Exam 70-680

Configuring Windows 7

Mega Guide

Prepare With Confidence

This PrepLogic Mega Guide was written by certified subject matter experts and published authors to provide you accurate, in-depth exam coverage. All exam objectives are covered in detail, giving you the knowledge and confidence you need to pass your exam.

PrepLogic

Be Prepared. Be Confident. Get Certified.

PrepLogic, Inc. • 1300 N. Westshore Boulevard, Suite # 125 • Tampa, Florida 33607
Phone: (813) 769-0920 (800) 418-6789 • Fax: (813) 769-0926 • Website: www.preplogic.com

Configuring Windows 7 (70-680) Mega Guide

Product ID: 012356
Production Date: March 17, 2010

Warning and Disclaimer

Every effort has been made to make this document as complete and as accurate as possible, but no warranty or fitness is implied. The publisher and authors assume no responsibility for errors or omissions. The information provided is on an "as is" basis. The authors and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this document.

Volume, Corporate, and Educational Sales

PrepLogic offers favorable discounts on all products when ordered in quantity. For more information, please contact PrepLogic directly:

1-800-418-6789
solutions@preplogic.com

International Contact Information

International: +1 (813) 769-0920

Australia: (02) 8003 3878

South Africa: (0) 11 083 9973

United Kingdom: (0) 20 8816 8036

Abstract

In order to take the 70-680 Exam for Windows 7 you'll need to make sure you have a good, solid understanding of all of the skills measured by having a combination of academic knowledge of the subject matter as well as real world experience.

The exam itself is intended for technicians and desktop administrators that have at least one year of experience working with Microsoft desktop operating systems such as Windows XP and Windows Vista. You will also need to have about one year of experience implementing and administering systems in a networked environment.

This study guide is a last stop before the exam. It should be used as a last minute refresher and should not be considered a complete and full study tool on its own.

What to Know

When you pass Exam 70-680: TS: Windows 7, Configuring you will gain the following certification:

MCTS: Windows 7, Configuration

The 70-680: TS: Windows 7, Configuring certification counts as credit toward the following certification tracks:

- MCITP: Enterprise Administrator
- MCITP: Enterprise Desktop Administrator 7
- MCITP: Enterprise Desktop Support Technician 7

The Domains covered in the 70-680 Exam are:

- Installing, Upgrading, and Migrating to Windows 7
- Deploying Windows 7
- Configuring Hardware and Applications
- Configuring Network Connectivity
- Configuring Access to Resources
- Configuring Mobile Computing
- Monitoring and Maintaining Systems that Run Windows 7
- Configuring Backup and Recovery Options

Tips

I would recommend that you read through at least one full study guide on 70-680. Even if you are experienced on most or all of the domain topics, the exam topics as outlined and as intended for study are often askew of what most professionals come across in the "real world". By taking the time to go through at least one full study guide and then also using test prep practice questions and doing a last minute final review with a wrap up document like the Mega Guide you'll be better prepared for the exam than just going in on knowledge and experience alone.

Domain One: Installing, Upgrading, and Migrating to Windows 7

Identifying hardware requirements

In order to perform an installation successfully you'll need to be able to properly identify the Windows 7 hardware requirements.

The hardware requirements for the Windows 7 basic experience are:

- Current processor running at least 800 MHz
- 512 MB of system memory
- A graphics processor that is DirectX 9 capable

The hardware requirements for the Windows 7 premium experience are:

- 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)
- Support for DirectX 9 graphics with a Windows Display Driver Model (WDDM) driver, 128 MB of graphics memory (minimum), Pixel Shader 2.0, and 32 bits per pixel
- 40 GB of hard drive capacity with 16 GB available hard disk space (32-bit) or 20 GB (64-bit)
- DVD-ROM drive
- Audio output capability
- Internet access capability

In order for hardware and software vendors to get the Windows 7 Software Logo they have to meet the qualifying criteria:

- Comply with Anti-Spyware Coalition Guidelines
- Do not try to circumvent Windows Resource Protection
- Ensure ongoing quality
- Clean, reversible installation
- Install to the correct folders by default
- Sign files and drivers digitally
- Support x64 versions of Windows
- Do not block installation or application launch based on an operating system version check
- Follow UAC guidelines
- Adhere to Restart Manager messages
- Do not load services and drivers in safe mode
- Support multiuser sessions

In order to successfully install a specific version of Windows 7 on a system you need to make sure you understand the differences between the versions and which capabilities each version has.

