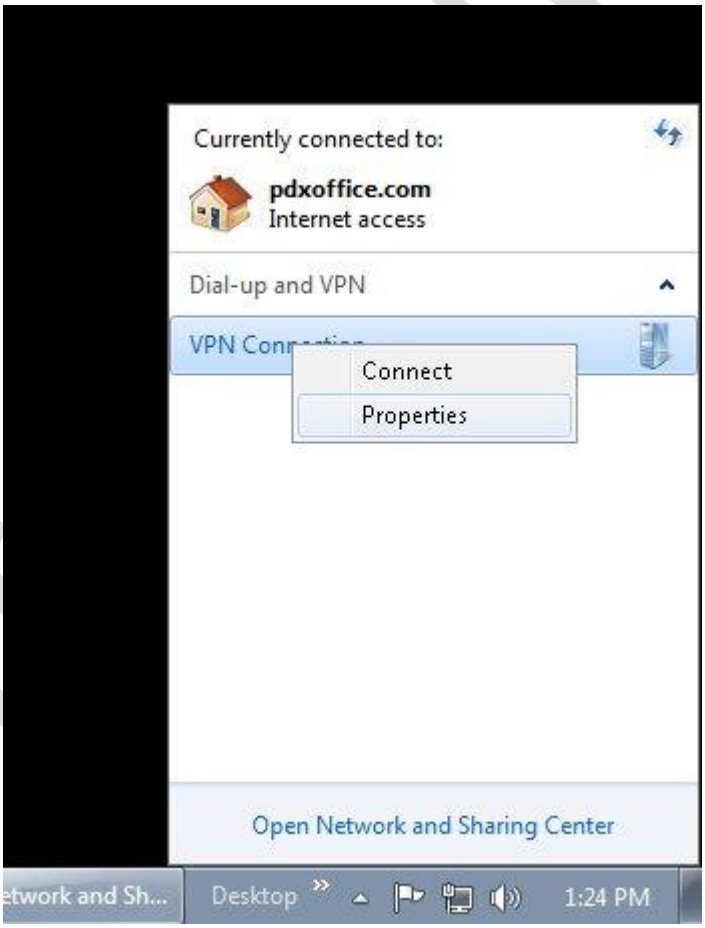


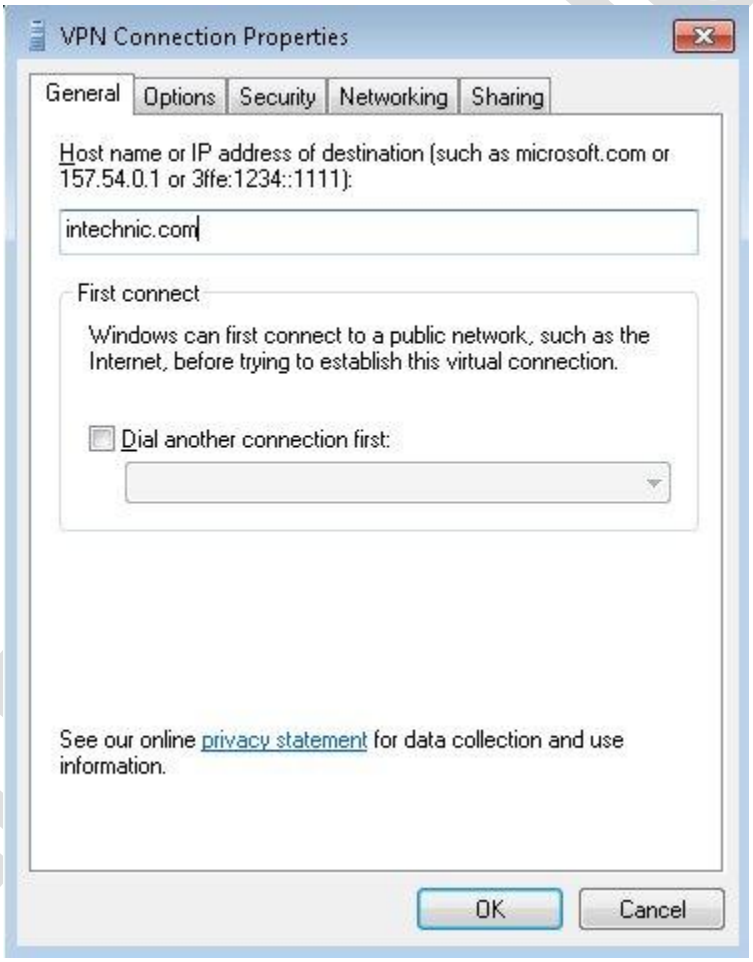
6. Next, you will need to enter a username and password to connect to the network. Click *Create* to finish the wizard.



Once the connection is created, you can modify additional settings such as the authentication protocols and sharing by following these steps:

1. In the Network and Sharing Center, click *Connect to a network*.
2. From the list of networks, right click on your VPN and click *Properties*.





VPN Reconnect:

In previous versions of Windows, when Internet connectivity is lost, the VPN connection is also lost. This means that if the user was working with an application or had a document open when the interruption occurred, the user's work would be lost. In Windows 7, VPN Reconnect uses IKEv2 technology to provide seamless and consistent VPN connectivity, automatically re-establishing a VPN when users temporarily lose their Internet connections. Users who connect using wireless mobile broadband will benefit most from this capability.

Only VPN servers running Windows Server 2008 R2 support IKEv2. You can configure VPN Reconnect with a maximum timeout of 8 hours. After the period specified in the Network Outage Time setting has expired, the user must reconnect manually.

NAP Remediation:

NAP enforces health requirements by monitoring and assessing the health of client computers when they attempt to connect or communicate on a network. Client computers that are not in compliance with the health policy can be provided with restricted network access until their configuration is updated and brought into compliance with policy. Typical problems might include having Windows Firewall turned off, missing or out-of-date virus protection, uninstalled security updates, etc.

On NAP client computers running Windows 7, NAP is integrated into Action Center. If a NAP client computer is determined to be noncompliant with network health polices, you can obtain more information by reviewing the Network Access Protection category under Security. NAP client computers that are compliant with health requirements and computers that are not running the NAP Agent service do not display NAP information in Action Center.

With regard to VPN connections, achieving compliance often requires access to a remediation network. A remediation network hosts necessary services that can allow the client to achieve compliance. Noncompliant clients can communicate with hosts on the remediation network but not other hosts on the internal corporate network. A remediation network might include a Windows Server Update Services (WSUS) server, Antivirus signature server, System Center component server, etc.

70-680 Study Guide - Configure Updates to Windows 7

Windows Update:

Windows Update is a utility that connects to Microsoft's website and checks to ensure that you have the most

up-to-date versions of Microsoft products. These updates include bug fixes, program enhancements, and service packs designed to improve the functionality of your system, and more often, keep it secure.

Service packs are a type of update to the Windows 7 operating system that includes cumulative bug fixes and product enhancements. Some of the options that are included in service packs are security fixes or updated versions of software, such as Internet Explorer. Before installing a service pack, you should perform the following steps:

- Back up your computer.
- Check your computer and ensure that it does not contains any malware or other unwanted software.
- Check with your computer manufacturer to see whether there are any special instructions for your computer prior to installing a service pack.

You can download service packs from Microsoft's web site, and you also receive service packs by Windows Update. Before installing a service pack, you should read the release note that is provided for each service pack on Microsoft's website to understand the prerequisites and installation steps and requirements.

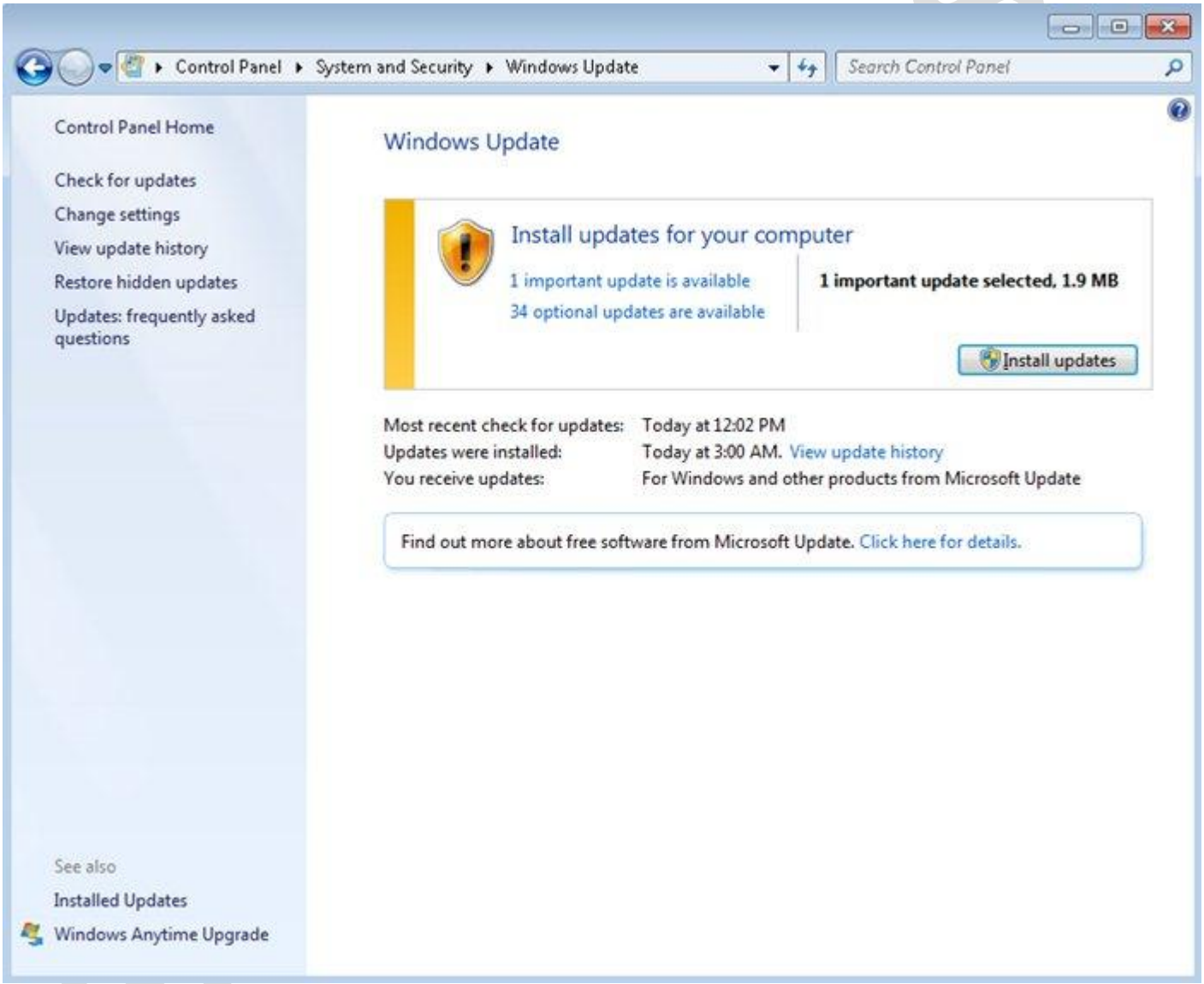
Windows Update is managed through the Windows Update control panel. With this control panel, a user with administrator privileges is able to check for updates, change update settings, review installed updates, and review hidden updates. A user without administrator privileges is able to check for and install updates. Windows Update relies upon the Windows Update service which is enabled by default.

For computers without internet access, you will need to use Windows Update Stand-alone Installer.

Configuring Windows Update:

Follow these steps to configure Windows Update:

1. Click *Start* and then click *Control Panel*.
2. Type *Updates* in the Control Panel's search box and then click *Windows Updates* from the search results.

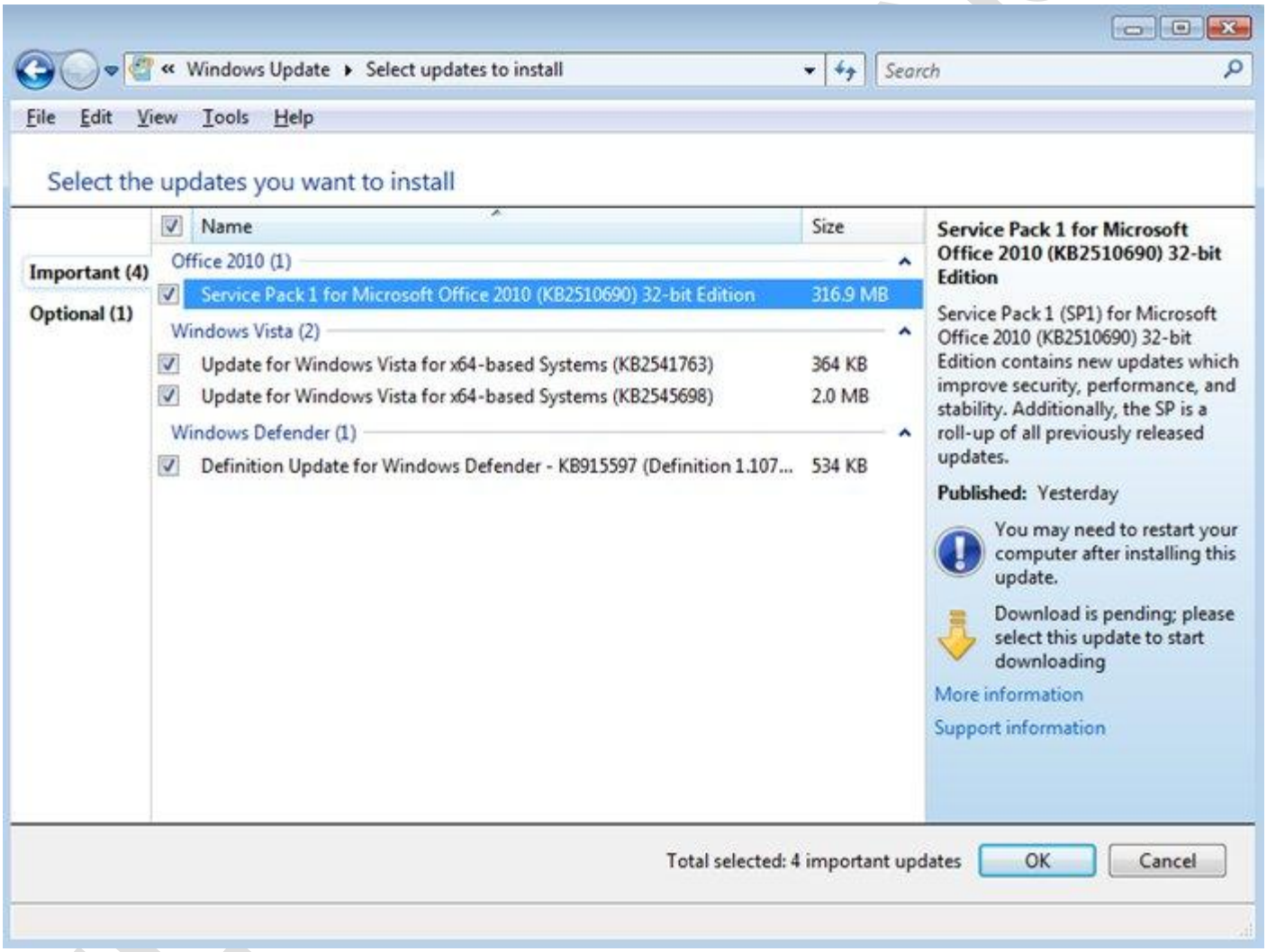


3. Configure the options you want to use for Windows Update from the left pane, and click *OK*.

Now let's take a look at the specific configuration options available in the left pane:

- **Check for Updates** - This link retrieves a list of available updates from the Internet. You can click *View Available Updates* to see which updates are available. Updates are marked as Important, Recommended, or Optional which are explained below:
  - Important Updates: Typically correct critical security issues.
  - Recommended Updates: Typically address functionality issues.

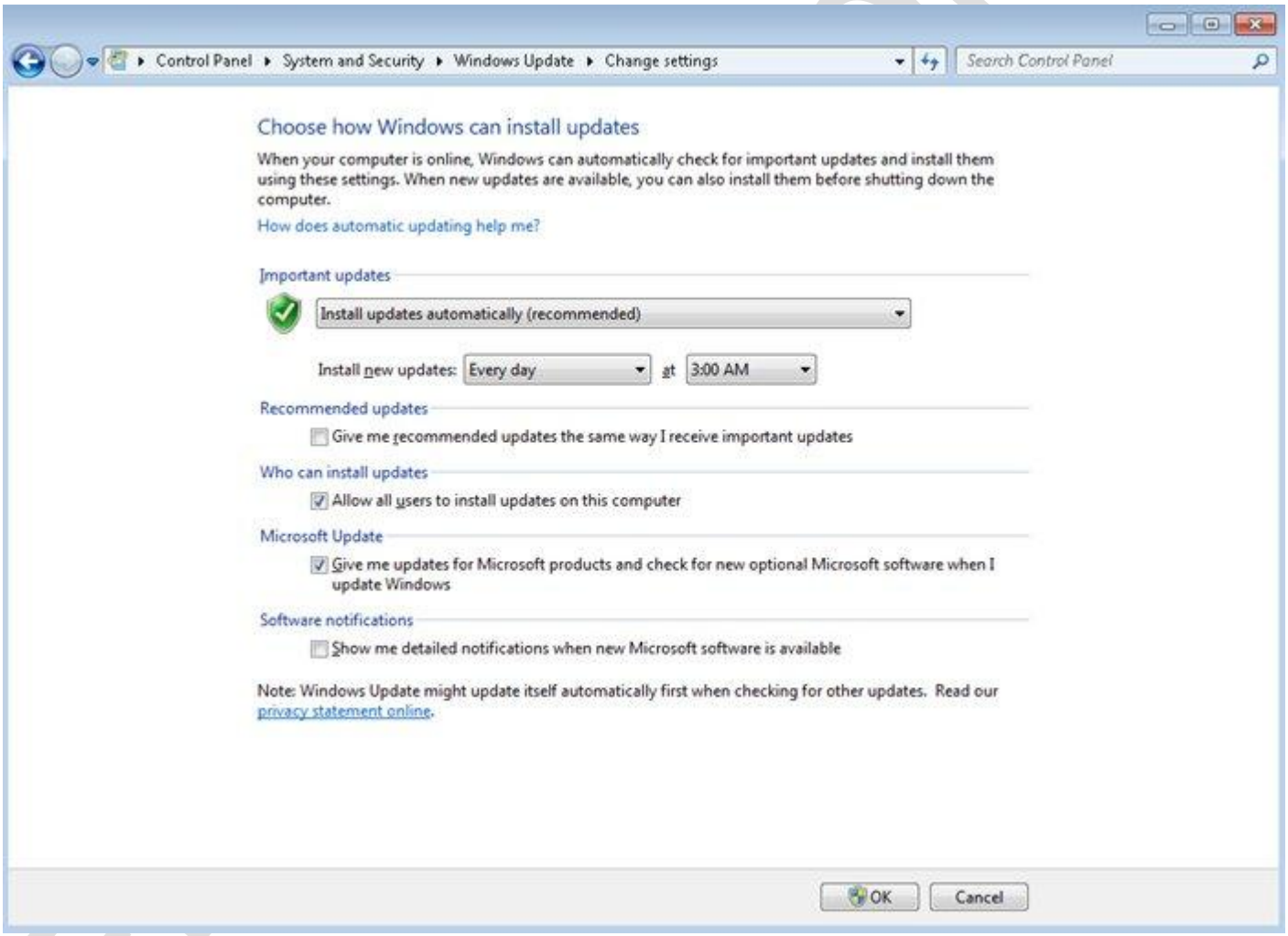
- Optional Updates: Optional updates provide items such as driver updates, language packs, and updates to help files.



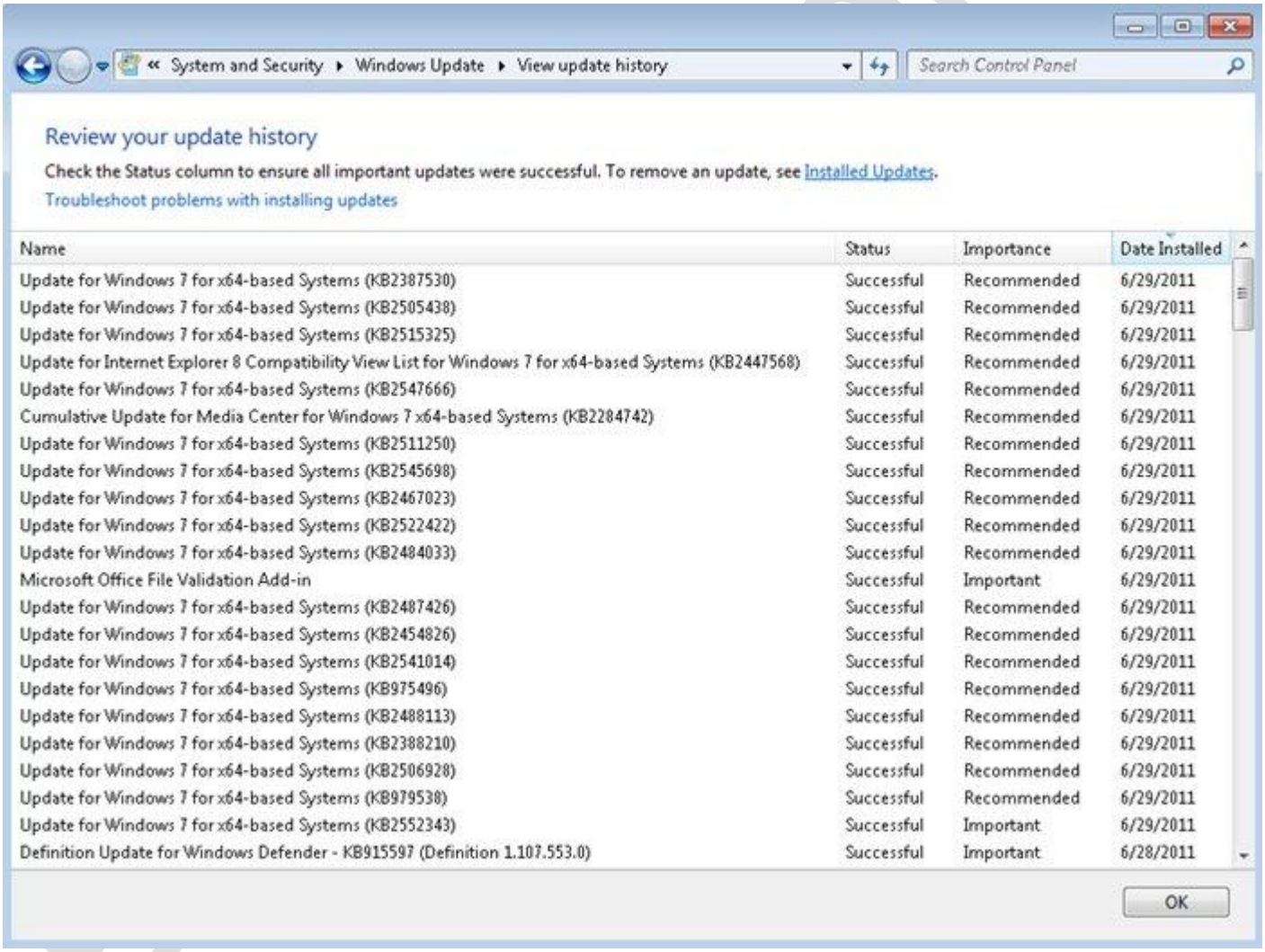
A user with administrative rights can right click on an update to hide it from other users if there is a reason it shouldn't be installed.

- **Change Settings** - Change Settings allows you to customize how and when Windows should install updates. Most importantly is setting how Windows handles important updates. The following options are available:
  - Install updates automatically (recommended)
  - Download updates but let me choose whether to install them
  - Check for updates but let me choose whether to download and install them
  - Never check for updates (not recommended)

Another important setting on this screen is "Give Me Recommended Updates The Same Way I Receive Important Updates". Checking this box will force Windows to treat recommended updates the same way as important updates. Optional updates always have to be installed manually.



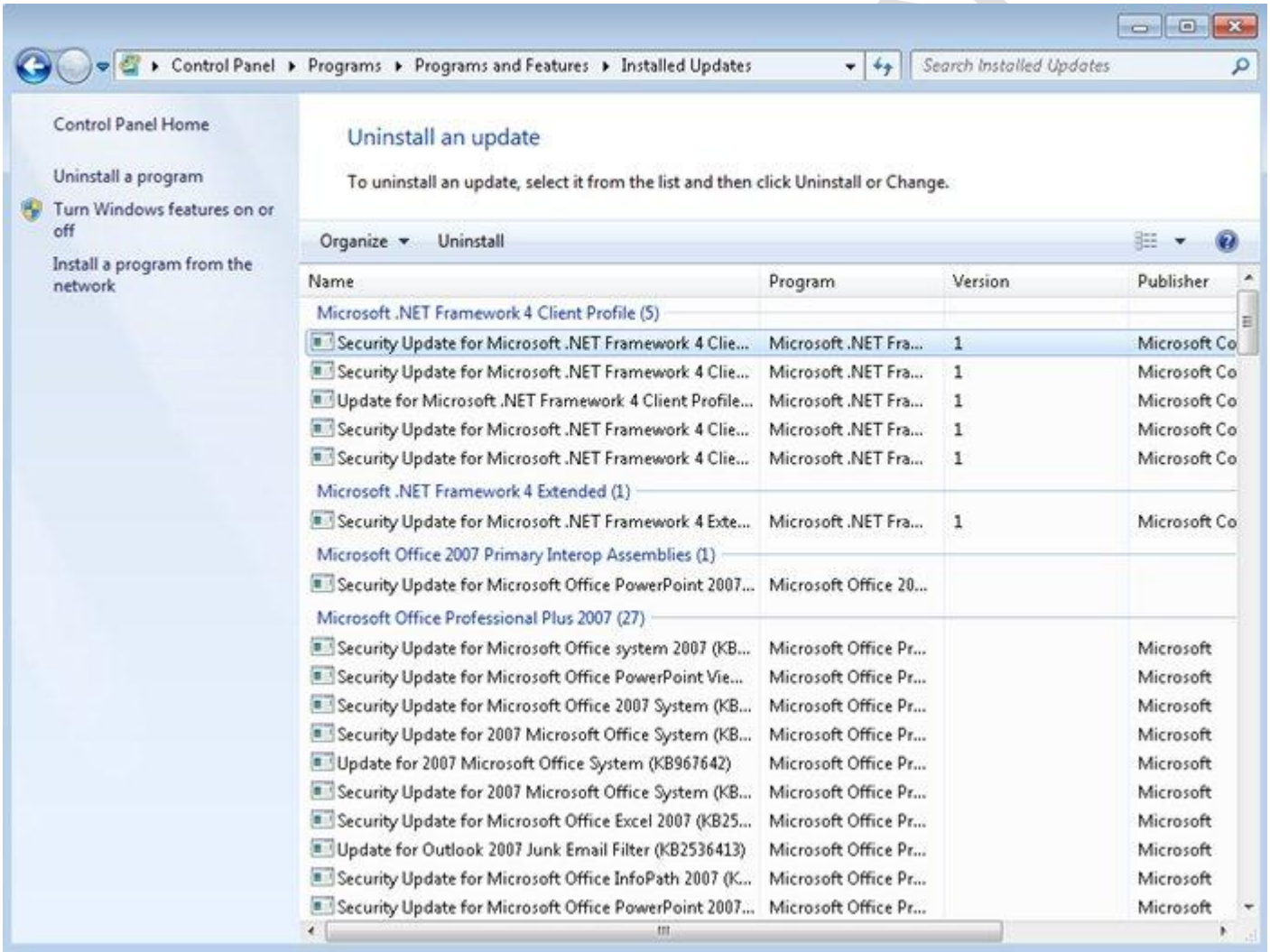
- **View Update History** - View Update History, is used to view a list of all of the installations that have been performed on the computer. Following information is avialable for each installation:
  - Update Name
  - Status (Successful, Unsuccessful, or Canceled)
  - Importance (Important, Recommended, or Optional)
  - Date Installed



You can view the details of an update on the list by right clicking on it and selecting *View Details*.

- **Restore Hidden Updates** - With Restore Hidden Updates you can list the updates that you have hidden from available updates list. An administrator can hide updates that they do not want users to install. It gives the opportunity for an administrator to test and verify updates before the users can install them.
- **Installed Updates** - Installed Updates allows you to see the updates that you have installed earlier and you can also uninstall or change them if necessary. The link in the lower left pane is actually a shortcut to the Programs And Features Control Panel applet. If you uninstall an update, it will become available

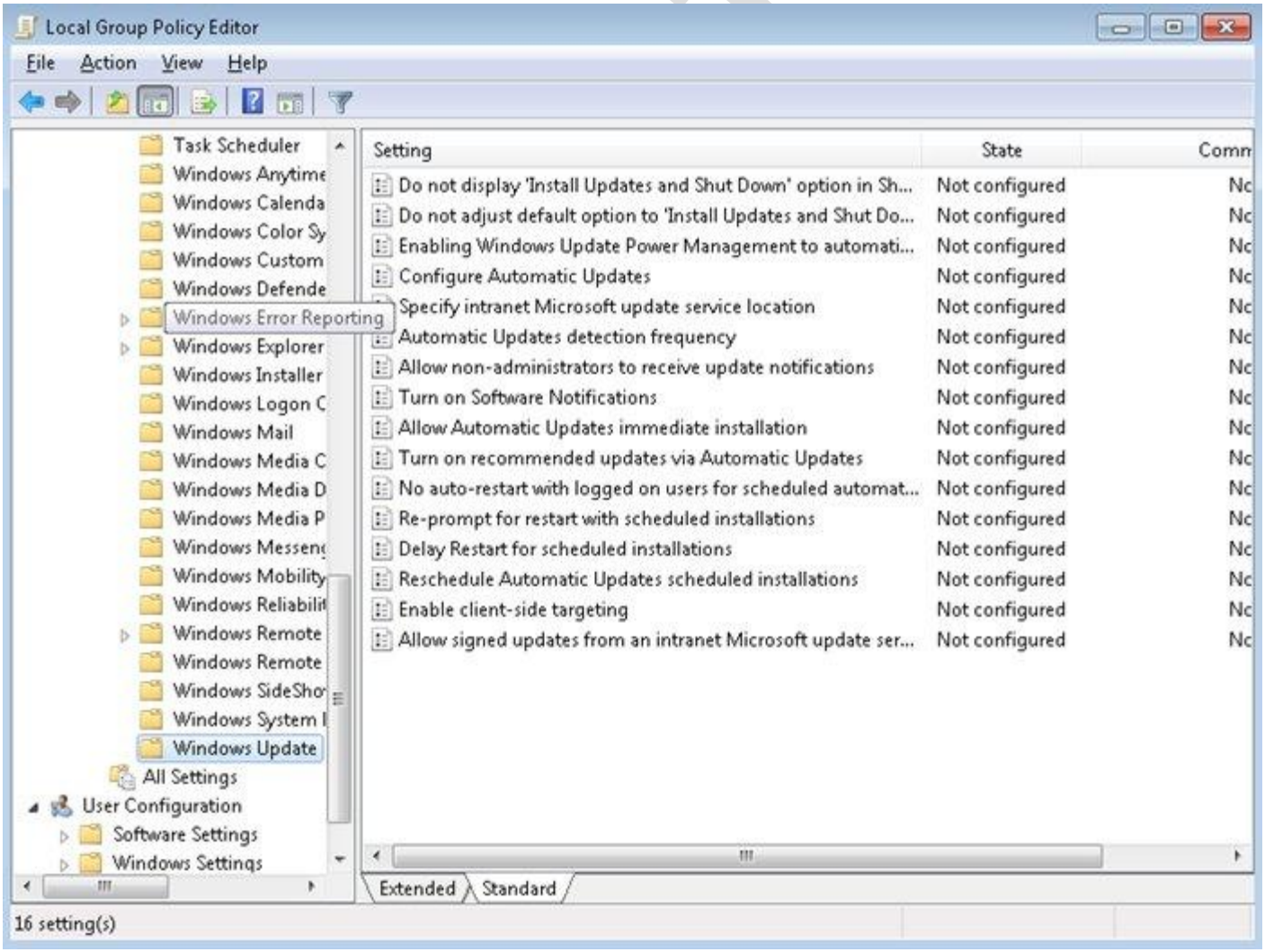
for installation again unless you mark it as hidden.



Windows Update Policies:

Group policy provides additional configuration options to those already discussed in the control panel applet. To access these policies, follow these steps:

1. Click *Start* and in the search box enter *group policy*.
2. Click *Edit group Policy*.
3. Browse the folders on the left to the following location: Computer Configuration\Administrative Templates\Windows Components\Windows Update.



The table below explains what each of these group policy settings does:

Policy	Description
Do Not Display "Install Updates And Shut Down" Option In Shut Down Windows Dialog Box	This policy allows you to configure whether the Shut Down menu displays the Install Updates And Shut Down option. The default setting has this option available.
Do Not Adjust Default Option To "Install Updates And Shut Down" in Shut Down Windows Dialog Box	When this policy setting is enabled, the user's last shutdown choice is the default shutdown option. When this policy setting is disabled or is not configured, Install Updates and Shut Down is the default option if updates are available for installation. This policy is deprecated when the Do Not Display "Install Updates And Shut Down" Option In Shut Down Windows Dialog Box policy is enabled.
Enabling Windows Update Power Management To Automatically Wake The System To Install Scheduled Updates	This policy allows Windows Update to wake a hibernating computer to install updates. Updates does not install if the computer is hibernating on battery power.
Configure Automatic Updates	This policy, allows you to configure update detection, download, and installation settings. Several of these settings are similar to the ones that you can configure through the Windows Update control panel.
Specify Intranet Microsoft Update Service Location	This policy allows you to specify the location of an internal update server, such as one running WSUS. This policy is the only way that you can configure Windows Update to use an alternate update server. Using this policy, you can specify the update server and the statistics server. In most cases, these are the same servers. The updates server is where the updates are downloaded from, and the statistics server is the server where clients report update installation information.
Automatic Updates Detection Frequency	Configure this policy to specify how often Windows Update checks the local intranet update server for updates. This policy does not work if you configure a client to retrieve updates from the Windows Update servers.
Allow Non-Administrators To Receive Update Notifications	This policy specifies whether users who are not members of the local Administrators group are able to install updates.
Turn On Software Notification	When you enable this policy, Windows Update presents users with information about optional updates.
Allow Automatic Updates Immediate Installation	When you enable this policy, updates that do not require a restart install automatically. Updates that do require a restart are not installed until the conditions set in the Configure Automatic Updates policy are met.
Turn On Recommended Updates	Use this policy to configure Windows Update to install recommended updates

Via Automatic Updates	as well as important updates.
No Auto-Restart With Logged On Users For Scheduled Automatic Updates Installation	When you enable this policy, Windows Update waits until the currently logged on user logs off if Windows Update installs updates that requiring a restart. If you disable or do not configure this policy and the Configure Automatic Updates policy is set to install updates at a specific time, Windows Update gives the logged-on user a 5-minute warning prior to restarting to complete the installation.
Re-prompt For Restart With Scheduled Installations	Use this policy to set the amount of time that a user can postpone a scheduled restart when the Configure Automatic Updates policy is set to install updates at a specific time.
Delay Restart For Scheduled Installations	Through this policy, you can specify the amount of time that Windows waits before automatically restarting after a scheduled installation. This policy applies only if the Configure Automatic Updates policy is set to install updates at a specific time.
Reschedule Automatic Updates Scheduled Installations	You can use this policy to configure a computer that has missed a scheduled update to perform the update a specific number of minutes after startup. For example, use this policy to ensure that a computer that was switched off at the scheduled update time installs updates 1 minute after starting up. Disabling this policy means that updates install at the next scheduled time.
Enable Client-Side Targeting	This policy allows you to place computers into different software update groups. Different software update groups allow the software update administrator to target the deployment of updates, allowing updates to be deployed to specific groups of computers in the organization rather than all computers in the organization.
Allow Signed Updates From An intranet Microsoft Update Service Location	This policy allows updates from third-party vendors to be distributed from the Automatic Updates location so long as those updates are digitally signed by a trusted publisher.

Windows Server Update Services (WSUS):

Using Windows Update to update client computers works well for smaller networks, but for an enterprise network, this can cause management and bandwidth issues. Products such as Windows Server Update Services (WSUS), System Center Essentials, and System Center Configuration Manager (SCCM) can alleviate issues. These products download updates from Microsoft and then make them available to clients over the local network. Furthermore, these products give administrators a chance to test updates before releasing them to the clients on their network which can help avoid wide-spread problems. If problems do occur after a rollout, WSUS provides the ability to rollback the update across the enterprise.

To connect a client to a WSUS server, follow the instructions above to view Windows Update policies. Open the *Specify intranet Microsoft update service location*. Once opened, you must set two servername values: the server from which the Automatic Updates client detects and downloads updates, and the server to which

updated workstations upload statistics. You can set both values to be the same server.

70-680 Study Guide - Manage Disks

File Systems:

Before we get into managing disks in Windows 7, let's review file systems first. A file system is a method of storing and organizing computer files and their data. There are two types of file systems supported by Windows as follows:

- **FAT File System** - File Allocation Table (FAT) is a file system that was created by Microsoft in 1977. FAT is still in use today as the preferred file system for floppy drive media and portable, high capacity storage devices. FAT is the most simple of the file systems supported by Windows. It is characterized by the file allocation table (FAT), which is a table that resides at the very "top" of the volume. To protect the volume, two copies of the FAT are kept in case one becomes damaged. In addition, the FAT tables and the root directory must be stored in a fixed location so that the system's boot files can be correctly located. There is no organization to the FAT directory structure, and files are given the first open location on the drive. In addition, FAT supports only read-only, hidden, system, and archive file attributes. There are three versions of the FAT file system.
    - FAT12 - This initial version of the FAT file system was introduced in 1977, even before MS-DOS, and was the primary file system for Microsoft operating systems up to MS-DOS 4.0. FAT12 supports drive sizes up to 32MB.
    - FAT16 - The second implementation of FAT was FAT16, introduced in 1988. FAT16 was the primary file system for MS-DOS 4.0 up to Windows 95. FAT16 supports drive sizes up to 2GB.
    - FAT32 - FAT32 is the latest version of the FAT file system. It was introduced in 1996 for Windows 95 OSR2 users and was the primary file system for consumer Windows versions through Windows ME. FAT32 supports drive sizes up to 8TB.
- **NTFS File System** - The New Technology File system (NTFS) was introduced by Microsoft in 1993 with Windows NT 3.1. NTFS supports hard drive size up to 256TB. NTFS is the primary file system used in Microsoft's Windows 7, Windows Vista, Windows XP, Windows 2000, and Windows NT Operating Systems. The goals of NTFS are to provide:
    - Reliability, which is especially desirable for high end systems and file servers
    - A platform for added functionality
    - Support for POSIX requirements
    - Removal of the limitations of the FAT and HPFS file systems

  To ensure reliability of NTFS, three major areas were addressed: recoverability, removal of fatal single sector failures, and hot fixing.

  NTFS is a recoverable file system because it keeps track of transactions against the file system. When a CHKDSK is performed on FAT or HPFS, the consistency of pointers within the directory, allocation, and file tables is checked. In NTFS, a log of transactions against these components is maintained so that CHKDSK need only roll back transactions to the last commit point in order to recover consistency within the file system. In FAT or HPFS, if a sector that is the location of one of the file system's special objects fails, then a single sector failure will occur. NTFS avoids this in two ways: first, by not using special

objects on the disk and tracking and protecting all objects that are on the disk. Second, NTFS keeps multiple copies (the number depends on the volume size) of the Master File Table.

Some features that are available when you choose NTFS:

- File encryption allows you to protect files and folders from unauthorized access.
- Permissions can be set on individual files, as well as on folders.
- Disk quotas allow you to monitor and control the amount of disk space used by individual users.
- Better scalability allows you to use large volumes. The maximum volume size for NTFS is much greater than it is for FAT.
- Additionally, NTFS performance does not degrade as volume size increases, as it does in FAT systems.
- Recovery logging of disk activities helps restore information quickly in the event of power failure or other system problems.

Windows supports the FAT16, FAT32, and NTFS file systems. Because NTFS has all the basic capabilities of FAT16 and FAT32, with the added advantage of advanced storage features such as compression, improved security, and larger partitions and file sizes, it is the recommended file system for Windows 7. The table below compares some additional NTFS and FAT32 capabilities.

Comparison Issues	NTFS	FAT32
Operating system compatibility	A computer running Windows Vista, Windows Server 2003, Windows 2000, or Windows XP can access files on an NTFS partition. A computer running Windows NT 4.0 with Service Pack 4 or later can access files on the partition, but some NTFS features, such as Disk Quotas, are not available. Other operating systems allow no access.	File access is available only to computers running Microsoft Operating Systems.
Volume size	Volumes up to 2 terabytes, but support for much larger sizes is possible.	Supports volumes from 512 MB to 2 terabytes. Cannot be used on floppy disks.
File size	Maximum file size is 2 terabytes.	Volumes from 512 MB to 2 terabytes.
Files per volume	4,294,967,295 (2^{32} minus 1 files)	Approximately 4,177,920

MBR vs GPT:

When you prepare any drive or volume to be used by Windows 7, you must first partition and then format the disk. Partitioning is defining and dividing the physical or virtual disk into logical volumes called partitions. Each partition functions as if it were a separate disk drive. Windows 7 supports two types of disk partitioning - Master Boot Record (MBR) and GUID partition table (GPT).

Master Boot Record (MBR) is the standard partitioning scheme that's been used on hard disks since the PC first came out. It supports 4 primary partitions per hard drive, and a maximum partition size of 2TB.

GUID Partition Table (GPT) disks are a newer partitioning type that was introduced with Intel Itanium-based processors and the Extensible Firmware Interface (EFI). EFI is used instead of the BIOS as the interface between the computer's hardware devices, its firmware, and the operating system as found with MBR. A GPT disk can support a volume up to 2^64 blocks in length. For 512-byte blocks, this is 9.44 ZB – zettabytes. 1 ZB is 1 billion terabytes. It can also support theoretically unlimited partitions. Windows restricts these limits further to 256 TB for a single partition (NTFS limit), and 128 partitions. When using a drive over 2 TB, you must use GPT. The GPT partitioning style cannot be used on removable media.

Instructions for converting between these partition type are provided in the Disk Management Tool section below.

Basic Disks vs Dynamic Disks:

Basic disks and dynamic disks are two types of hard disk configurations in Windows. Most personal computers are configured as basic disks, which are the simplest to manage. Advanced users and IT professionals can make use of dynamic disks, which use multiple hard disks within a computer to manage data, usually for increased performance or reliability.

A basic disk uses primary partitions, extended partitions, and logical drives to organize data. A formatted partition is also called a volume (the terms volume and partition are often used interchangeably). In this version of Windows, basic disks can have either four primary partitions or three primary and one extended partition. The extended partition can contain multiple logical drives (up to 128 logical drives are supported). The partitions on a basic disk cannot share or split data with other partitions. Each partition on a basic disk is a separate entity on the disk.

Dynamic disks can contain a large number of dynamic volumes (approximately 2000) that function like the primary partitions used on basic disks. In Windows 7, you can combine separate dynamic hard disks into a single dynamic volume (called spanning), split data among several hard disks (called striping) for increased performance (no fault tolerance), or duplicate the data on one disk to another (called mirroring).

Let's take a look at these configurations in a little more detail.

- **Spanned volumes** - A spanned volume is a formatted partition which data is stored on more than one hard disk, yet appears as one volume. Spanned volumes are a non-RAID drive architecture. If you extend a simple volume to another dynamic disk, it automatically becomes a spanned volume. You can extend a simple volume to make it a spanned volume, and you can also further extend a spanned volume to add disk storage capacity to the volume. After a volume is spanned, you cannot stripe or mirror it.
- **Striped volumes** - Striped volumes are dynamic volumes that contain disk space from two to thirty-two hard disks. Data that is written to a striped volume is divided by the operating system into chunks of 64KB. The operating system stores each chunk on a separate disk. Since, in a striped volume, a large amount of data is divided into identical portions, it is faster to read or write the data from a striped volume than from a spanned volume. Striped volumes are not fault tolerant and are also referred to as RAID-0. A striped volume's capacity is limited to the space available on the disk with the smallest amount of available space.