This will allow you to pick the specific edition of Windows 7 that you need for your installation.

Windows 7 Starter Edition

Windows 7 Starter does not support or include:

- Windows Aero user interface
- DVD playback
- Windows Media Center
- IIS Web Server
- Internet connection sharing
- Domain join
- Encrypting File System (EFS)
- AppLocker
- DirectAccess
- BitLocker
- Remote Desktop Host
- BranchCache

Windows 7 Starter Edition supports a maximum of one physical processor. The following features are available and supported on Windows 7 Starter Edition:

- Jump Lists
- Windows Search
- HomeGroup Join
- Windows Media Player
- Backup and restore
- Enhanced Media Playback
- Action Center
- Device Stage
- Home Media Streaming
- Bluetooth Support
- Fax and Scan
- Credential Manager

Windows 7 Home Basic Edition

Windows 7 Home Basic is available only in emerging markets.

Windows 7 Home Basic also has the same feature limitation set as Windows 7 Starter Edition as shown above with the exception of Internet connection sharing – this is available on Windows 7 Home Basic.

Windows 7 Home Basic Edition supports a maximum of one physical processor.

The x86 version supports 4 GB of RAM in total and the x64 version supports up to 8 GB of RAM.

Windows 7 Home Basic Edition does include the same features as Windows 7 Starter Edition. In addition to those features it also supports:

- Taskbar Thumbnail Preview
- Fast User Switching
- Ad-hoc wireless networks
- Internet connection sharing
- Multi-Monitor Support
- Windows Mobility Center

Windows 7 Home Premium Edition

Windows 7 Home Premium supports a wider array of features than the prior two editions of Windows 7. It supports all of the features that are supported in Windows 7 Home Basic Edition as well as these additional features:

- Aero Glass
- Aero Background
- Windows Touch
- HomeGroup Create
- Windows Media Center
- Remote Media Streaming
- DVD Playback and authoring
- Snipping Tool
- Sticky Notes
- Windows Journal
- Windows Side Show

The x86 version of Windows 7 Home Premium supports up to 4 GB of RAM on the x86 architecture and the x64 version supports up to 16 GB of RAM.

Windows 7 Home Premium Edition supports up to two physical processors.
It does not support:

- Domain join
- Encrypting File System (EFS)
- AppLocker
- DirectAccess
- BitLocker
- Remote Desktop Host
- BranchCache

Windows 7 Professional Edition

Windows 7 Professional Edition supports all the features that are available under Windows Home Premium. In addition to those features Windows 7 Professional Edition also supports:

- Domain join
- Encrypting File System (EFS)
- Location Aware Printing
- Group Policy
- Remote Desktop Host
- Advanced Back-up
- Windows XP Mode
- Windows Mobility Center Presentation Mode
- Offline Folders

It does not support AppLocker, DirectAccess, BitLocker, or BranchCache.

Windows 7 Professional Edition supports up to 4 GB of RAM on the x86 architecture and the x64 version supports up to192 GB of RAM.

Windows 7 Professional Edition can support up to two physical processors.

Windows 7 Enterprise Edition / Windows 7 Ultimate Edition

The final two editions of Windows 7 are exactly identical to one another as far as feature support goes. The only difference in them is the licensing. Windows 7 Enterprise Edition is available only through Microsoft's volume licensing; it is not available through retail channels or installed on systems by Original Equipment Manufacturers (OEM) for sale to the general public.

Windows 7 Ultimate Edition on the other hand is directly available through retail channels or Original Equipment Manufacturers (OEM) for sale to the general public through retail channels.

Both of these versions of Windows 7 support all of the features supported under
Windows 7 Professional Edition.

In addition to those features the following is also supported:

- BitLocker
- BitLocker To Go
- AppLocker
- Direct Access
- Branch Cache
- Multi-User Interface Language Packs
- Enterprise Search Scopes
- VDI Enhancements
- Boot from VHD

Both of these editions support up to 4 GB of RAM on the x86 architecture and the x64 version supports up to 192 GB of RAM.