- **Mirrored volumes** - A mirrored volume, also known as RAID-1, is a fault-tolerant volume that duplicates data on two different physical disks. If one of the disks fails, the data is not lost as an exact copy remains on the surviving disk. Mirroring costs disk space - for example, if you mirror two 100 GB disks, you are left with just 100GB of space rather than 200GB. While great for redundancy, mirroring isn't ideal for performance as all data has to be written twice.

While Windows 7 only supports RAID levels 0 and 1 via software, a 3rd party solution can provide additional RAID services such as RAID-5. For more information about RAID, read Hardware and Software RAID.

Note: Dynamic disks are supported only on computers that use the Integrated Drive Electronics (IDE), Small Computer System Interface (SCSI), Fibre Channel, or Serial Storage Architecture (SSA). Laptops and other mobile devices, removable disks, and disks connected via Universal Serial Bus (USB) or FireWire (IEEE 1394) interfaces are not supported for dynamic storage. Dynamic disks are also not supported on hard drives with a sector size less than 512 bytes and the disk must have at least 1mb of free space for the dynamic disk database.

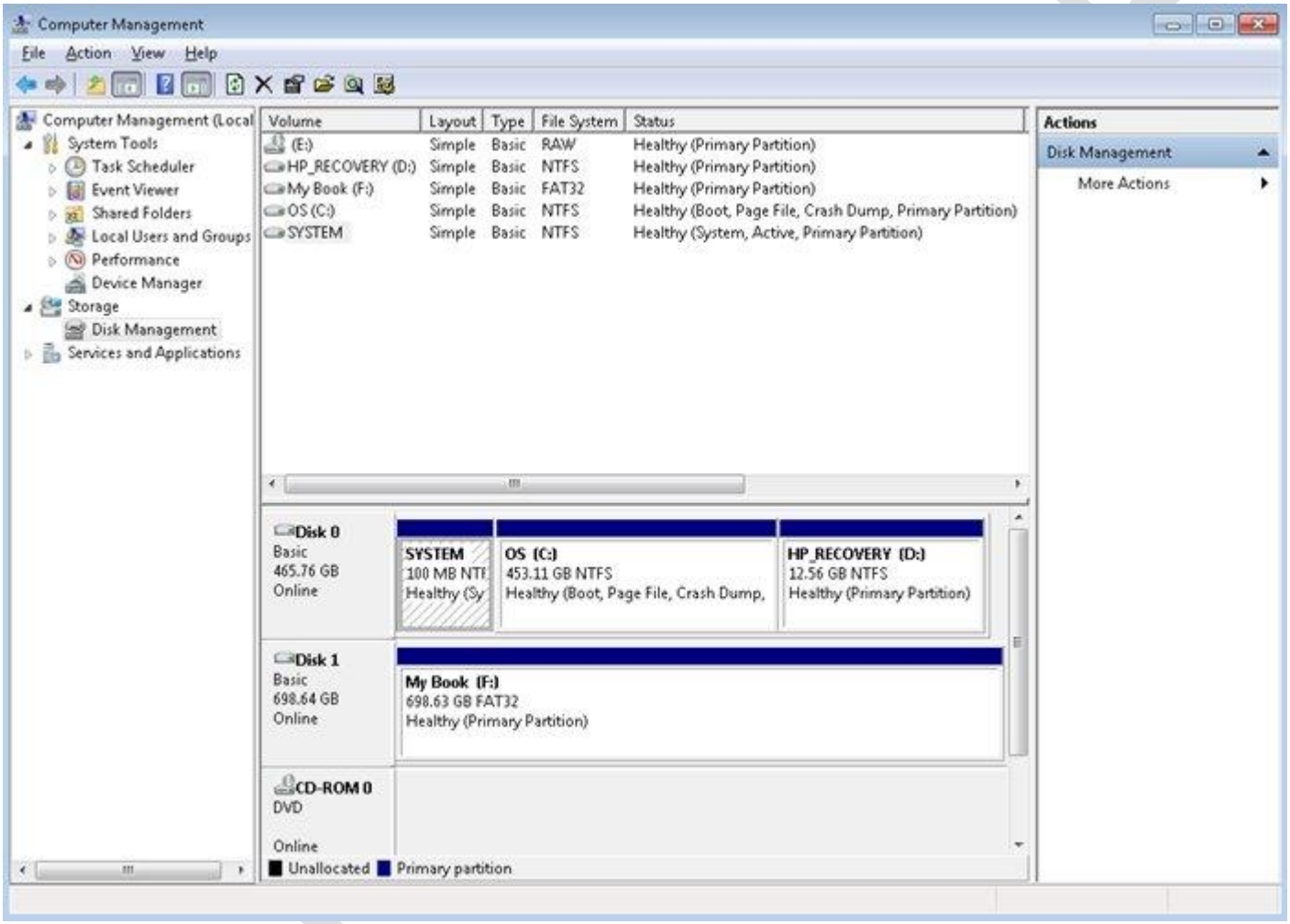
Disk Management Tool:

Disk Management is a useful built-in Windows 7 partition manager that makes hard disk partitioning quick and simple. Windows 7 Disk Management includes:

- A built-in partition manager
- A graphical user interface (GUI)
- Ability to create new disk partitions within Windows 7
- Ability to shrink existing disk partitions

With Disk Management, you can initialize disks, create volumes, format volumes with file systems FAT, exFAT, FAT32 or NTFS. You can also extend a disk, reduce a disk, check if a disk is healthy or unhealthy, create partitions, delete partitions, or change a drive letter. Disk Management enables you to perform most disk-related tasks without restarting the system, and most changes take effect immediately. To access Disk management, perform these steps:

1. Click *Start*, right-click *Computer*, and click *Manage*.
2. In the left pane click *Disk Management*.



The Disk Management console shown above lists each volume in alphabetical order. Each hard disk is then broken down into Type, File System, Status, Capacity, and Free Space. In the second horizontal column, each logical drive is labeled by its letter and given a color. Right-clicking on each drive opens a menu where users can extend volumes, shrink volumes, or create new logical drive. You need Administrator or Backup Operator credentials to perform most Disk Management tasks.

Configuring Disks:

Follow the steps below to create a new partition in Windows 7:

1. In the Disk Management Console, right-click the unallocated space and select *New Simple Volume*, and click *Next*.
2. Select the size for the new volume or partition in MB.
3. Assign the drive letter to the new partition.
4. Format the partition with the appropriate file system and select the check box *Perform a Quick Format*. To enable compression, select the check box *Enable File and Folder compression*.
5. Click *Finish*.

Perform these steps to shrink an existing partition in order to create a new partition:

1. In the Disk Management Console, right-click on the partition which you want to resize. The system displays the capacity of the drive and the option to enter an amount you'd like to "shrink" your partition by. Click *Shrink*.
2. You can now see the unallocated space on your hard drive in the capacity you specified, situated just after your now resized original partition.
3. Right-click the unallocated volume, select *New Simple Volume*, assign a drive letter, and quick format the volume using the NTFS file system and default allocation unit size.

Extending a partition:

1. In the Disk Management Console, right-click the partition that you want to extend and select *Extend Volume*.
2. Click *Next*. The system displays the capacity of the drive and the option to enter an amount you'd like to extend your partition by. Click *Next*.
3. Click *Finish*.

Deleting a partition:

1. In the Disk Management Console, right-click the partition that you want to delete and select *Delete Volume*.
2. Click *Yes* to continue the deletion process.
3. Click *Yes* to delete the partition.

Changing the drive letter:

1. In the Disk Management Console, right-click on a partition and select *Change drive letters and paths*.
2. The current drive letter will display. The *Add* button typically allows the partition to be placed inside an existing NTFS folder.
3. Click *Change* to assign a new drive letter.

To convert from an MBR partition to a GPT partition, or vice versa, follow these steps:

1. Back up or move the data on the basic MBR disk you want to convert.
2. Open Computer Management (Local).
3. In the console tree, click *Computer Management* (Local), click *Storage*, and then click *Disk Management*.

4. The disk must not contain any partitions or volumes. If these exist, right-click any volumes on the disk and then click *Delete Partition* or Delete Volume.
5. Right-click the MBR disk that you want to change into a GPT disk, and then click *Convert to GPT Disk*.

Converting a basic disk to a dynamic disk:

1. In the Disk Management Console, simply right-click the disk you want to convert and click *Convert To Dynamic Disk*. If you want to convert from a dynamic disk to a basic disk, you must first delete all volumes, hence all data, on the disk.

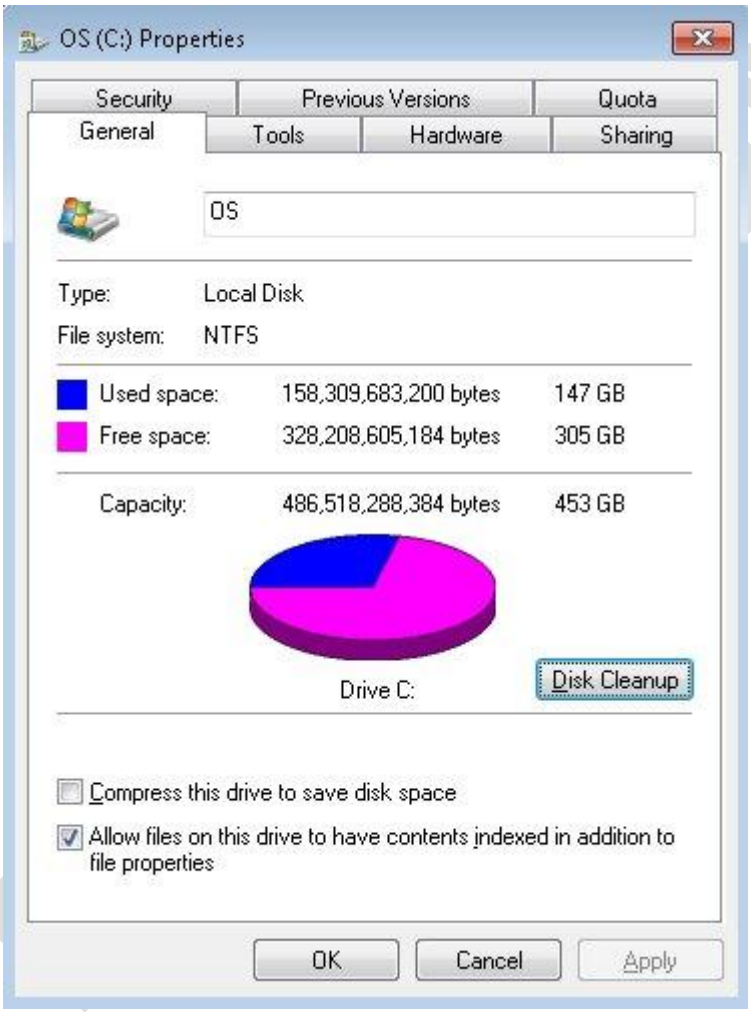
Windows 7 will disallow any of the changes listed above if the partition is currently used as a system, boot, or page file drive.

In addition to the Disk Management Console, Windows also includes a command line utility called DiskPart that can be used to configure disks. For more information, read A Description of the Diskpart Command-Line Utility.

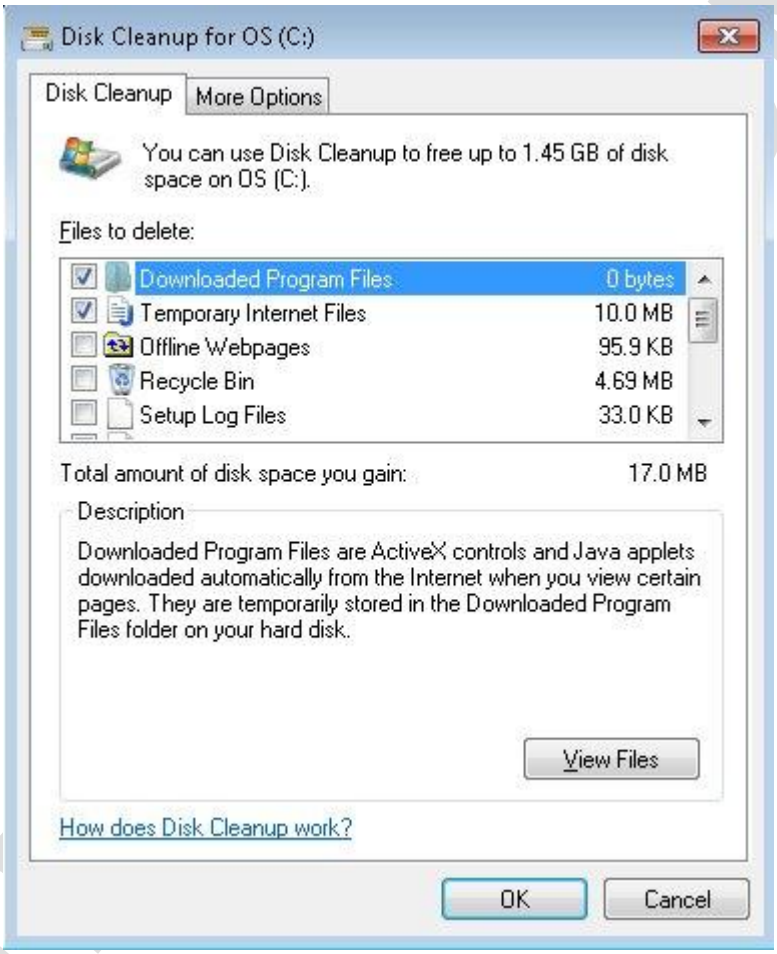
Disk Maintenance:

Windows provides a number of tools that can help keep your disks healthy and optimized. Let's start with Disk Cleanup. If you want to reduce the number of unnecessary files on your hard disk to free up disk space and help your computer run faster, use Disk Cleanup. It removes temporary files, empties the Recycle Bin, and removes a variety of system files and other items that you no longer need. Follow these steps:

1. Open *Computer*, right click on the drive you wish to clean and select *Properties*.



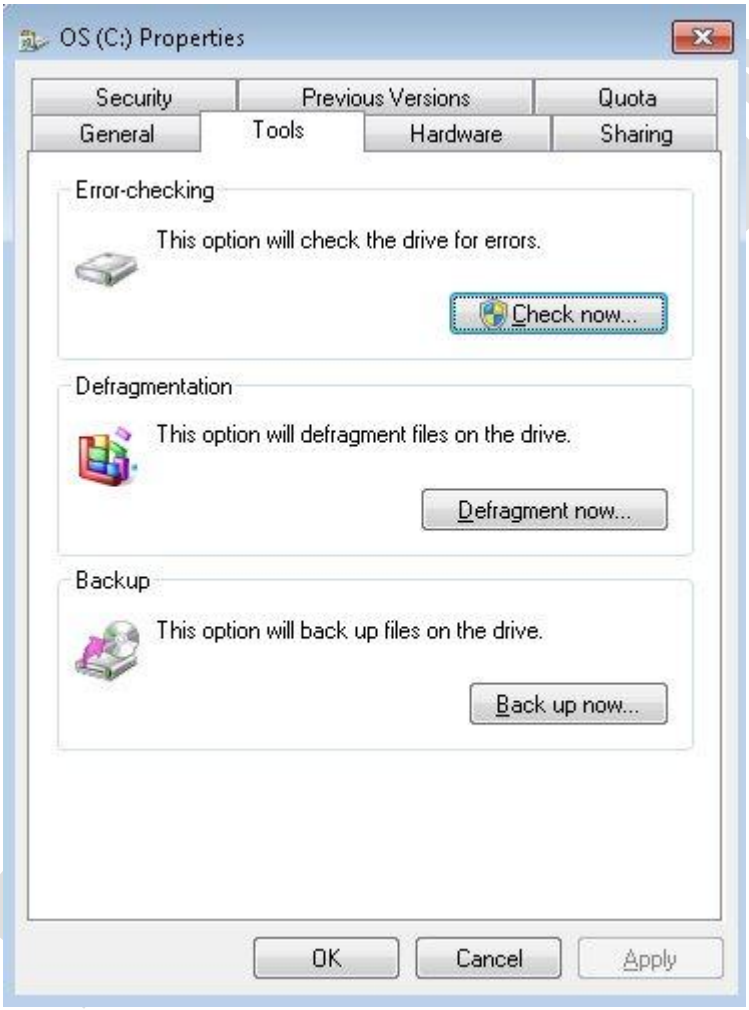
2. Click the *Disk Cleanup* button on the General tab and Windows will calculate how much space it can free up.
3. Select the items from the list that you wish to delete and click *OK*.

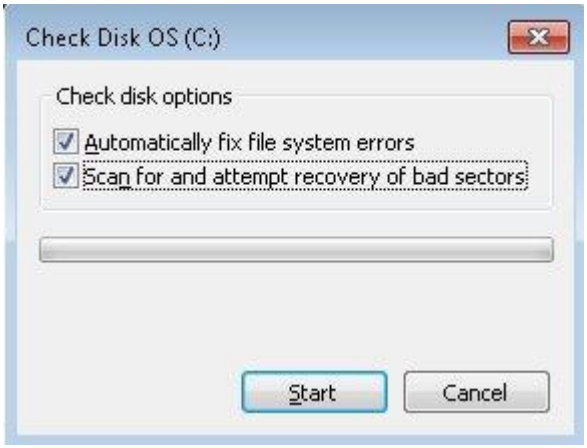


4. When asked "Are you sure you want to permanently delete these files, click *Delete Files*.

As you use your hard drive, it can develop bad sectors. Bad sectors slow down hard disk performance and sometimes make data writing (such as file saving) difficult or even impossible. The Error Checking utility scans the hard drive for bad sectors and scans for file system errors to see whether certain files or folders are misplaced. To scan a disk, follow these steps:

1. Open *Computer*, right click on the drive you wish to check and select *Properties*.
2. Click the *Tools* tab and then click the *Check Now* button.

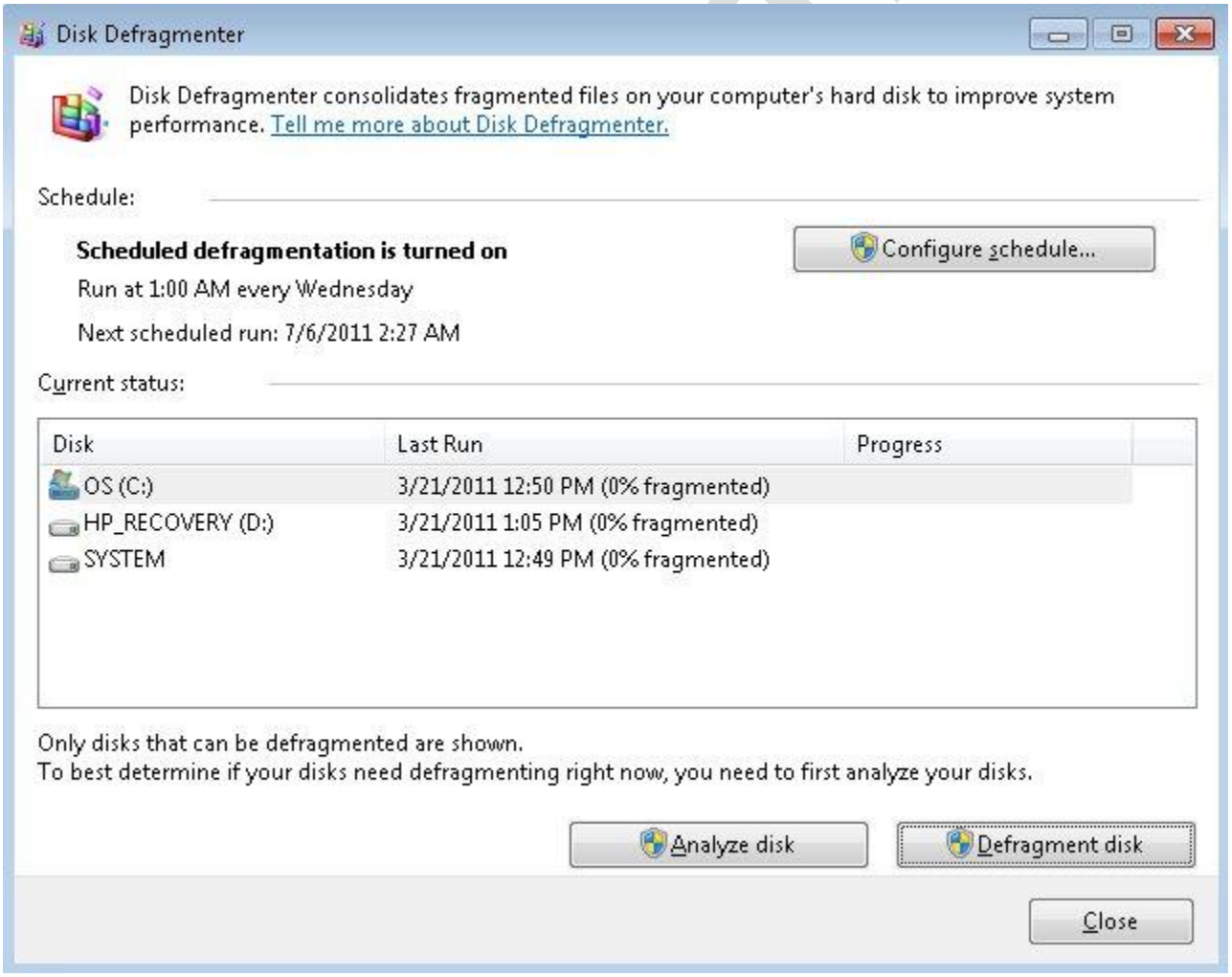




3. Click *Start* to begin checking the drive.

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 rearranges fragmented data so your disks and drives can work more efficiently. Disk Defragmenter runs on a schedule, but you can also analyze and defragment your disks and drives manually. To do this, follow these steps:

1. Open *Computer*, right click on the drive you wish to check and select *Properties*.
2. Click the *Tools* tab and then click the *Defragment Now* button.