Enterprise and Ultimate Editions can each support up to two physical processors.

Setting up Windows 7 as the Sole OS: a Clean Installation

You have to consider the installation method you need to use to roll out Windows 7 and that is mainly going to be dependent on what you have access to (e.g. network share, DVD, etc) to what makes sense (e.g. one or two system installs or numerous).

The right installation method for the job at hand is in tune with the old saying "the right tool for the right job."

Using a DVD to install Windows 7 is standard fare - you pop the DVD into the drive in a system with an existing operating system and it will auto run which will allow you to either perform an in place upgrade (under a supported operating system) or a custom installation (clean install).

If you choose to boot from the DVD you just need to make sure the system you are performing the installation on has its BIOS set to boot from the DVD drive ahead of booting from the hard drive.

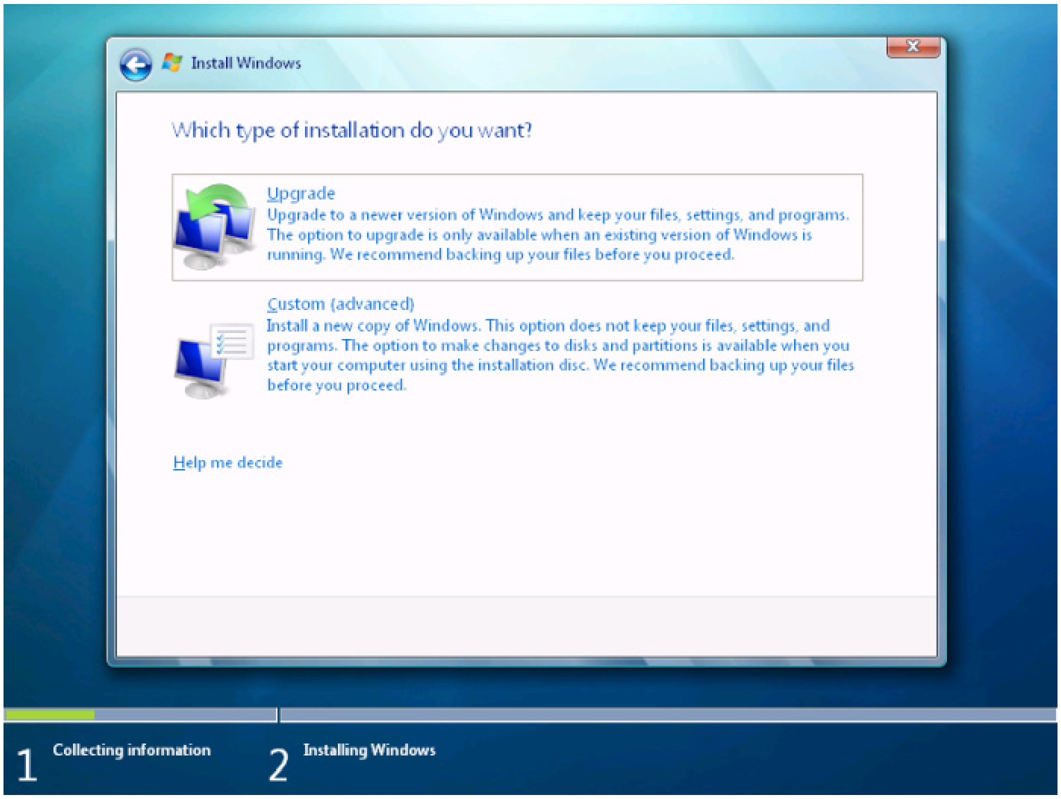
You can also use a USB DVD drive if your system does not currently include one or if you're using a system like a netbook portable system that does not come with an internal DVD drive. Additionally you can use a USB flash drive as an installation source as well as long as the drive is 4GB in size or larger and is formatted with the FAT32 file system.

The other ways that you can deploy Windows 7 is by using a network share as an installation source or Windows Deployment Services.

Setting up Windows 7 as the sole operating system would be done where you are either replacing the currently installed operating system, (and not configuring it in a dual boot scenario) or where you are installing it in place of an existing one. By performing a clean installation it into another directory you'll be preserving data already on the hard drive but not applications and settings by default. If settings need to be saved, you should use the User State Migration Tool (USMT) and then import settings after re-installing the application. If you wanted to start clean you could reformat the hard drive and start from scratch.