3. On the screen shown above, click on *Analyze disk* button to check the drive for fragmentation.
4. If the drive needs to be defragmented, click the *Defragment disk* button. This process can take a long time.

In most cases, manual defragmentation won't need to be done because, by default, this process is scheduled to run every week. By clicking on the *Configure schedule* button on the screen shown above, you can change the interval and select which drives you want automatically defragmented.

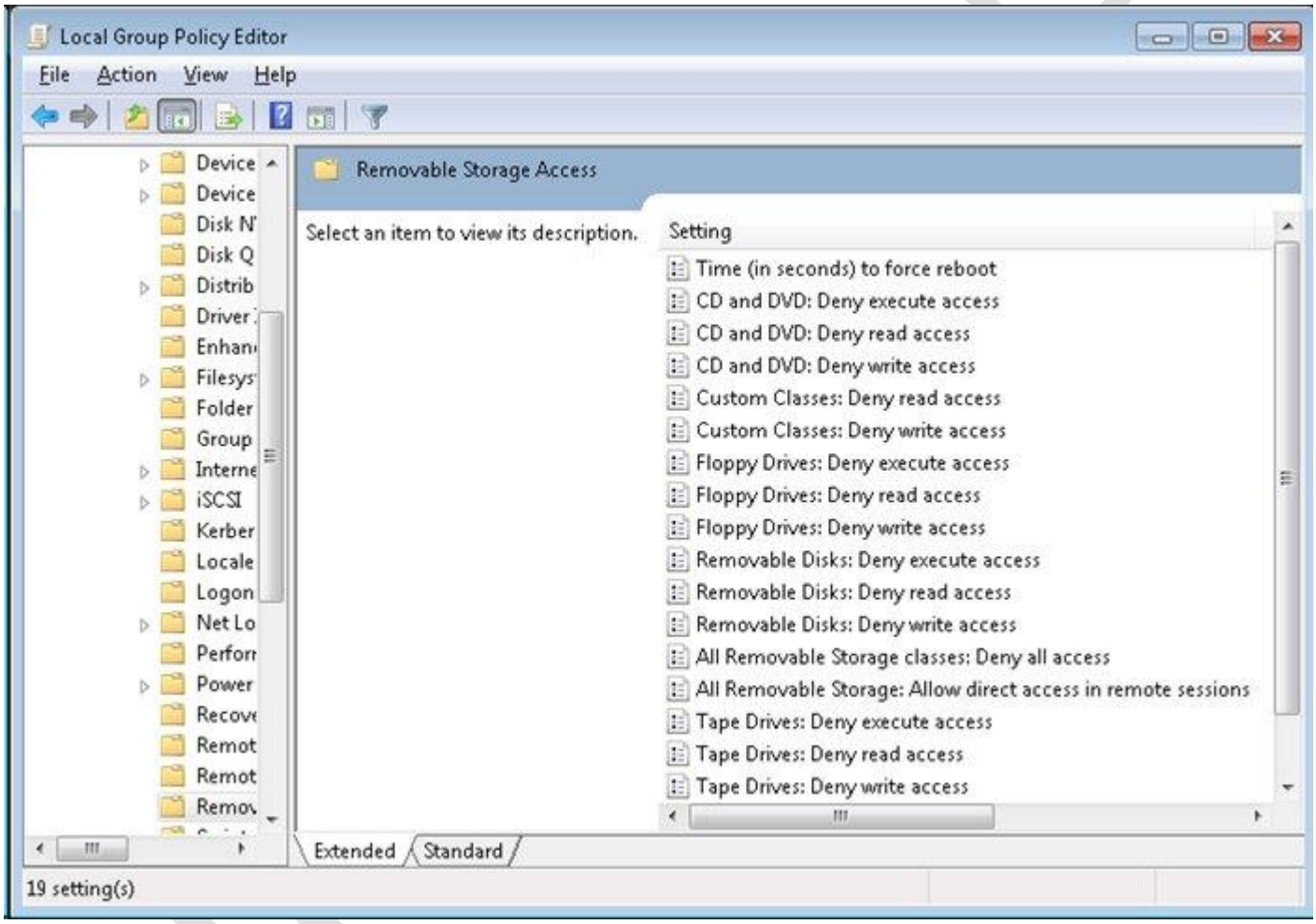
Removable Storage Access Policies:

Removable media can also pose a security threat as it can be lost or stolen, and some administrators may need to lock down client computers' ability to read, write, or execute files on such media. Local and group policy provide a method to prevent or limit users' abilities to interact with removable media. On a stand-alone client computer, you can do this through Local Group Policy Editor. In an enterprise, you would edit domain Group Policy at a domain controller and apply it to all clients in the domain.

To modify these settings in local policy, follow these steps:

1. Click *Start* then type *group policy* into the search box.
2. Click *Edit Group Policy* to open the Local Group Policy Editor.

3. Browse to Computer Configuration/Administrative Templates/System/Removable Storage Access.



4. Here you can double click on a policy to edit it. These are pretty self-explanatory so we won't go into them here.

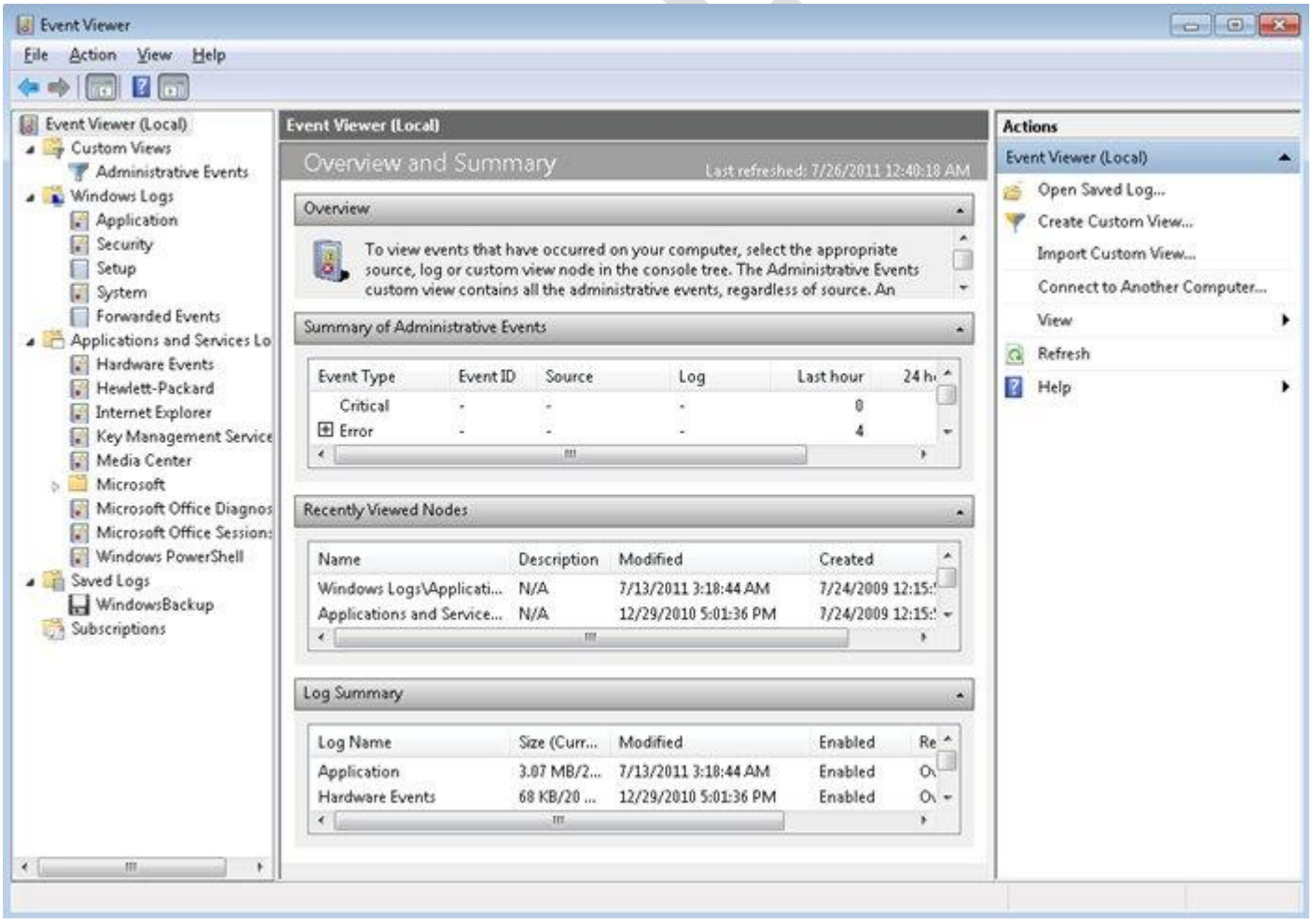
Note: The "WPD devices" policies refer to cell phones, media players, Windows CE devices, etc.

70-680 Study Guide - Monitor Systems

Event Viewer:

Event Viewer is a utility that is used to view and manage logs of system, application, and security events on a computer. Event Viewer gathers information about hardware and software problems and monitors Windows security events.

You must have administrative permission to open the Event Viewer. You can Open Event Viewer by clicking the *Start* button, then *Control Panel*, then *System and Maintenance*, then *Administrative Tools*, and then double-clicking *Event Viewer*. Another way is to click the *Start* button and then type *Event Viewer* into the search box. It is also part of the Computer Management Console. You can also open it by executing eventvwr.msc at a command prompt or using the Run option.



Event Viewer tracks information in several different logs. Windows Logs include:

- **Application** - 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.
- **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.
- **Setup** - This enables you to more easily review the actions that occurred during Windows Setup and to review the performance statistics for different parts of Windows Setup. The Windows Setup performance events are saved into a log file called Setup.etl, which is available in the %WINDIR%\Panther directory of all Windows 7 installations.
- **System** - System events are logged by Windows and Windows system services, and are classified as error, warning, or information.
- **Forwarded Events** - These events are forwarded to this log by other computers.

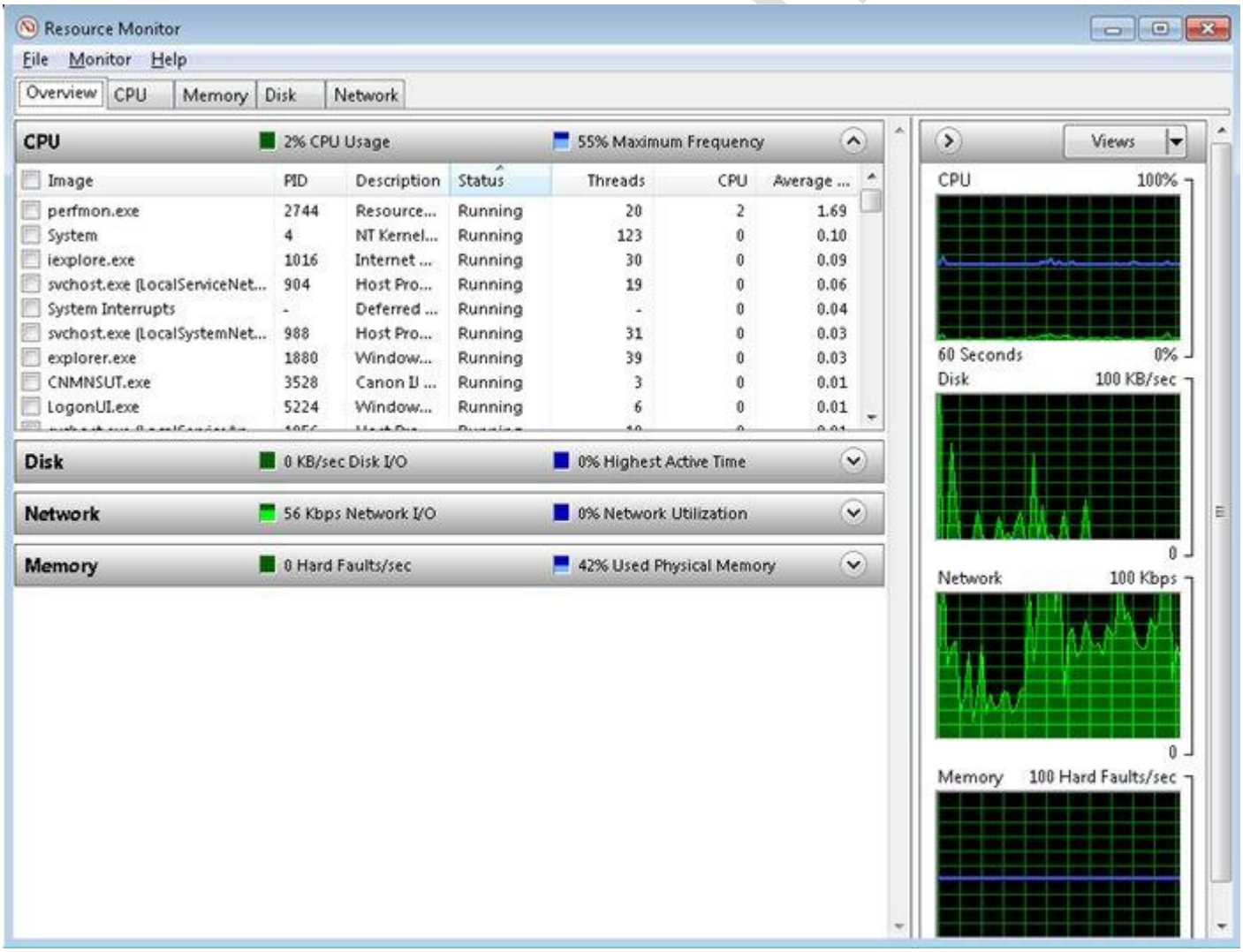
These logs can be very long and tedious to go through. In those cases, you can use the *Filter Current Log* option in the right pane to narrow down the results. Filters are not persistent, however, you can create filters for future use by clicking *Create Custom View* in the right pane. This brings up the same window as the filtering option, however, it stores the view in the Custom Views section of the left pane.

In some situations, it may be necessary to examine the event logs from multiple computers at the same time. In these cases, Windows 7 can be a collector of event logs from other computers, or forward its own event logs to another computer. To learn more about this, read Event Subscriptions.

Resource Monitor:

Windows 7 Resource Monitor provides a quick summary of overall CPU, disk, network and memory utilization. Resource Monitor can be used to see which programs and/or services are consuming Windows 7 system resources, and it is also a good troubleshooting tool if any programs are crashing. In short, Resource Monitor builds on Task Manager by adding more detailed information and graphs in one easy-to-use interface.

To open Resource Monitor, type *resmon* in the Start menu's search box. The default window appears with the Overview tab displayed. In the Overview tab, you can see the four monitored resources -- CPU, disk, network and memory - with their corresponding graphs as shown below.



Click on the CPU, Disk, Network, or Memory bars to expand information about that resource.

Performance Monitor:

The Performance Monitor utility is used to measure the performance of a local or a remote computer on the network. Performance Monitor enables you perform following activities:

- Collect data from your local computer or remote computers on the network. You can collect data from a single computer or multiple computers concurrently.
- View data as it is being collected in real time, or previously collected data.
- You can control data collection by selecting which specific objects and counters will be collected.
- You can choose the sampling parameters (time interval) that will be used, for collecting data points and the time period that will be used for data collection.
- Determine the format in which data will be viewed, that is, in line, histogram bar, or report views.
- Create HTML pages for viewing data.
- Create specific configurations for monitoring data that can then be exported to other computers for performance monitoring.

Windows 7 Performance Monitor includes the new data collector set. This tool works with performance logs, manages where Performance Monitor logs are stored and when the log needs to run. The data collector sets also define the credentials used to run the set.

Data collector sets are used to collect data into a log so that the data can be reviewed. You can view the log files with Performance Monitor. Data collector sets can collect the following data:

- Performance counters
- Event trace data
- System configuration information

Windows 7 includes the following four data collector sets that are stored within the System subfolder:

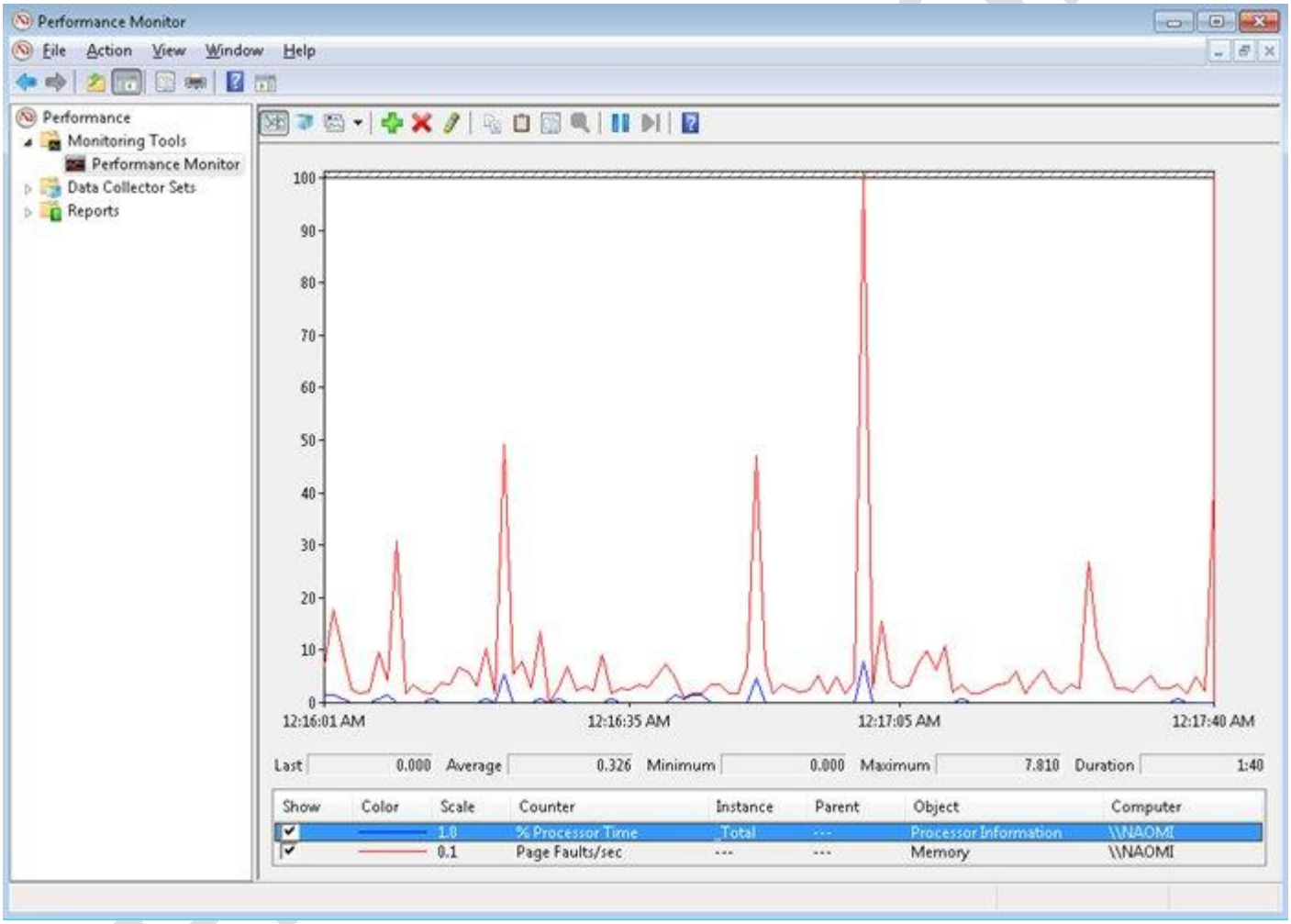
- LAN Diagnostics
- System Diagnostics
- System Performance
- Wireless Diagnostics

Follow these steps to access Performance Monitor:

1. Click *Start*, then click *Control Panel* and then click *System and Security*.
2. Click *Administrative Tools* and then click *Performance Monitor.*

Alternatively, you can click the *Start* button and enter *perfmon* into the search box.

The Overview Of Performance Monitor page is displayed. The System Summary pane of this page gives a snapshot of which resources are being used in your computer. The four initial resources that are tracked are: Memory, Network Interface, Physical Disk, and Processor Information. You can view detailed information about each resource by clicking the Open Resource Monitor link.



Important Performance Monitor Counters:

The following three counters are the three most important counters for monitoring memory:

- **Memory - Available MBytes:** Available MBytes measures the amount of physical memory that is available to run processes on the computer. If this number is less than 20 percent of your installed memory, it indicates that you might have an overall shortage of physical memory for your computer, or you possibly have an application that is not releasing memory properly. You should consider adding more memory or evaluating application memory usage.

- **Memory - Pages/Sec:** Pages/Sec shows the number of times the requested information was not in memory and had to be retrieved from disk. This counter's value should be below 20; for optimal performance, it should be 4 or 5. If the number is above 20, you should add memory. Sometimes a high Pages/Sec counter is indicative of a program that is using a memory - mapped file.
- **Paging File - % Usage:** % Usage indicates the percentage of the allocated page file that is currently in use. If this number is consistently over 70 percent, you might need to add more memory or increase the size of the page file.

You can track processor utilization through the Processor and System objects to determine whether a processor bottleneck exists. The following counters are the most important counters for monitoring the system processor:

- **Processor - % Processor Time:** This measures the time that the processor spends responding to system requests. If this value is consistently above an average of 80 percent, you likely have a processor bottleneck.
- **Processor - Interrupts/Sec:** This shows the average number of hardware interrupts received by the processor each second. If this value is more than 3,000, you might have a problem with a program or hardware that is generating spurious interrupts.

If you suspect that you have a processor bottleneck, you can try the following solutions:

- Use applications that are less processor - intensive.
- Upgrade your processor.
- If your computer supports multiple processors, add a processor.