Once you decide to run the executable for a clean installation most of the steps are the same.

1. To get started, boot from the DVD.
2. Once the pre-execution environment is set up, the first screen you arrive at requires that you choose a language to install, the time and currency format, and what keyboard or input method you are using for the installation.
3. Once you choose your options, you will arrive at the Install Windows 7 page and you would continue forward by selecting Install Now.
4. The next step is to review and accept the Windows 7 license terms and from there you would choose which type of installation you want to perform: Upgrade or Custom (Advanced).
5. Since we are discussing performing a clean installation, select Custom to continue. (If you are performing the install on a completely bare system the Upgrade option should be unavailable).



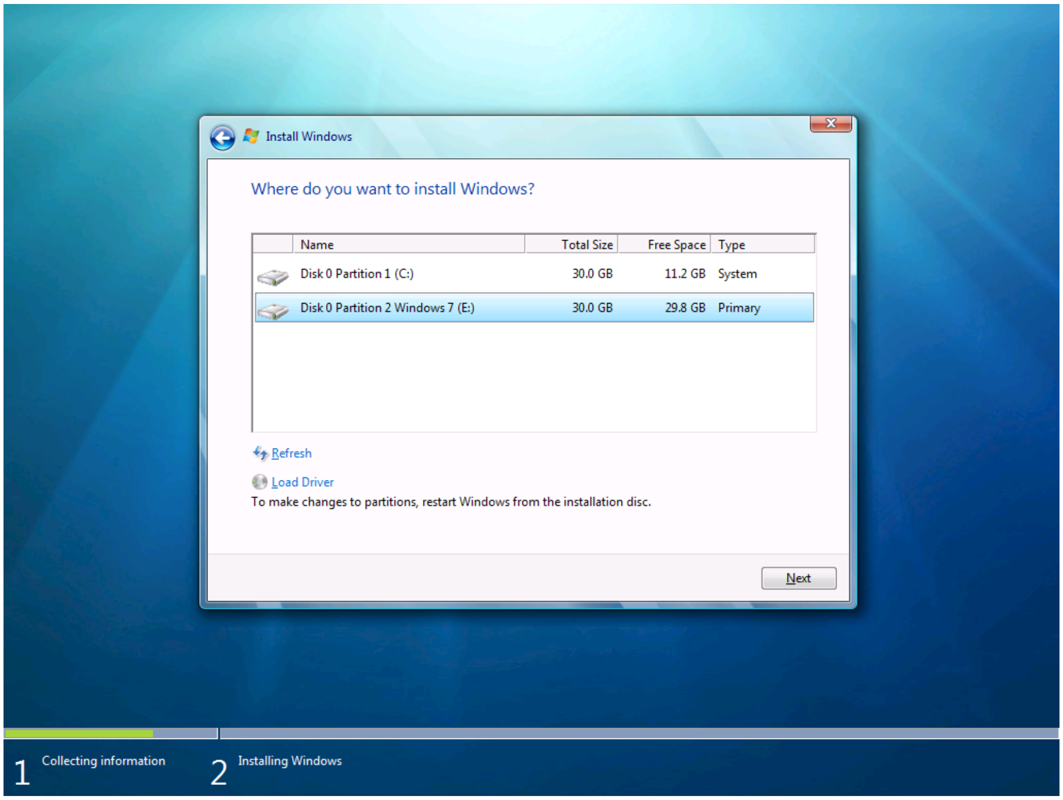
Which type of installation do you want?

Upgrade
Upgrade to a newer version of Windows and keep your files, settings, and programs. The option to upgrade is only available when an existing version of Windows is running. We recommend backing up your files before you proceed.

Custom (advanced)
Install a new copy of Windows. This option does not keep your files, settings, and programs. The option to make changes to disks and partitions is available when you start your computer using the installation disc. We recommend backing up your files before you proceed.