The important counters for monitoring the disk subsystem are as follows:

- **PhysicalDisk - % Disk Time:** This shows the amount of time the disk is busy because it is servicing read or write requests. If your disk is busy more than 90 percent of the time, you can improve performance by adding another disk channel and splitting the disk I/O requests between the channels.
- **PhysicalDisk - Current Disk Queue Length:** This indicates the number of outstanding disk requests that are waiting to be processed. On average, this value should be less than 2.
- **LogicalDisk % Free Space LogicalDisk:** This specifies how much free disk space is available. This counter should indicate at least 15 percent.

When you suspect to have a disk subsystem bottleneck, then firstly check your memory subsystem. Insufficient physical memory can cause excessive paging, which in turn affects the disk subsystem. If you do not have a memory problem, then you can use following solutions to improve disk performance:

- Use faster disks and controllers.
- Confirm that you have the latest drivers for your disk adapters.
- Use disk striping to take advantage of multiple I/O channels.
- Balance heavily used files on multiple I/O channels.
- Add another disk controller for load balancing.
- Use Disk Defragmenter to consolidate files so that disk space and data access are optimized.

If you are using the Performance Monitor utility to monitor local network traffic, the following two counters are useful for monitoring the network subsystem:

- **Network Interface - Bytes Total/Sec:** This measures the total number of bytes sent or received from the network interface and includes all network protocols.
- **TCPv4 - Segments/Sec:** This measures the number of bytes sent or received from the network interface and includes only the TCPv4 protocol.

You can use the following to optimize and minimize network traffic and to enhance network performance on your system:

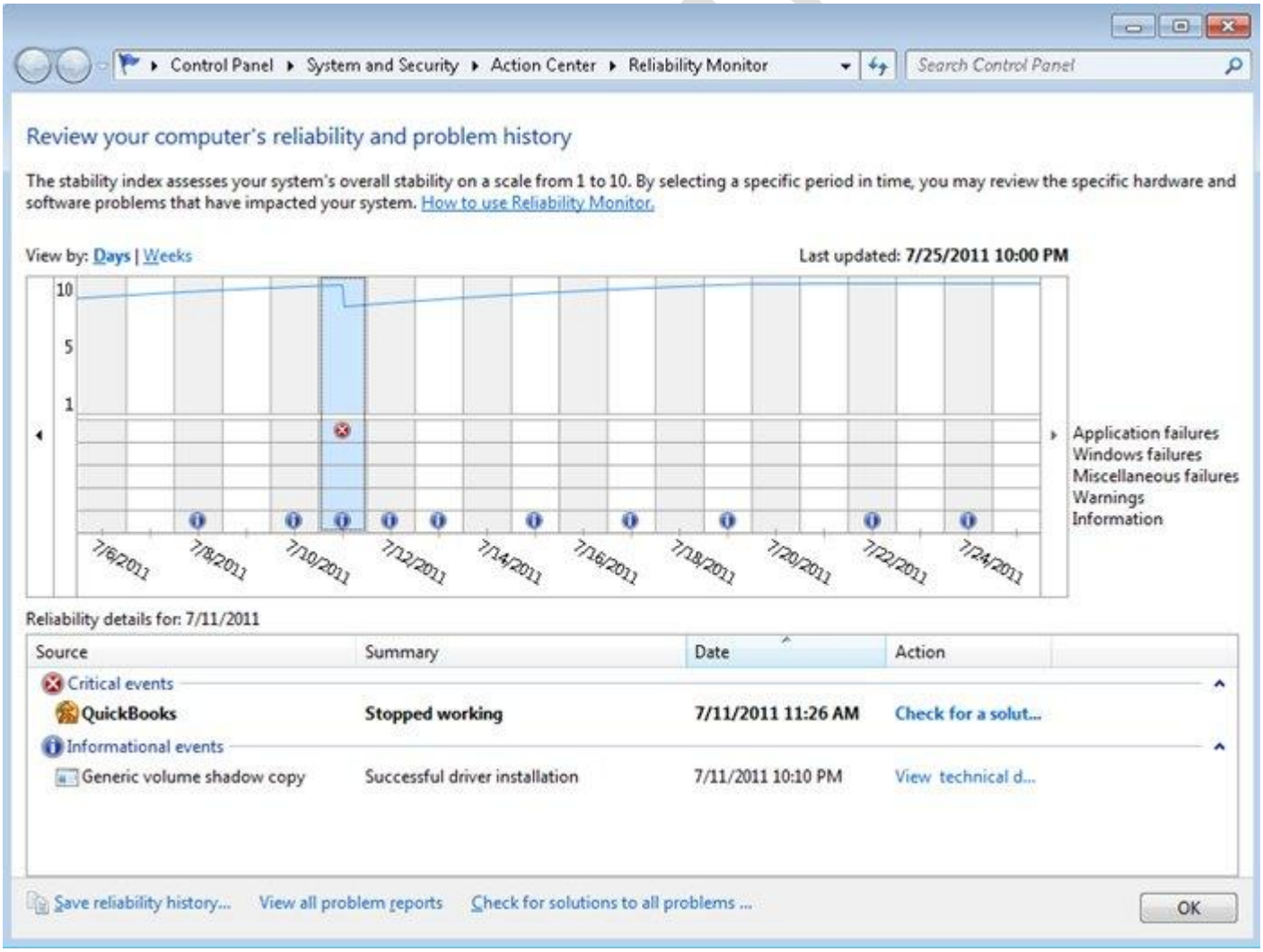
- Install and configure only the network protocols you need.
- Use network cards that take advantage of your bus speed.
- Use faster network cards. for example, 100 Mbps Ethernet or 1 Gbps Ethernet instead of 10 Mbps Ethernet.

Reliability Monitor:

Reliability Monitor is an advanced tool that measures hardware and software problems and other changes to your computer. It provides a stability index that ranges from 1 (the least stable) to 10 (the most stable). You can use the index to help evaluate the reliability of your computer. Any change you make to your computer or problem that occurs on your computer affects the stability index. To open the Reliabilty Monitor, follow these steps:

1. Click *Start*, then choose *Control Panel*. Next click *Action Center*.
2. Click *Maintenance*. Then, under *Check for solutions to problem reports*, click *View reliability history*.

A faster way to access this is to click *Start* and enter *perfmon /rel* in the search box.



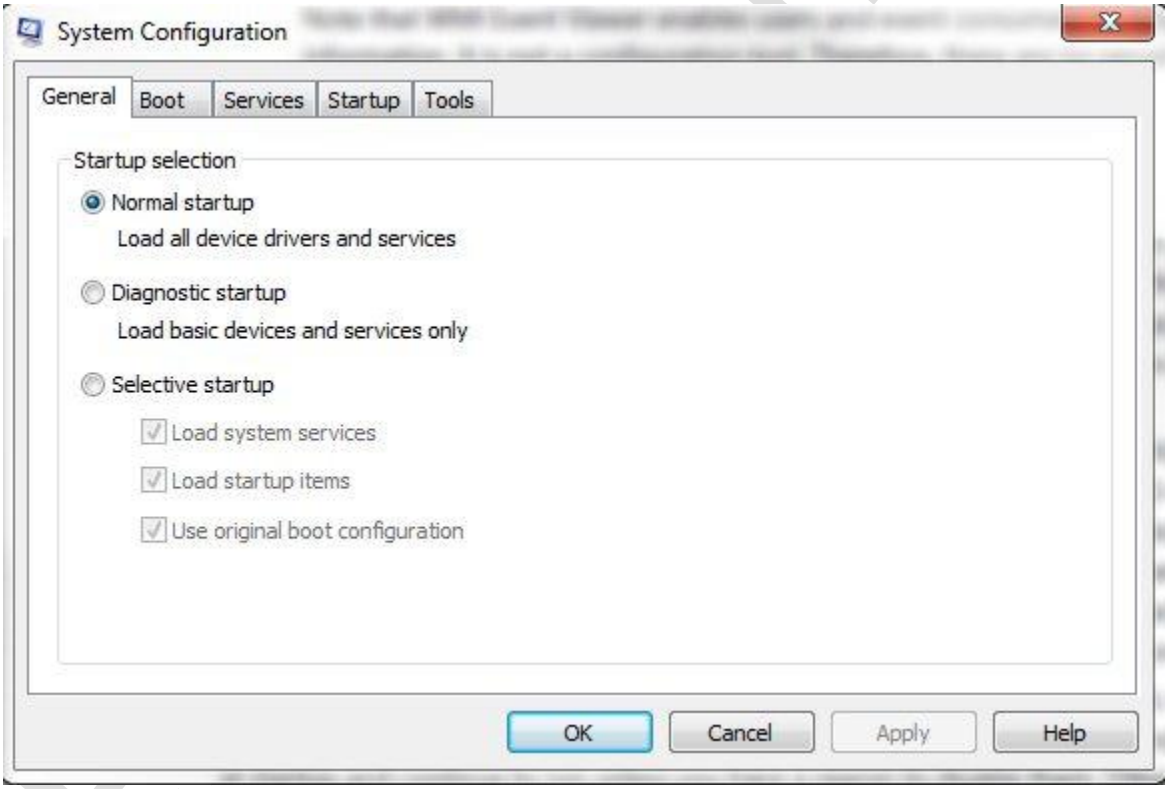
In Reliability Monitor, you can:

- Click any event on the graph to view its details.
- Click *Days*, or *Weeks*, to view the stability index over a specific period of time.
- Click items in the Action column to view more information about them.
- Click *View all problem reports* to view only the problems that have occurred on your computer. This view does not include the other computer events that show up in Reliability Monitor, such as events about software installation.

70-680 Study Guide - Configure Performance Settings

System Configuration Tool:

The system configuration tool is mainly used for troubleshooting startup issues and can be accessed by entering *msconfig* in the Start menu searchbox.



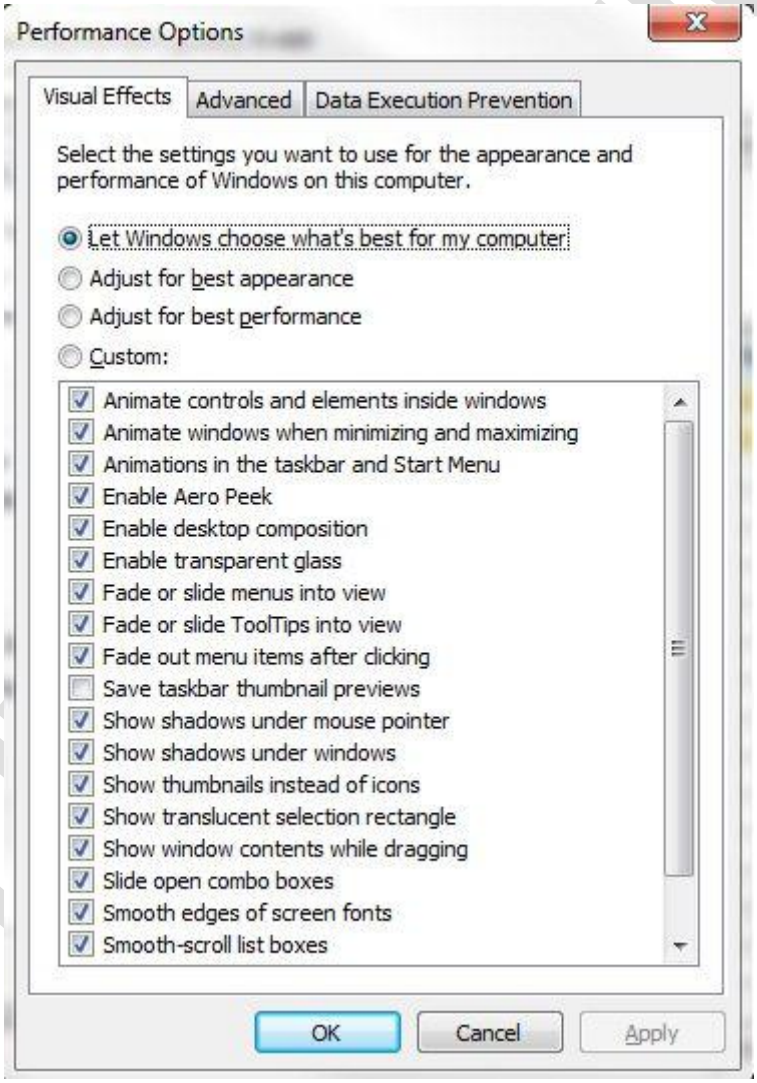
System Configuration can disable or re-enable software, device drivers and Windows services that run at startup, or change boot parameters. Stopping services and/or applications from running at startup can not only solve startup issues, it can improve overall performance by preventing unnecessary items from automatically running and consuming resources.

From the tools tab, you can launch many other Windows 7 built-in troubleshooting tools.

Performance Options:

To access performance options, follow these steps:

1. Click *Start*, then *Control Panel*.
2. Next, click *System and Security*.
3. Click *System*.
4. Click *Advanced System Settings* in the left pane.
5. Click *Settings* in the Performance section to display the Performance Options dialog box.



The performance options tool has a couple of noteworthy settings to look at. The visual effects tab allows you to configure the effects used by Windows. If Windows is running slowly, you can speed it up by disabling some of its visual effects. By default, Windows chooses what it thinks is best, but this can be changed to *Adjust for best appearance* (slower and prettier) or *Adjust for best performance* (faster and uglier). The other option is to select *Custom* and choose the specific effects to turn off. There are 20 visual effects you can control, such as the

transparent glass look, the way menus open or close, and whether shadows are displayed.

The Advanced tab of the Performance Options dialogue box has two sections; Processor Scheduling and Virtual Memory (discussed in the next section below).

In most cases, a Windows 7 computer will be used to run programs for a user, however, in some cases, a workstation may be dedicated to a particular tasks such as a print server. The default processor scheduling setting is set so that user programs are given a higher priority than those running in the background. However, if you have a Windows 7 workstation that is dedicated to a specific task, such as monitoring an assembly line or acting as a print server, you can have Windows share processor resources equally between background and foreground programs by checking the *Background Services* radio button.

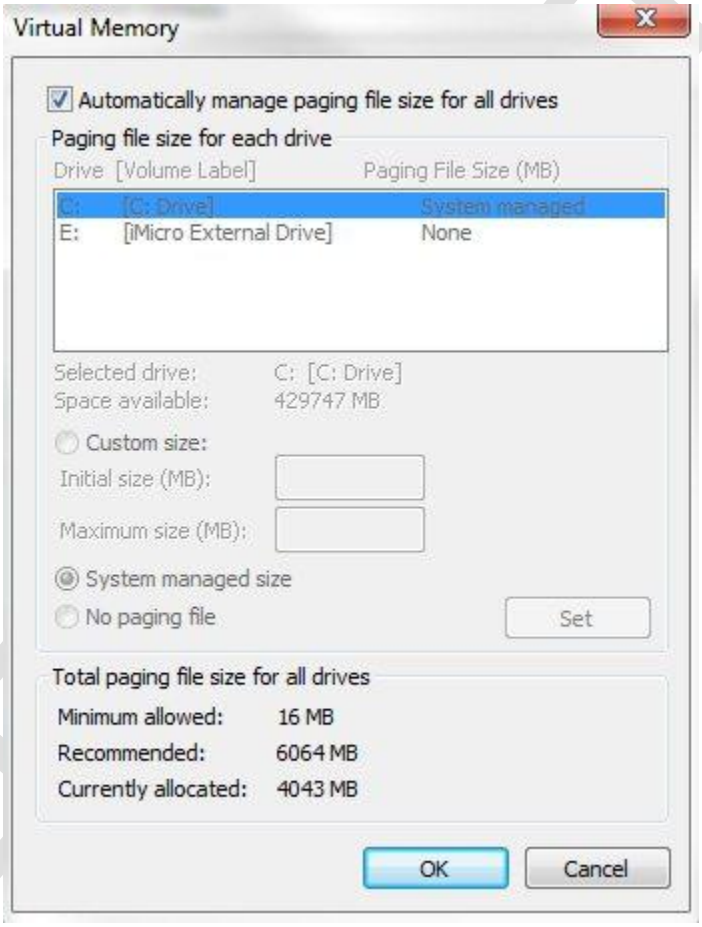
Configuring Virtual Memory:

Manually configure virtual memory usage by completing the following steps:

1. Click *Start*, then *Control Panel*.
2. Next, click *System and Security*.
3. Click *System*.
4. Click *Advanced System Settings* in the left pane.
5. Click *Settings* in the Performance section to display the Performance Options dialog box.
6. Click the *Advanced* tab, and then click *Change* to display the Virtual Memory dialog box.
7. Uncheck the *Automatically manage paging file size for all drives* checkbox.
8. In the list of drives, click the drive that contains the paging file you want to change.
9. Click *Custom size*, and enter a new size in megabytes in the Initial size (MB) or Maximum size (MB) boxes.
10. Click *Set*, and then click *OK*.

If you would like to change the location of your paging file, follow steps 1-8 above and then the following:

- Click the *No paging file* radio button.
- Next, select the hard drive you would like to store your paging file on and choose *System managed size*.
- Click *OK*. Changes won't take effect until you restart your computer.



ReadyBoost:

Windows 7 supports Windows ReadyBoost. This feature uses external USB flash drives as a hard disk cache to improve disk read perfor¬mance. Supported external storage types include USB thumb drives, SD cards, and CF cards. Since ReadyBoost will not provide a perfor¬mance gain when the primary disk is an SSD, Windows 7 disables ReadyBoost when reading from an SSD drive.

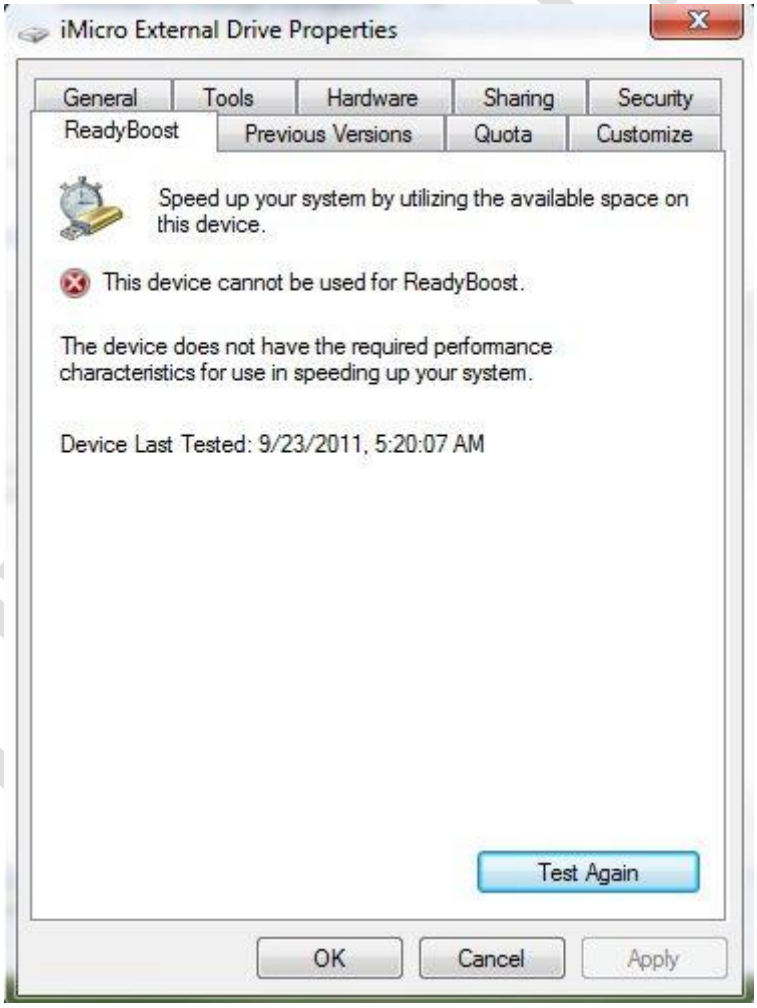
ReadyBoost offers the most improvement in the following situations:

- You have a slow hard disk drive. Computers with a primary hard disk Windows Experience Index (WEI) subscore lower than 4.0 will see the most improvement.
- The flash storage provides fast, random, non-sequential reads. Sequential read speed is less important.
- The flash storage is connected by a fast bus. Typically, USB memory card readers are not sufficiently fast. However, connecting flash memory to an internal memory card reader might provide sufficient performance.

External storage must meet the following requirements:

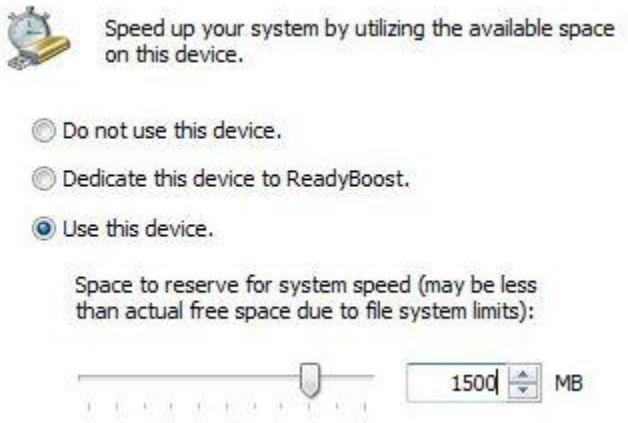
- Capacity of at least 256 MB, with at least 64 kilobytes (KB) of free space.
- At least a 2.5 MB/sec throughput for 4-KB random reads
- At least a 1.75 MB/sec throughput for 1-MB random writes

The easiest way to tell if a drive meets the specs is to test it. If the device is not compatible, you will see this:



You can configure ReadyBoost by right-clicking the device in Explorer, selecting *Properties*, and then clicking the *ReadyBoost* tab. You can also get here via the Autorun dialogue box when the device is connected if your device

is ReadyBoost capable. The only configuration options are to enable ReadyBoost on the drive and set the space reserved for the cache.



The minimum you can reserve is 256 MB. Larger caches can improve performance, but the ReadyBoost cache cannot be greater than 4 GB on a FAT32 file system or greater than 32 GB on NTFS. For best results, the drive should have available space 2x greater than the amount of RAM in the computer.

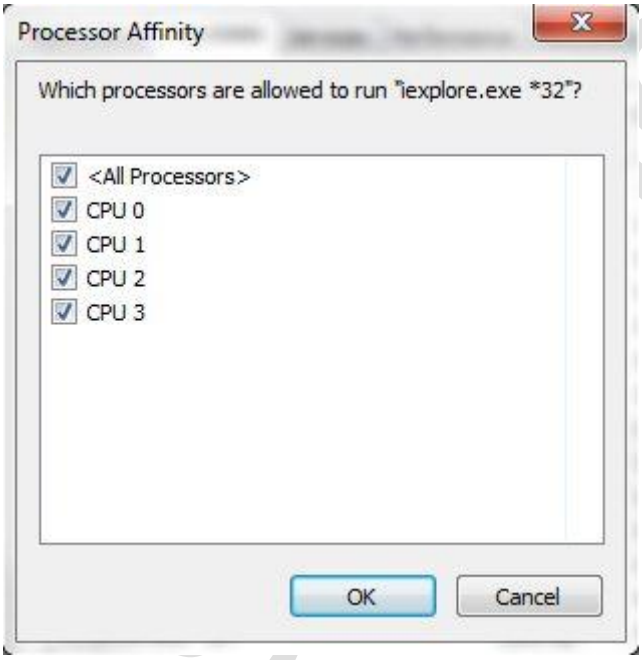
ReadyDrive:

ReadyDrive improves performance on mobile computers with hybrid drives - a drive that uses both flash RAM and physical drive for storage. Because flash RAM is faster than a physical disk, Windows 7 can write data (and changes to data) to flash memory first and then periodically sync to the physical disk. This reduces the spinning of the physical drive, saves battery power, provides faster startup, and faster resuming from sleep/hibernation. ReadyDrive is enabled by default on mobile computers with hybrid drives.

Processor Affinity:

If your computer has more than one processor, you can configure the affinity of your processes to use particular processors. By default, processes that install on a multiprocessor computer are set to use whatever processor is available. If an additional processor is added later to a computer, however, processes might require configuration so that they use the new processor. If Task Manager shows that one processor on a multi-processor computer is heavily used and the others are not, you should change the affinity of your intensive processes use all processors. To find out which process or processes are being used by a service, right-click the service in the Services tab of Task Manager and click *Go To Process*. This selects the Processes tab and

highlights the relevant process. To set the affinity for a process, right click on it and select *Set Affinity*. Then check the processors you wish for this process to use.



Windows Performance Toolkit:

For the exam you may need to know how to use the Windows Performance Toolkit (WPT) which is part of the Windows SDK for Windows 7. This kit contains the following tools:

- Trace Capture, Processing, and Command-Line Analysis tool (Xperf.exe)
- Visual Trace Analysis tool (Xperfview.exe)
- On/Off Transition Trace Capture tool (Xbootmgr.exe)

70-680 Study Guide - Configure Backup

System Recovery Options:

System recovery options are a set of tools you can use to repair Windows if a serious error occurs. To open the System Recovery Options menu, follow these steps:

1. Remove all floppy disks, CDs, etc, and restart your computer.
2. Press and hold the *F8* key while your computer restarts (before the Windows logo appears).
3. On the Advanced Boot Options screen, use the arrow keys to highlight *Repair your computer* and then press *Enter*. If this option isn't available, your computer doesn't have the recovery options installed and you will need to get them from the Windows installation disk.
4. Select a keyboard layout and then click *Next*.

Note: If your computer has more than one operating system, use the arrow keys to select the operating system you want to repair, then press and hold F8.

After performing these steps, you will see the screen below:

On this screen you can access the following tools:

- **Startup Repair:** Fixes certain problems, such as missing or damaged system files, that might prevent Windows from starting correctly. Startup Repair isn't designed to fix Windows installation problems, nor is it a backup tool, so it can't help you recover personal files, such as photos or documents.
- **System Restore:** Restores your computer's system files to an earlier point in time without affecting your files, such as e-mail, documents, or photos. Restore points are created automatically every week, and just before significant system events, such as the installation of a program or device driver. You can also create a restore point manually.
- **System Image Recovery:** You need to have created a system image beforehand to use this option. A system image is a personalized backup of the partition that contains Windows, and includes programs and user data. A system image is an exact copy of a drive.
- **Windows Memory Diagnostic Tool:** Scans your computer's memory for errors.
- **Command Prompt:** Self-explanatory.

System Repair Disc:

If the system recovery options are not installed on your computer, and you do not have access to the Windows installation disk, you can gain access to the tools above by creating a system repair disc. To do this, follow these steps:

1. Click *Start*, then click *Control Panel*, click *System and Maintenance*, and then click *Backup and Restore*.
2. In the left pane, click *Create a system repair disc*. You may be prompted for an administrator password or confirmation.
3. Insert a disc into the drive, and click *Create disc*.

To use your system repair disc, follow these steps:

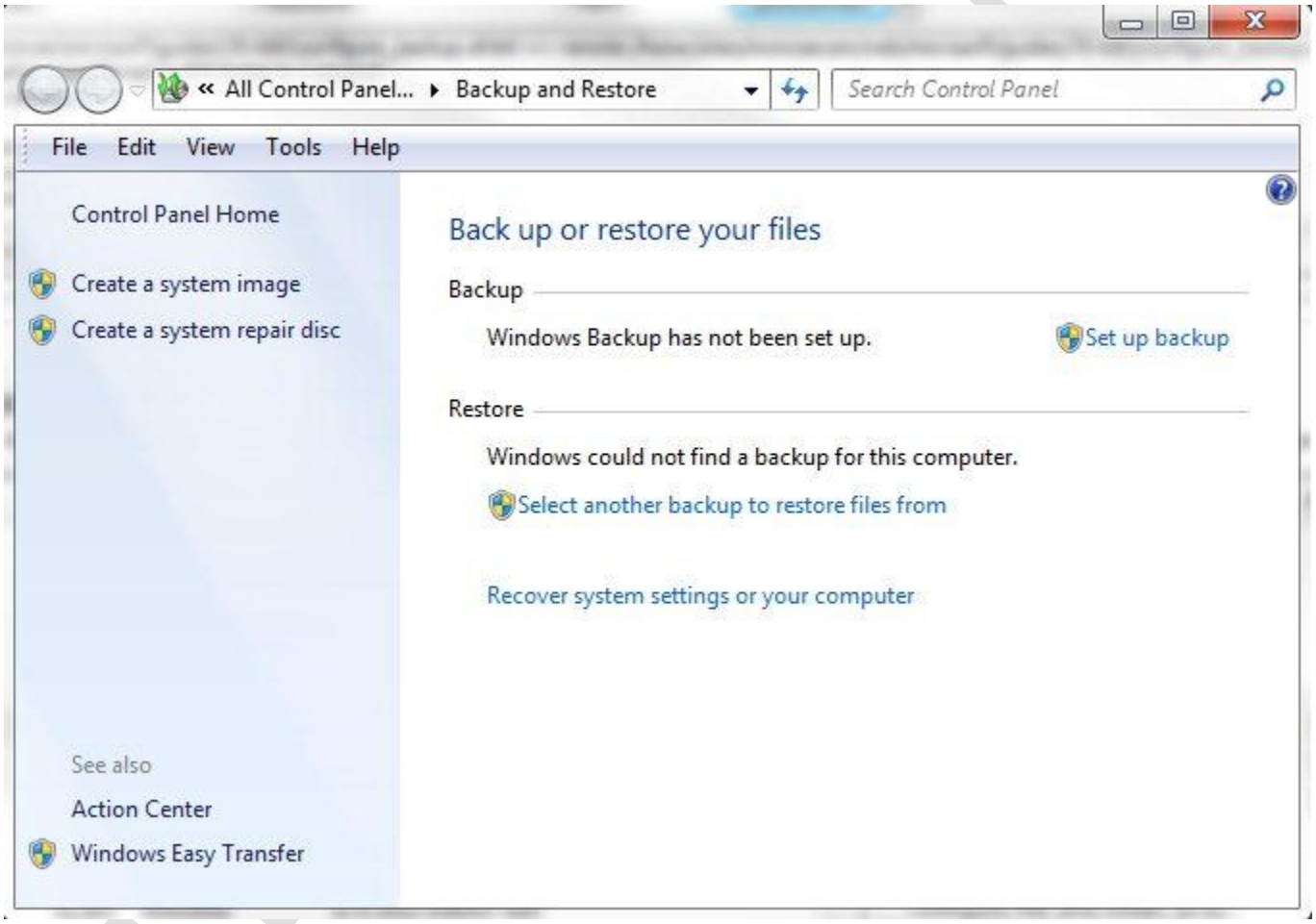
1. Insert the system repair disc into your CD or DVD drive.
2. Restart your computer using the computer's power button.
3. If prompted, press any key to start the computer from the system repair disc. If your computer isn't configured to start from a CD or DVD, you may need to change your computer's BIOS settings.
4. Choose your language settings, and then click *Next*.

These steps will display the system recovery options box discussed in the previous section.

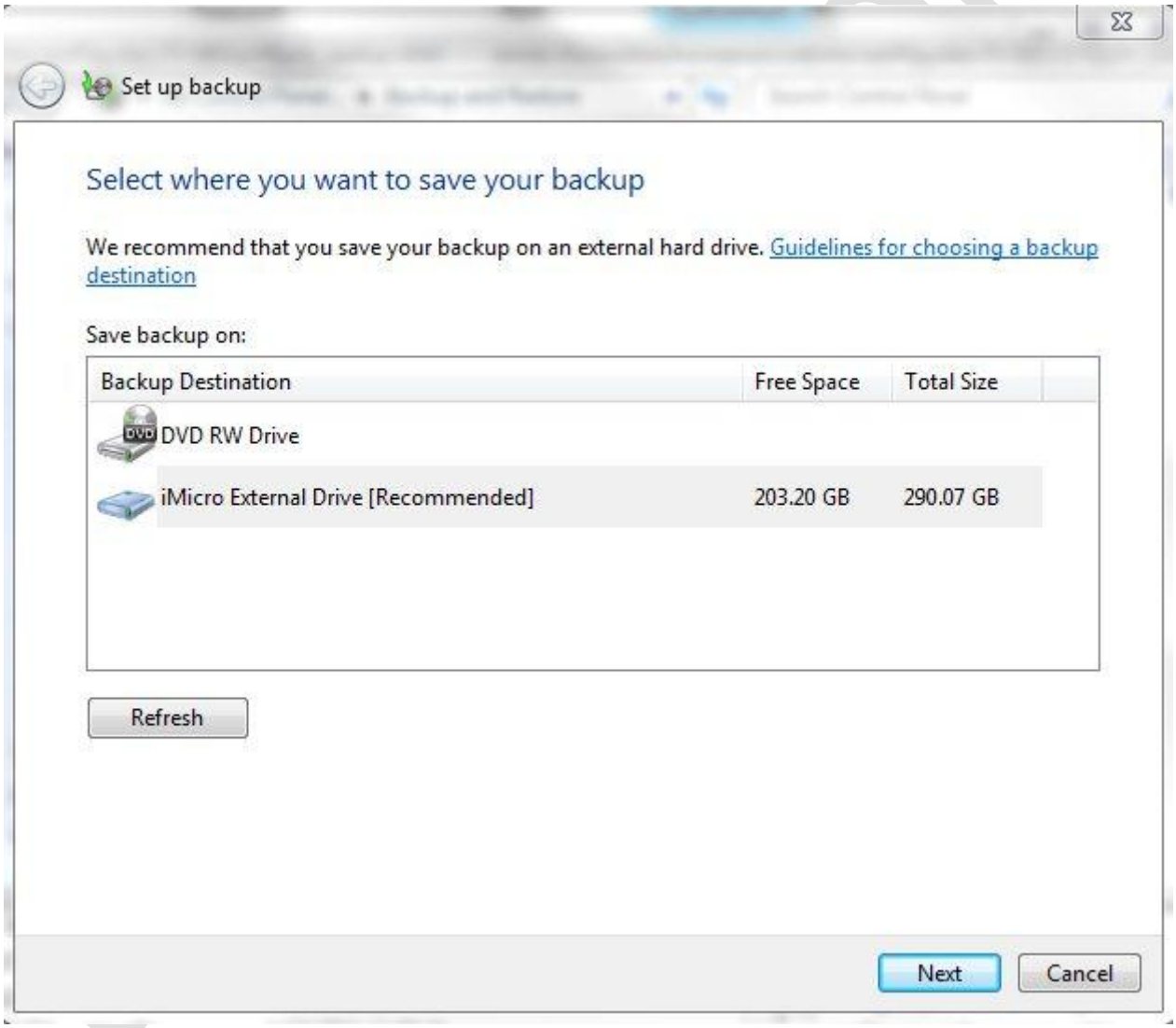
Configuring Backups:

The Windows 7 Backup and Restore utility enables you to create and restore backups. Backups protect your data in the event of system failure by storing the data on another medium, such a hard disk, CD, DVD, or network location. If your original data is lost because of corruption, deletion, or media failure, you can restore the data by using your saved backup. Windows 7 Backup uses shadow copies to take a snapshot of your files, allowing the backup to completely back up files even if they are open. Follow these steps to configure backup:

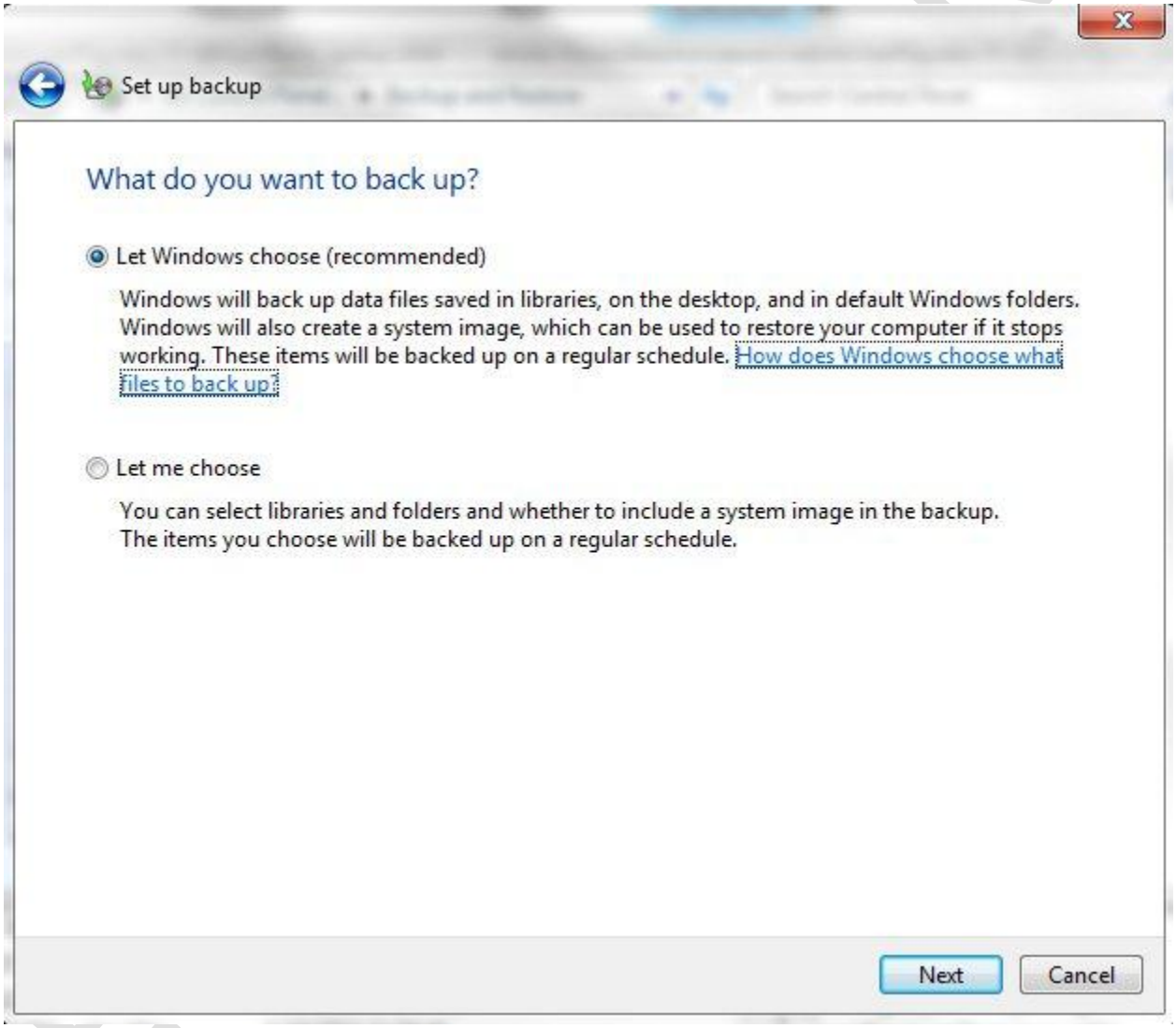
1. Click *Start*, and then enter *backup* in the search box.
2. Select *Backup and Restore* from the results to launch the Backup and Restore applet.
3. In the Back up or restore your files window, click the *Set up backup* link.



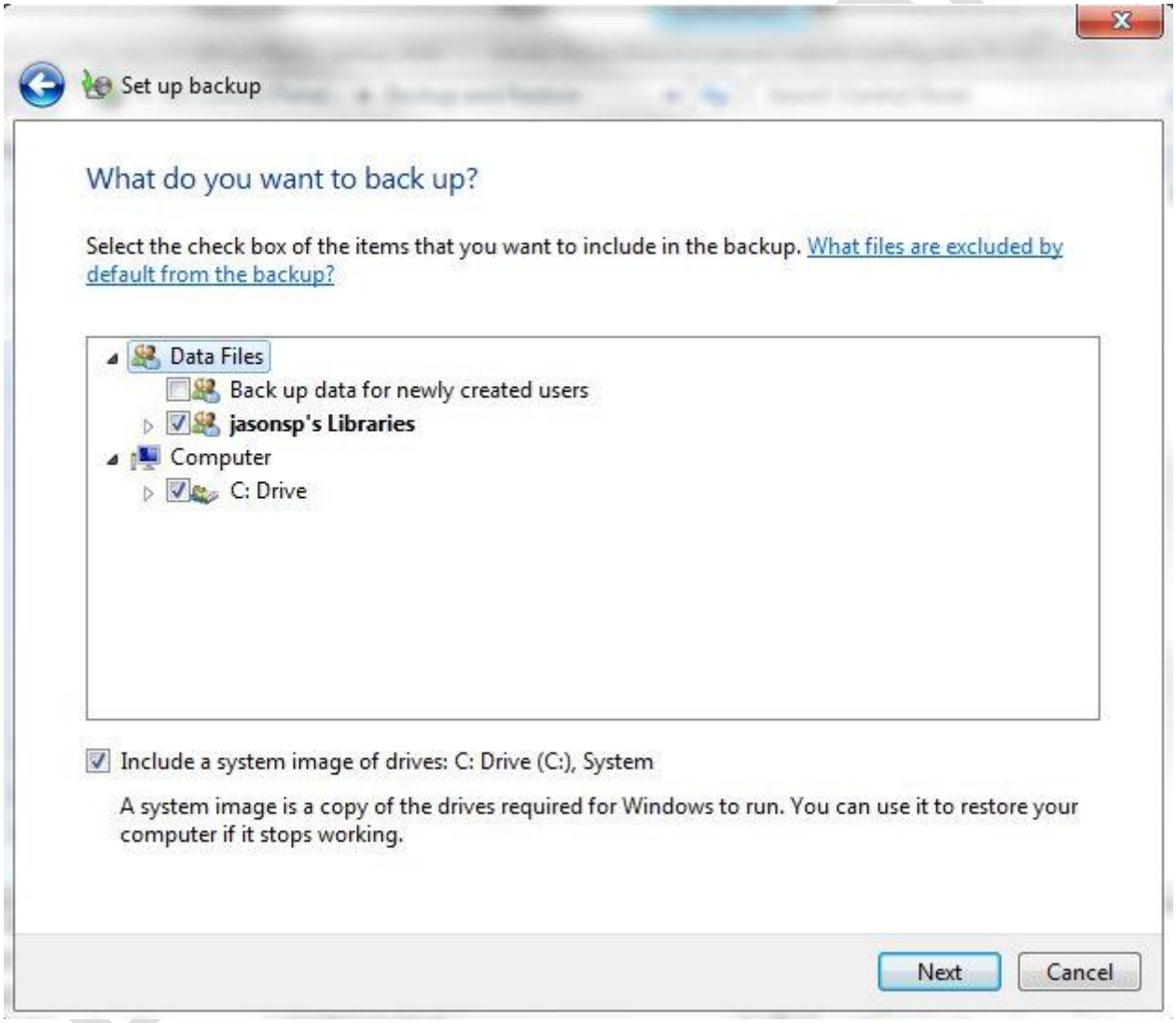
4. Windows will search for appropriate drives to store the backup and you can also choose a location on your network. Note: you cannot select a destination that has Bitlocker enabled. After selecting the backup destination, click *Next*.