Figure 1: Choosing an Install Option

6. From here you'll be asked where to install Windows 7.



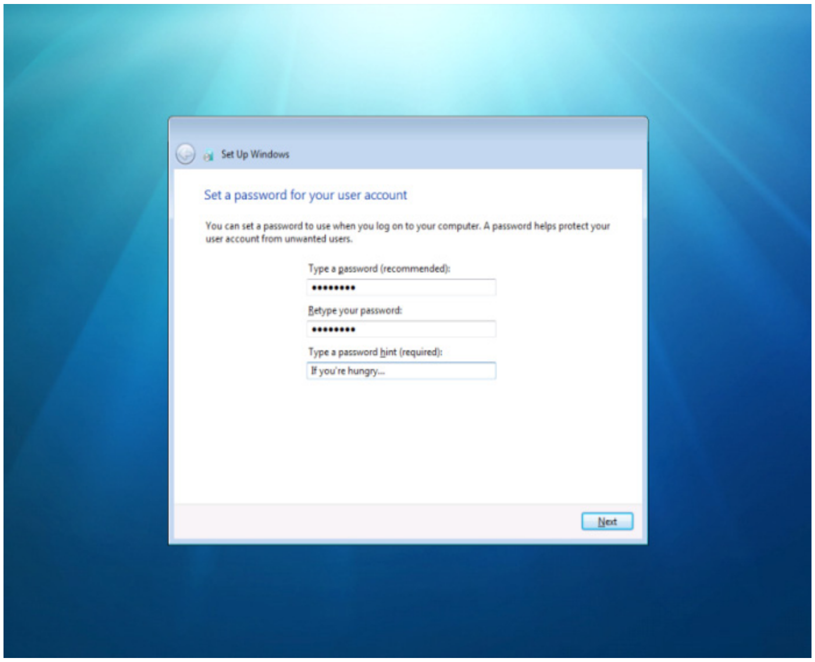
Where do you want to install Windows?

Name	Total Size	Free Space	Type
Disk 0 Partition 1 (C:)	30.0 GB	11.2 GB	System
Disk 0 Partition 2 Windows 7 (E:)	30.0 GB	29.8 GB	Primary

To make changes to partitions, restart Windows from the installation disc.

Figure 2: Choosing an Install Partition

7. You will be able to choose from any available disks and/or partitions that meet the minimum system requirements for install.
8. Once you make your choice, the Windows 7 installation process begins.
9. When the first part completes, the computer will reboot itself.
10. Upon restarting, you may see the option to press any key to boot from CD or DVD; you'll need to allow this choice to time out to continue with the installation you've already started. If you hit a key it will cause the system to boot from the DVD and restart the install process all over again. If you do this, you can simply restart the system and allow it to continue past this point.
11. Once setup comes back online, it will finish expanding all of the files (and reboot again) before it formally restarts in Windows 7.
12. At this point, you'll need to choose a username that will be the logon for the machine and a computer name for the system. You'll also be prompted to set a password for this account (which is the default Administrator account for the machine) as well as a password reminder.



Set Up Windows

Set a password for your user account

You can set a password to use when you log on to your computer. A password helps protect your user account from unwanted users.

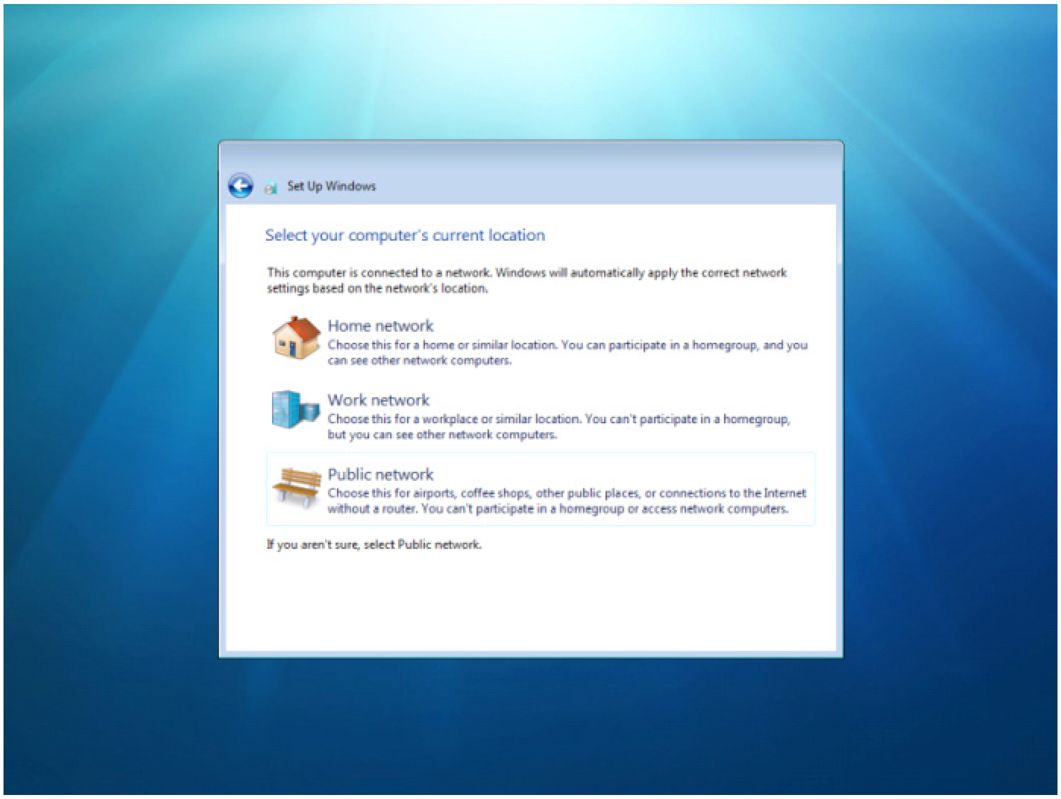
Type a password (recommended): ••••••••

Retype your password: ••••••••

Type a password hint (required): If you're hungry...

Figure 3: Creating the Administrator Account

13. Next, provide your product key. You can choose to continue without a key and will be able to run your installation of Windows 7 for up to 30 days before you'll be forced to supply it and activate your copy of Windows.
14. Most of the time, when doing these types of installs, you would simply enter your license key and leave the "Automatically activate Windows when I'm online" option checked and click next to continue.
15. Next, you'll be presented with the Help Protect Your Computer And Improve Windows Automatically page, which allows you to make initial configuration settings to Windows Update where you could choose to **Use recommended settings**, **Install important updates only** or **Ask me later**.
16. Once you make a choice, the next screen you'll arrive at is the **Review your time and date settings** page which allows you to change the time zone settings. You are also able to change the time and date as well (in case the information pulled from the system has not populated correctly).
17. On the next screen, you are presented with the **Select your computer's current location** page if a working network is detected. This is where you choose to identify the network settings as **Home**, **Work**, or **Public,** which will automatically configure network resource settings, firewall settings, network discovery and other parameters based on the profile you choose.



Select your computer's current location

This computer is connected to a network. Windows will automatically apply the correct network settings based on the network's location.

Home network
Choose this for a home or similar location. You can participate in a homegroup, and you can see other network computers.

Work network
Choose this for a workplace or similar location. You can't participate in a homegroup, but you can see other network computers.

Public network
Choose this for airports, coffee shops, other public places, or connections to the Internet without a router. You can't participate in a homegroup or access network computers.

If you aren't sure, select Public network.

Figure 4: Choosing a Network Location

18. Once you've made your choices, the final part of the installation routine completes and you are logged into the local system using the default Administrator account.

Setting up Windows 7 in a Dual or Multiboot Configuration

Some key points to consider before you take on the task of installing Windows 7 to dual boot with your existing operating system such as Windows XP and / or Windows Vista:

- Make sure to back up all of your important data
- Use System Restore and manually create a restore point
- Make sure you have a hard disk in the system that has a separate partition for each operating system that you want to install
- If the single disk does not have multiple partitions already configured you may need to reformat and / or repartition your hard disk or install an additional hard drive
- The partitions should be formatted with the NTFS file system
- To avoid major configuration problems, especially between older boot managers and newer boot managers, you should always install operating systems from oldest release to newest

You will not need a separate partition for each operating system in certain dual-boot scenarios such as when you dual-boot from a VHD file in a supported configuration.