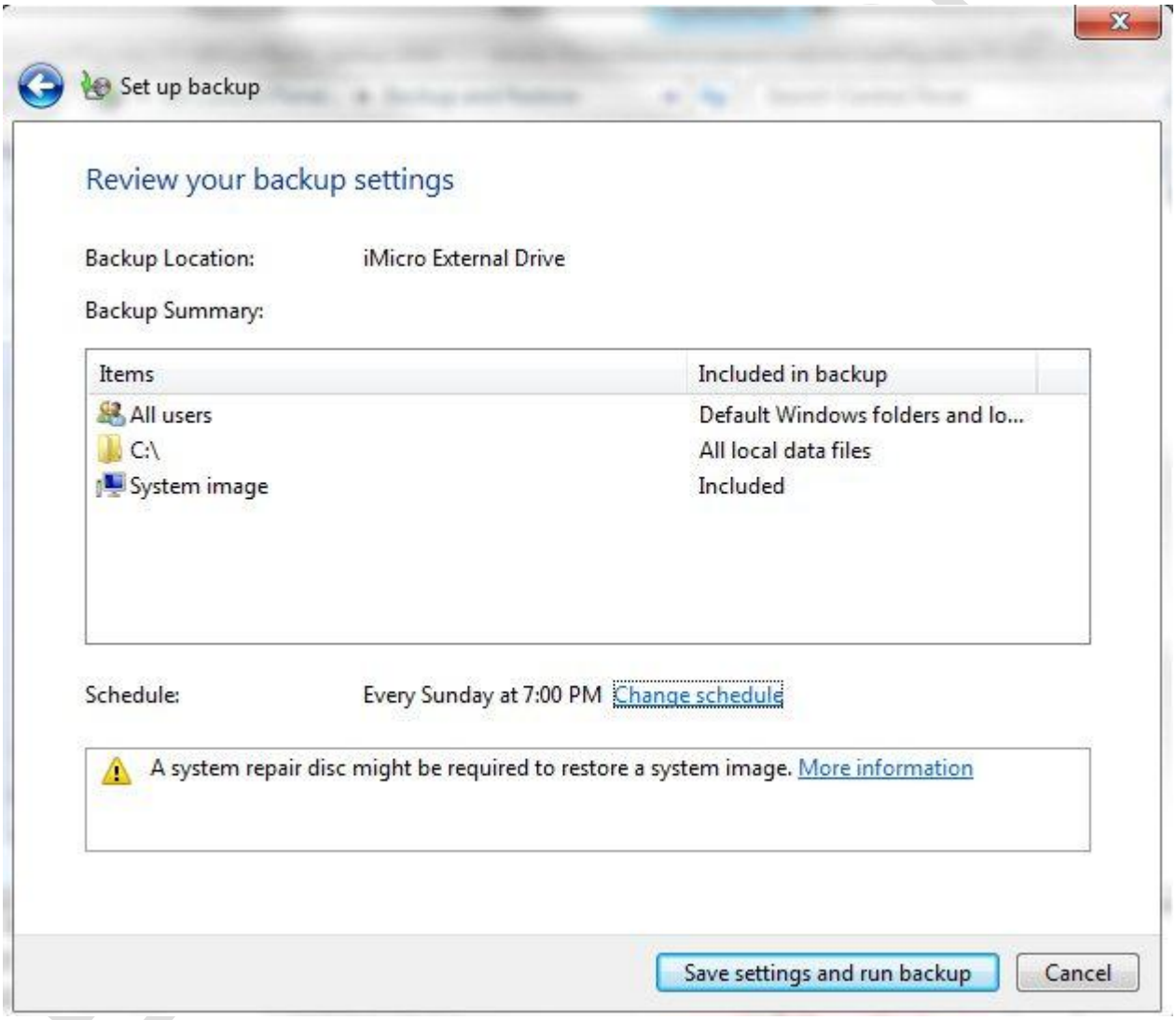
5. On the next screen you have the option to let Windows choose which files or folders to backup, or you can select *Let me choose* and select the files and folders yourself.



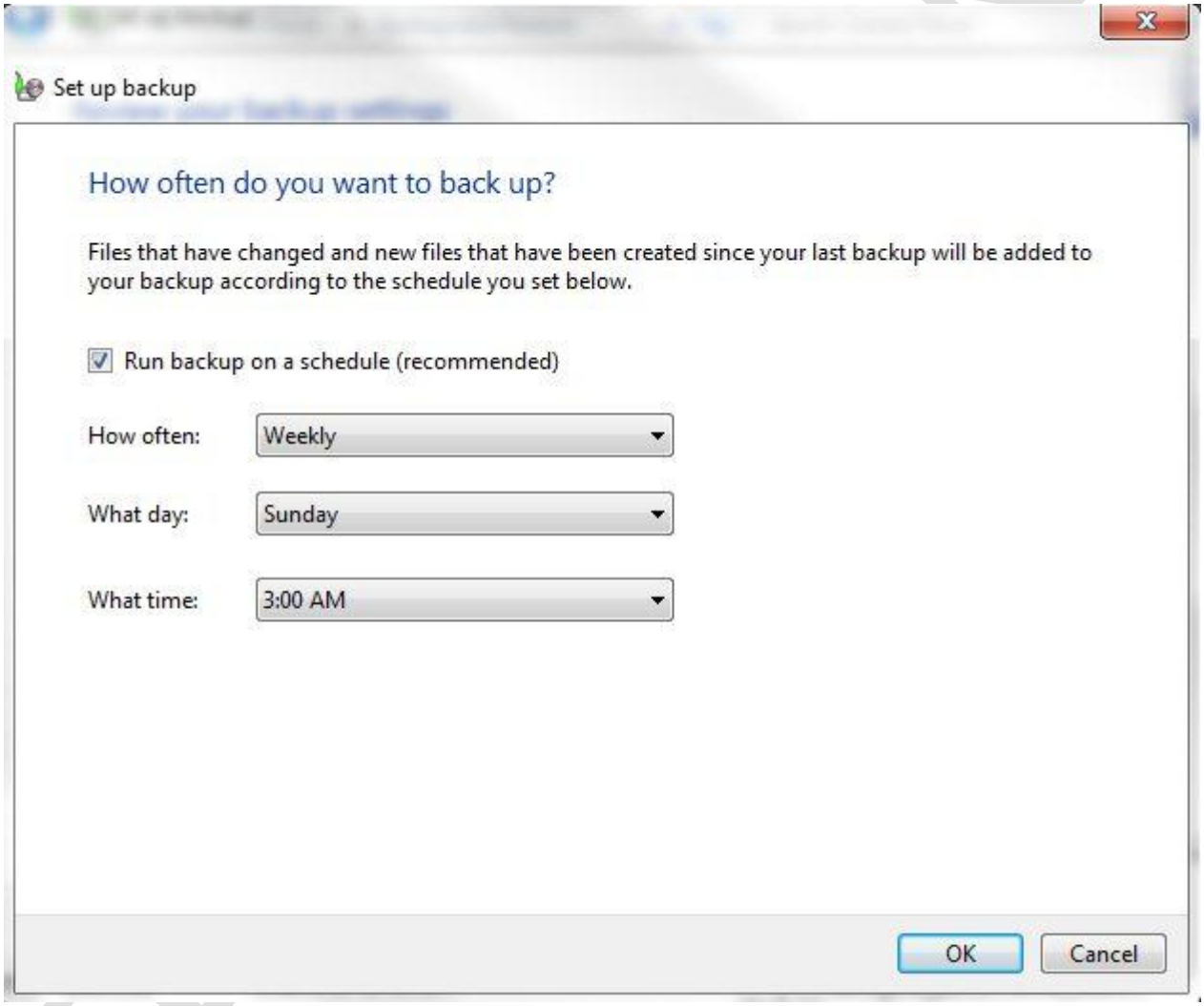
6. If you chose *Let me choose* on the previous screen, select the files and folder to be included in the backup. You can also select the option to create a system image of your local drive which is stored in VHD format.



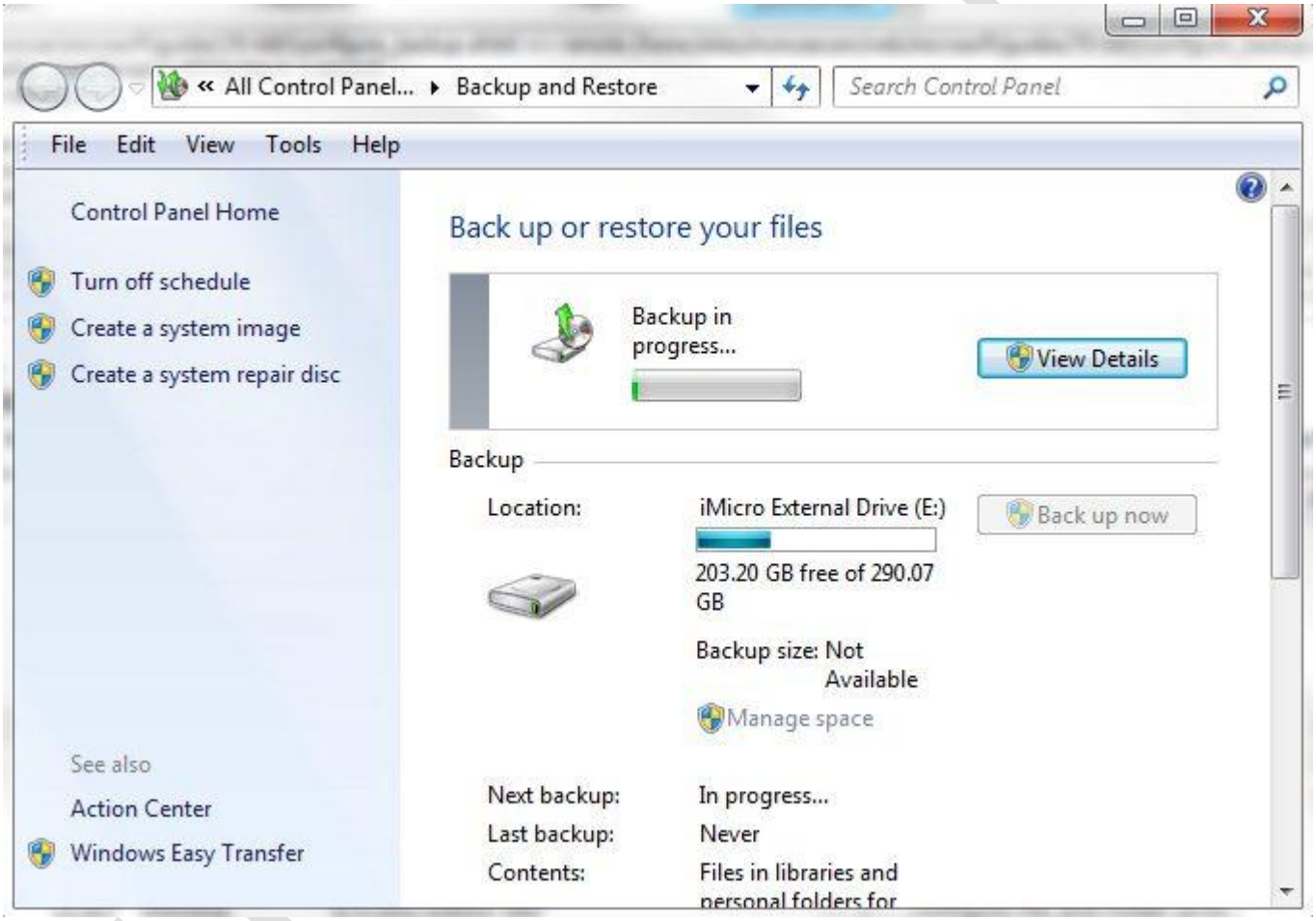
7. Review the backup job to ensure that backup includes all the required files and folders. You can also click the *Change schedule* link to configure the days and times for future automated backups. Note that system image backups are not performed during scheduled backups.



8. If you selected *Change schedule*, set the interval, day and time you would like your backups to run and click *OK*.



9. After setting the schedule, click *Save settings and run backup*.
10. You will be taken back to the Backup and Restore control panel which will allow you to monitor the progress.



The first backup performed is a full backup, while subsequent backups are incremental, and only backup files that have changed since the last backup.

There are several media types that can be used for backups as follows:

- **External hard drive** - You cannot use an external hard drive for a System Image backup unless the filesystem is NTFS.
- **USB flash drives** - You cannot save System Image backups to a flash drive. A flash drive must at least 1 GB of free space to store a backup.
- **DVDs** - DVDs are inexpensive, however it will likely take several DVDs to complete a single backup. You cannot save scheduled System Image backups on DVDs.

- **Network location** - In order to backup to a network location, you will need the username and password to the share, and you also must be running Windows 7 Professional or higher.
- **VHD** - In Windows 7, you can specify a VHD as a backup location. You can also carry out a System Image backup of an entire volume to a VHD disk image file. On Windows 7 Ultimate and Enterprise editions, you can use the Bcdedit tool to make a VHD bootable so you can boot the computer from a backed-up system image.

70-680 Study Guide - Configure System Recovery Options

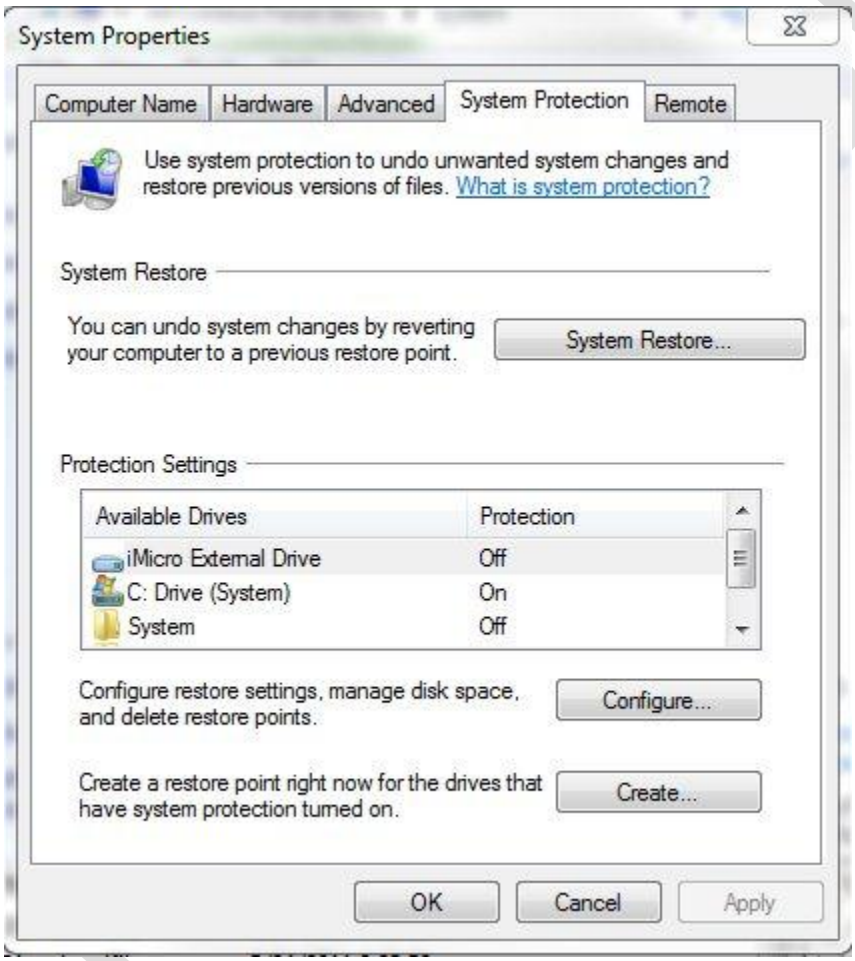
Note that some objectives for this section were covered in the previous one and will not be discussed again here.

System Restore:

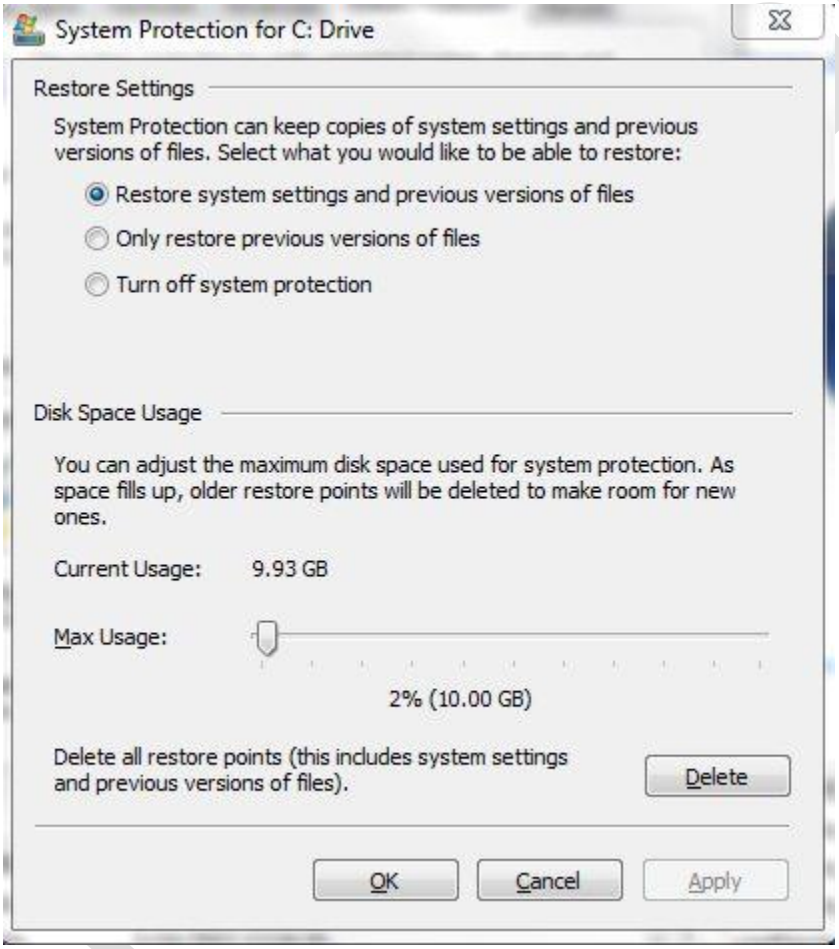
Windows 7's System Protection utility creates system restore points automatically every week, and just before significant system events, such as the installation of a program or device driver. You can also create a restore point manually. A restore point contains information about registry settings and other system information, but does not include user files. System Protection is enabled by default and is only available on NTFS drives.

If you have recently installed an application or driver that causes problems, you should try uninstalling the program or rolling back the driver. If this does not fix the problem, then you should try restoring the computer to its last system restore point.

There are a couple of different ways to access the system restore utility. You can manage System Protection and the restore points from the *System Protection* tab of the System Properties dialog box.

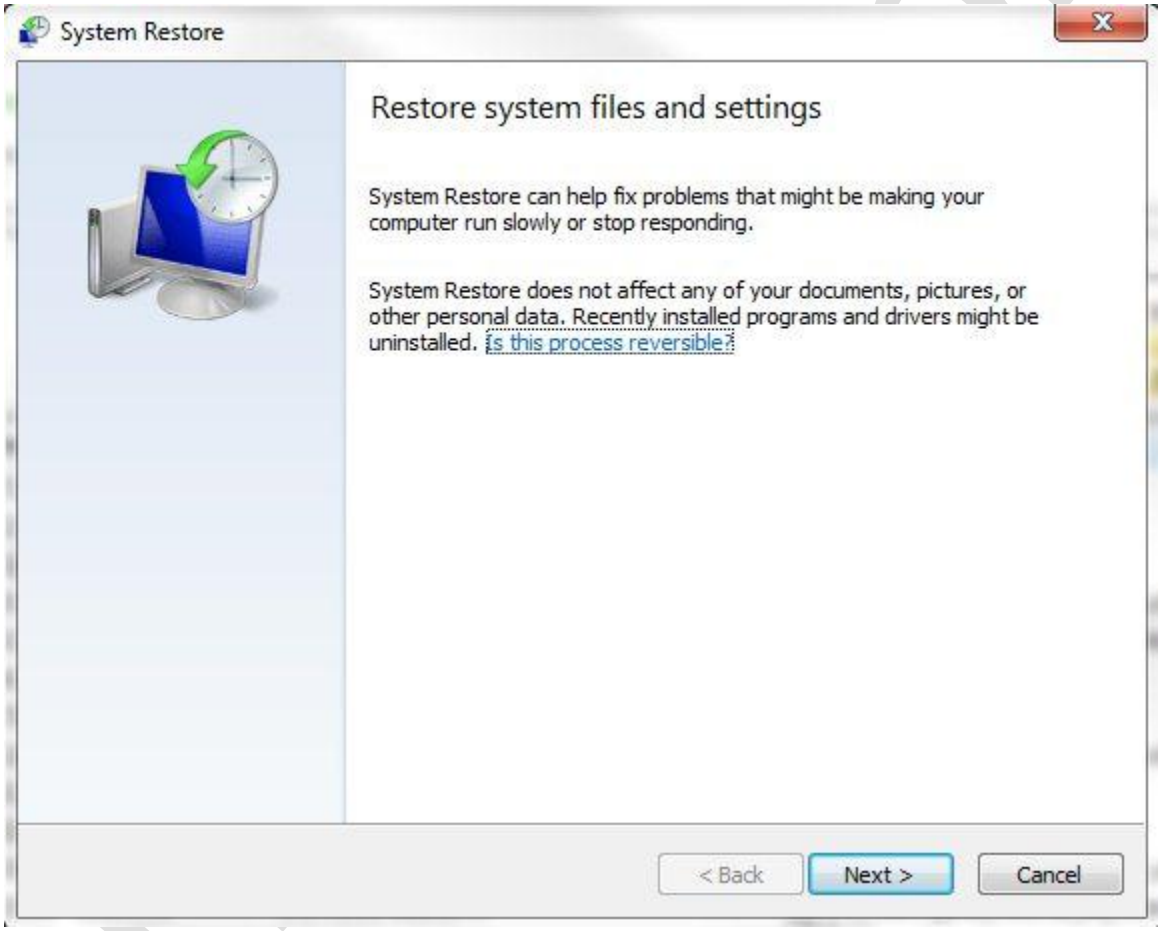


Here, you can click the *System Restore* button to launch the system restore wizard that allows you to reset Windows to a previous restore point. This tab also allows you to configure system restore options by clicking selecting the appropriate drive and clicking the *configure* button.

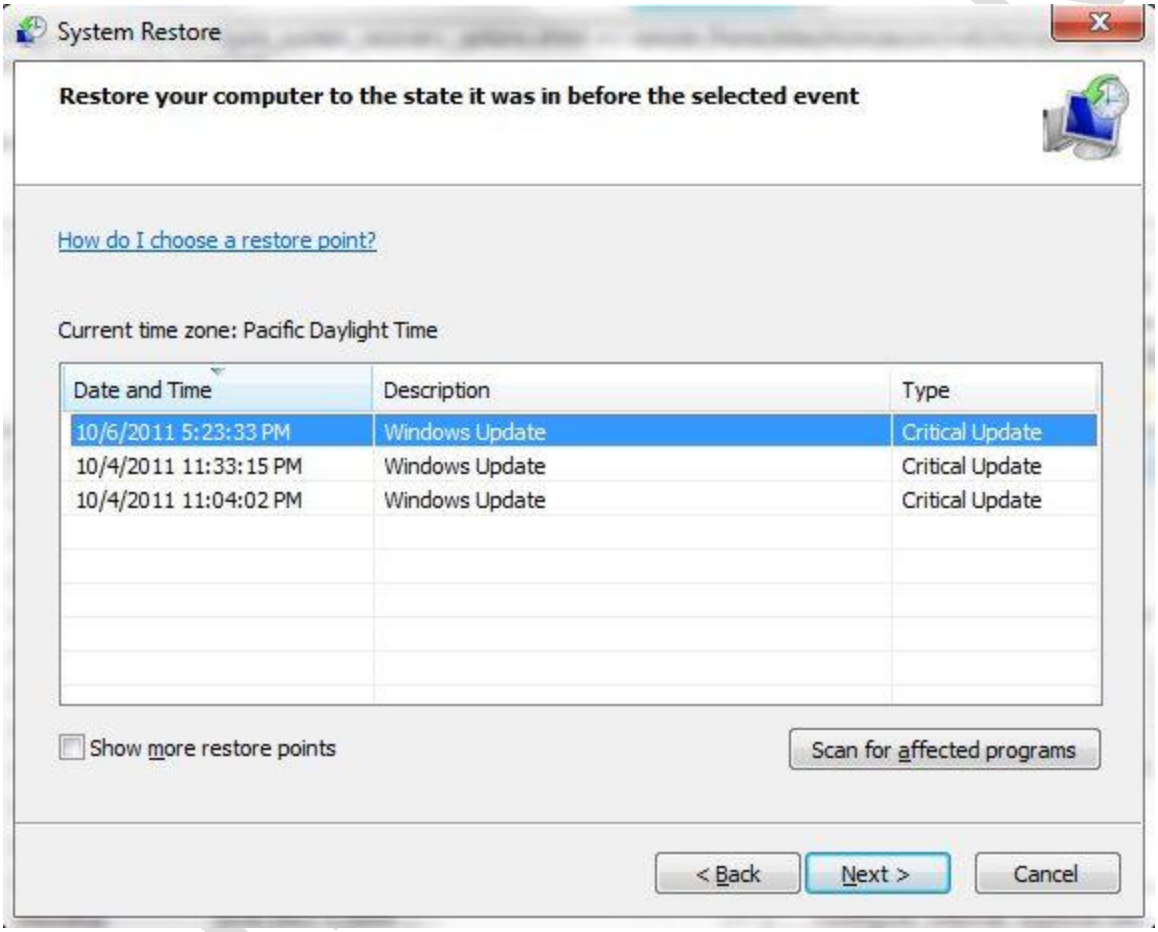


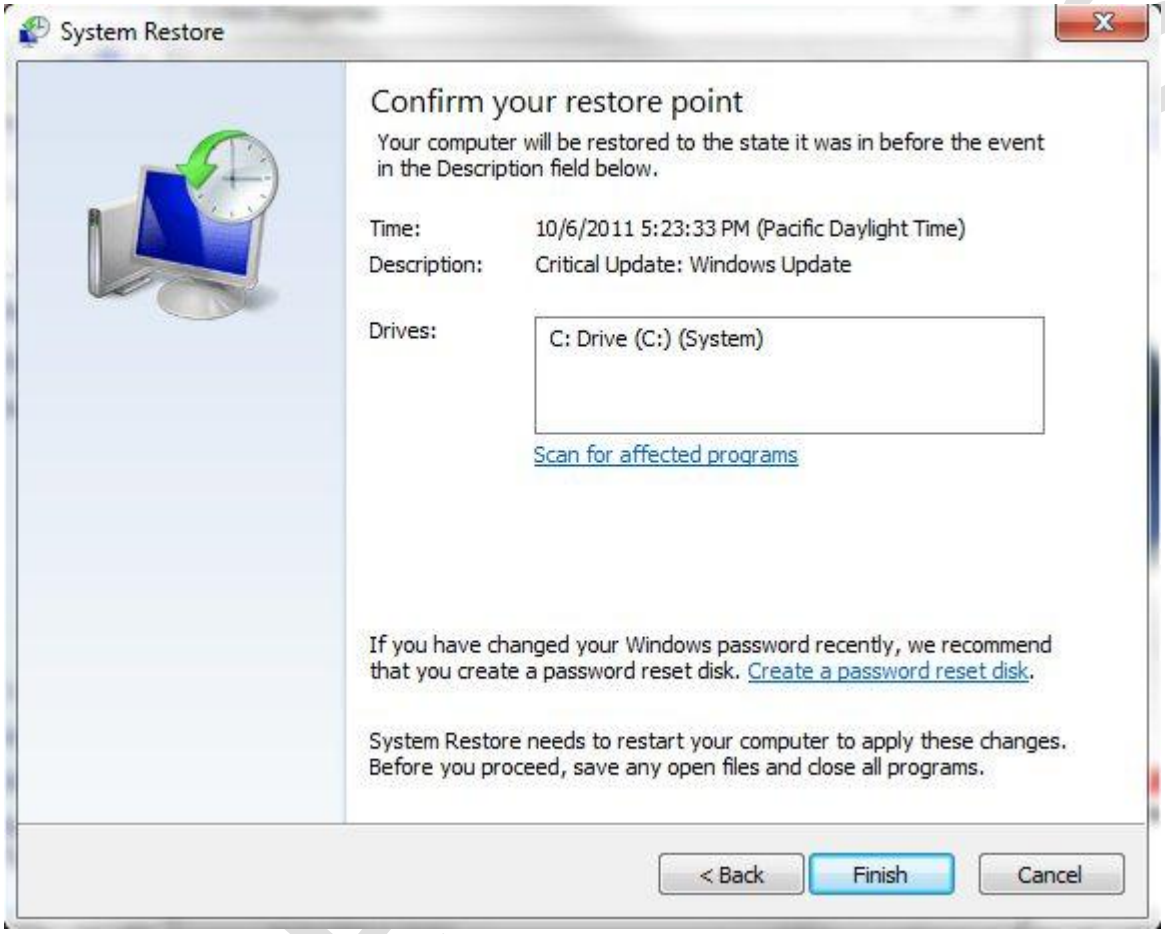
The System Protection tab of the system properties dialog box also allows you to manually create a new restore point. Select the appropriate drive and click the *Create* button. Next, enter a description for the new restore point and click *Create*. A dialog box appears stating that the restore point was created. Click *Close*.

To restore your system from a restore point, you will need to access the System Restore Wizard. You can do this from the System Protection tab discussed above, or by directly by typing *System Restore* into the Windows 7 search box, and selecting *System Restore*. You can also access system restore by clicking the *Recovery* icon in the Control Panel and then clicking the *Open System Restore* button to launch the wizard.



At the screen above, click *Next*, then select the restore point you would like to return Windows to and click *Next*.



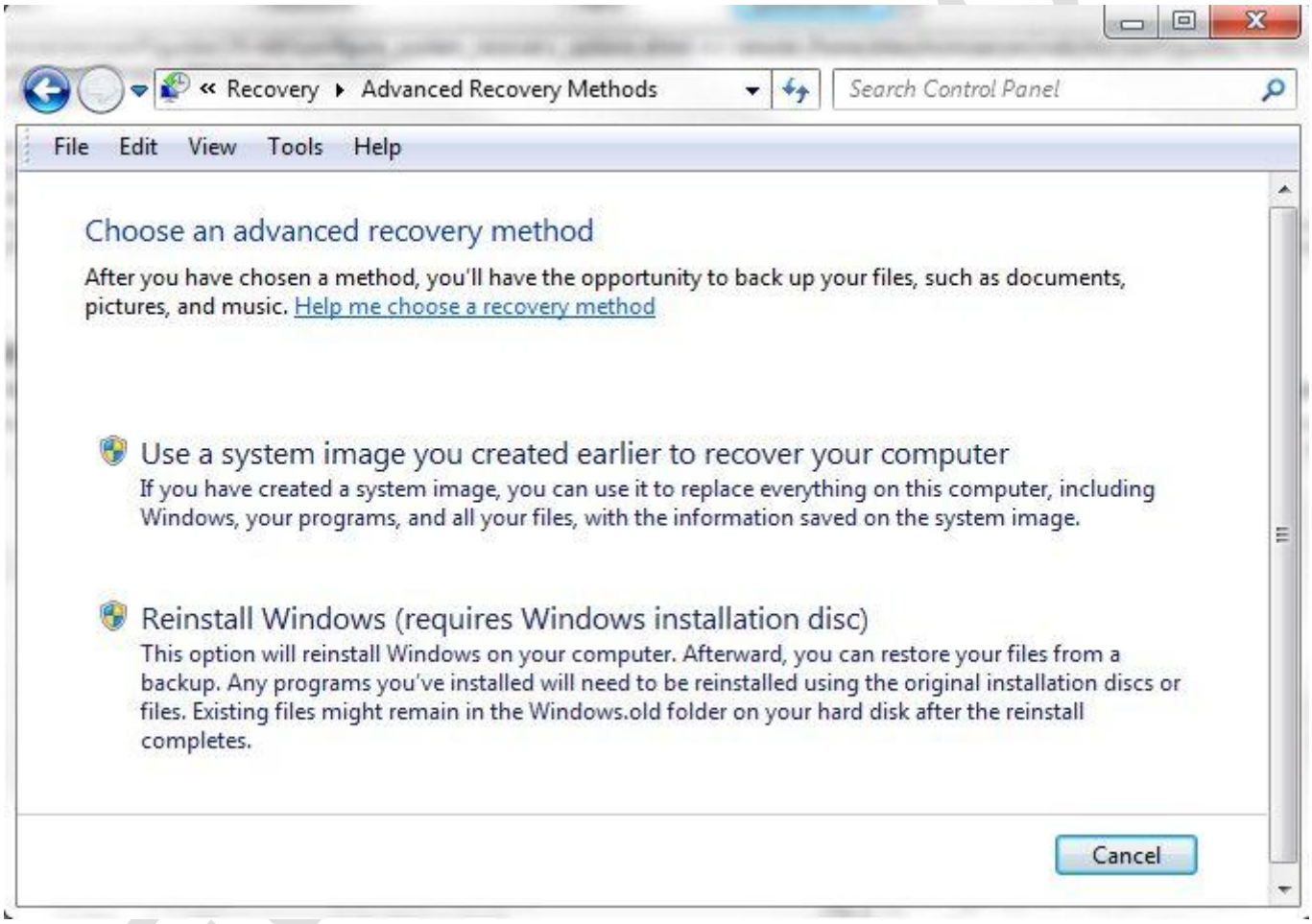


Click *Finish* to complete the restore.

Every time you use System Restore, a restore point is created before proceeding, so you can undo the changes if they don't fix your problem. If you use System Restore when the computer is in safe mode or using the System Recovery Options, you cannot undo the restore operation. However, you can run System Restore again and choose a different restore point, if one exists.

Advanced Recovery Methods:

If a Windows system is badly damage and cannot be fixed by backup or system restore, you may wish to try advanced recovery methods. To access this, go to the *Recovery* control panel. Click on the *Advanced recovery methods* link.



Here you have the option to recover the system using a previously created system image (AKA "Complete PC Restore"), or to reinstall Windows. Both of these options may result in the loss of personal files, so it is important to back these up to another drive first if possible. If you select *Use a system image you created earlier to recover your computer*, you will first be prompted to backup your files. After that, you will be prompted to restart the computer. From here, you will want to follow the instructions for accessing System Recovery Options in the previous section. Once the System Recovery Options are loaded, select *System Image Recovery* and follow the instructions.

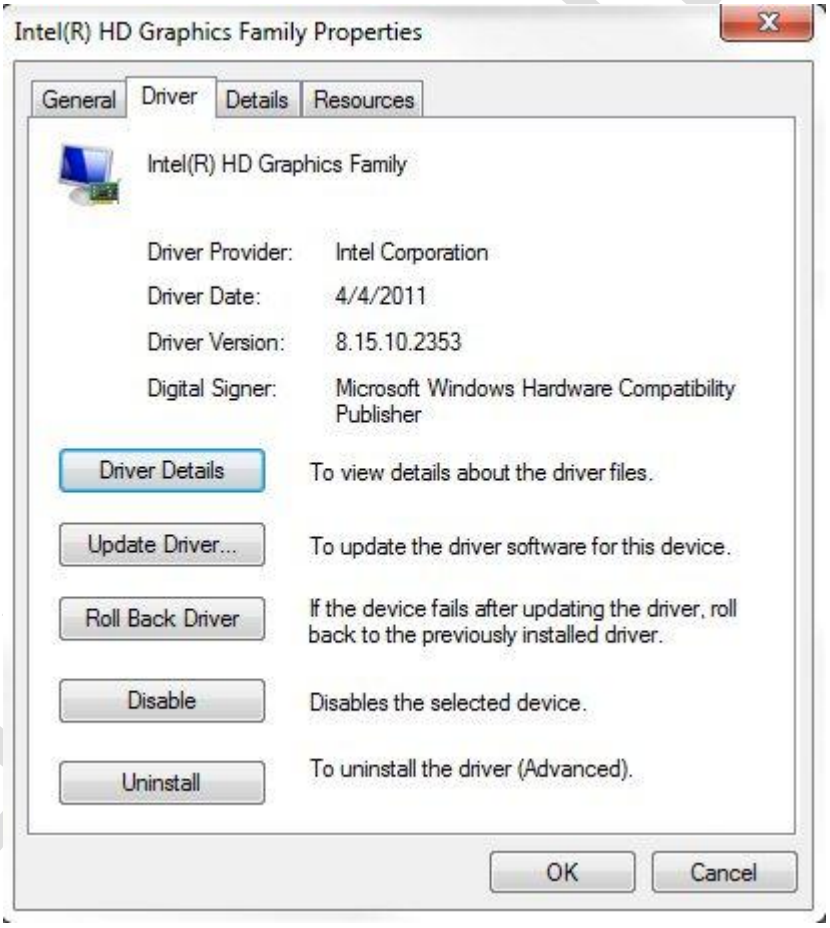
Advanced Boot Options:

In previous sections, we have briefly discussed the Advanced Boot Options menu by pressing F8 during startup. Specifically, we have discussed the "Repair your computer" option, however, there are a number of other features that can be accessed from this menu:

- **Safe mode** - Starts Windows with a minimal set of drivers and services.
- **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
- **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.
- **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.
- **Enable low resolution video (640 × 480)** - 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.
- **Last Known Good Configuration (advanced)** - Starts Windows with the last registry and driver configuration that worked successfully. For example, if a newly installed driver is causing problems, or an incorrect registry setting is preventing Windows from starting correctly, you can restart your computer using Last Known Good Configuration.
- **Debugging mode** - Starts Windows in an advanced troubleshooting mode. Boots Windows while sending debug information through a serial port to another computer. It's useful in the case of a persistent "blue screen" or "stop" error.
- **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.
- **Disable Driver Signature Enforcement** - Allows drivers containing improper signatures to be installed.
- **Start Windows normally** - Starts Windows in its normal mode.

Driver Roll Back:

In most cases, when a newly installed driver causes problems, you would correct the problem using the Last Known Good Configuration boot option, or restoring to the last working system restore point. In some rare cases, such as when a new driver was packaged with essential Windows updates, you may wish to roll back the driver. This would allow you to correct the problem while keeping the other installed updates, for example. To roll back a driver, access the properties for the device, and click on the *Driver* tab. Click on the *Driver Roll Back* button to revert to the previous version. Note that this button will only appear if the driver was updated at some point.

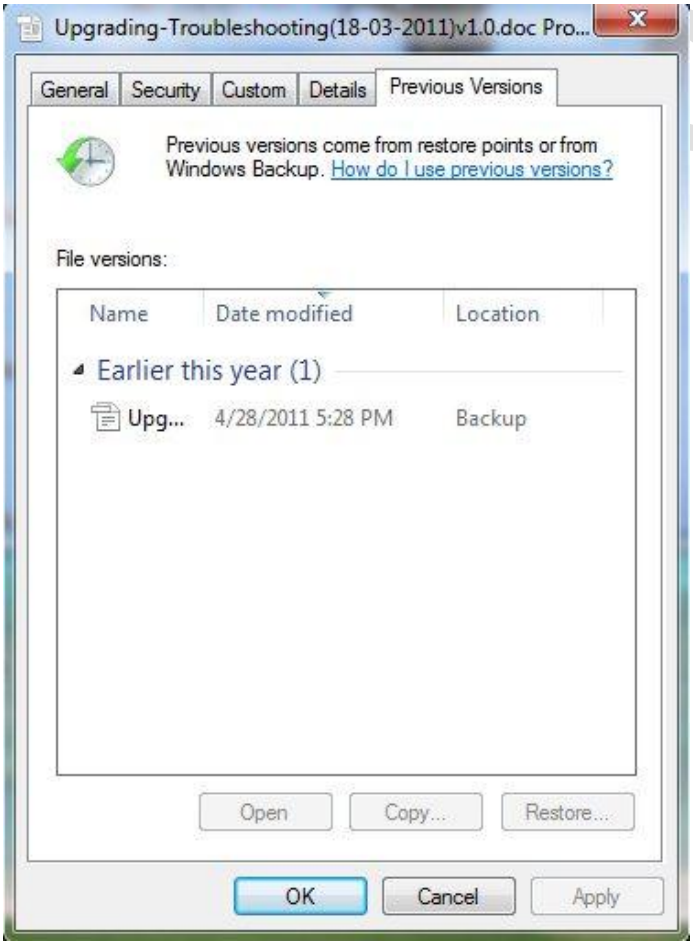


70-680 Study Guide - Configure File Recovery Options

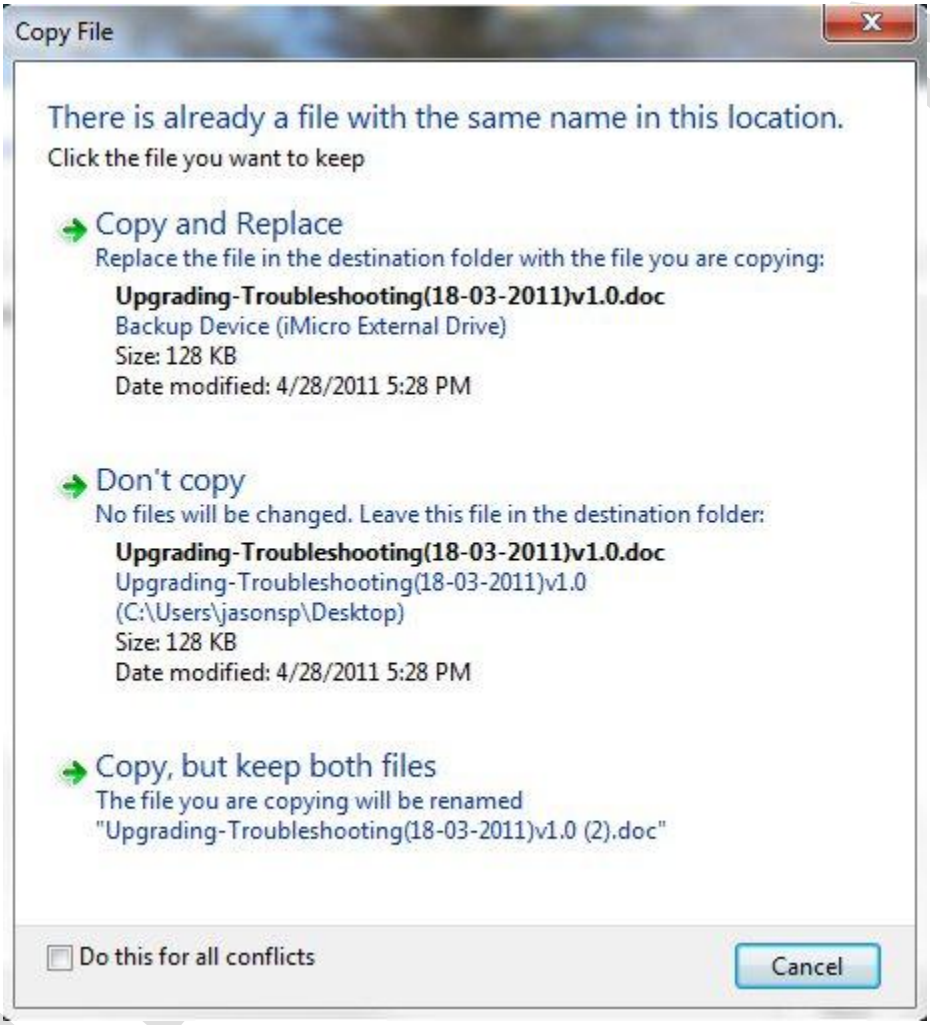
Restoring Previous Versions of Files:

If you have a file or files that are damaged, you can restore them to their previous version if one exists. Previous versions are automatically saved as shadow copies as part of a restore point. If system protection is turned on, Windows automatically creates previous versions of files and folders that have been modified since the last restore point was made. Previous versions are also created by Windows Backup when you back up your files.

To restore a previous version, right click on the file and select *Restore Previous Versions*.



Select the version you wish to restore and click *Restore*.



Next, select whether you wish to replace the existing file, "Don't Copy" which essentially cancels the restore, or keep both files (the original and the restored file).

Restoring Files and Folders From Backup:

If you have lost or destroyed folders or files that you still want on your Windows 7 system, you can restore them from your backup. Follow these steps to restore your files and/or folders:

1. Click *Start*, then click *Control Panel* and then click *Backup And Restore Center*.
2. Click *Restore My Files*.
3. On the Restore Files screen, click the *Browse For Files* or *Browse For Folders* button. You can add files AND folders to a single restore operation.

4. Click *Microsoft Windows Backup* in the left pane.
5. Double-click the backup that you created in the previous exercise. Choose the folders or files that you want to restore and click *Add Files* or *Add Folders*. Click *Next*.
6. Select whether you want files or folders saved in the original location or a different location. To begin the restore, select *Restore*.
7. When restore is complete, click *Finish*.

Note: To restore a user's profile, select *Browse for Folders* in the steps above and select the user's profile folder.