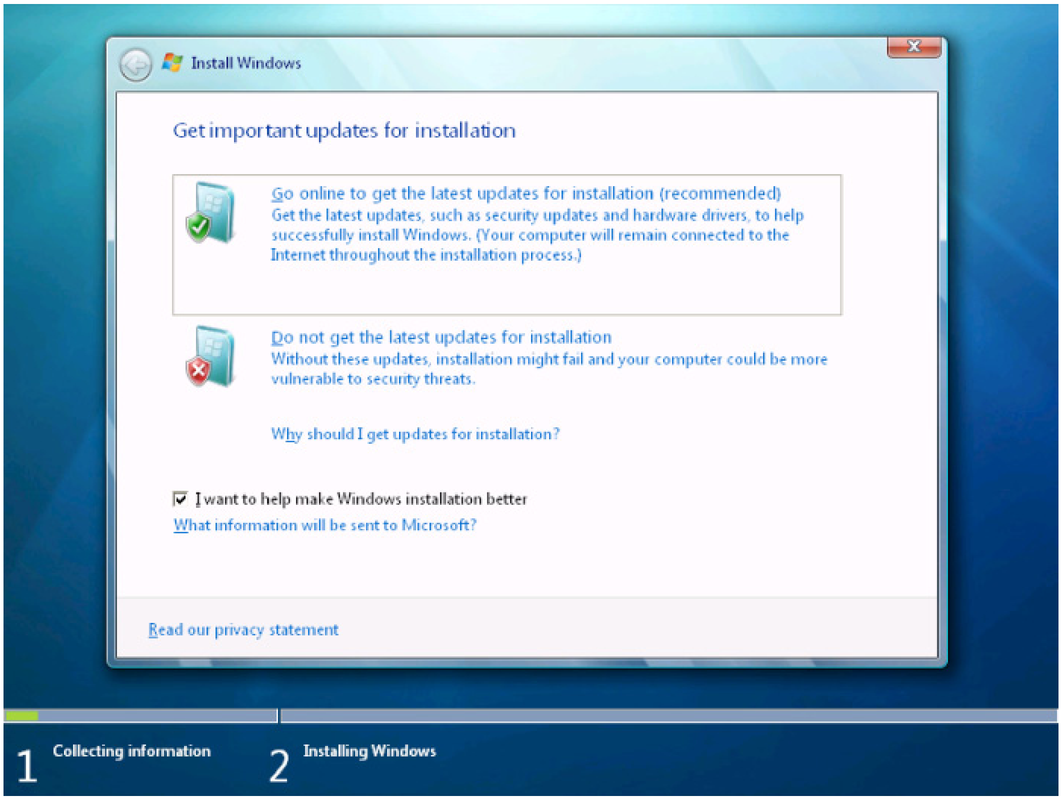
You can install and then boot Windows 7 Enterprise and Ultimate editions from VHD files.

Booting from VHD is only supported on Windows 7 or Windows Server 2008 R2 boot environments; you cannot dual-boot Windows XP or Windows Vista computers with Windows 7 installed on a VHD file because the Windows 7 boot environment, which is a requirement for booting to VHD, is not present on the legacy XP/Vista systems.

Generally when you are doing a dual boot installation you will be launching the installation routine from within the existing operating system and installing Windows 7 in another partition using the **Custom (advanced)** option.

Once the Windows 7 media is in the DVD drive auto-run should execute on its own. If it doesn't because you've change the default settings behavior you can launch the installation routine manually.

Setup will begin and after some initial setup present you with the **Get important updates for installation** options.



Get important updates for installation

Go online to get the latest updates for installation (recommended)
Get the latest updates, such as security updates and hardware drivers, to help successfully install Windows. (Your computer will remain connected to the Internet throughout the installation process.)

Do not get the latest updates for installation
Without these updates, installation might fail and your computer could be more vulnerable to security threats.

Why should I get updates for installation?

☑ I want to help make Windows installation better
What information will be sent to Microsoft?

Read our privacy statement

Figure 5: Choosing to Get Important Updates

Generally, it is recommended to go ahead and get the latest updates for installation (as recommended by the setup wizard) if you are connected to the internet at the time of the setup. Setup will search online for installation updates and will reboot the system when this part of the installation is complete.

Once the system reboots you'll reach the **Please read the license terms** screen; you'll need to accept the license terms to proceed to the next phase.

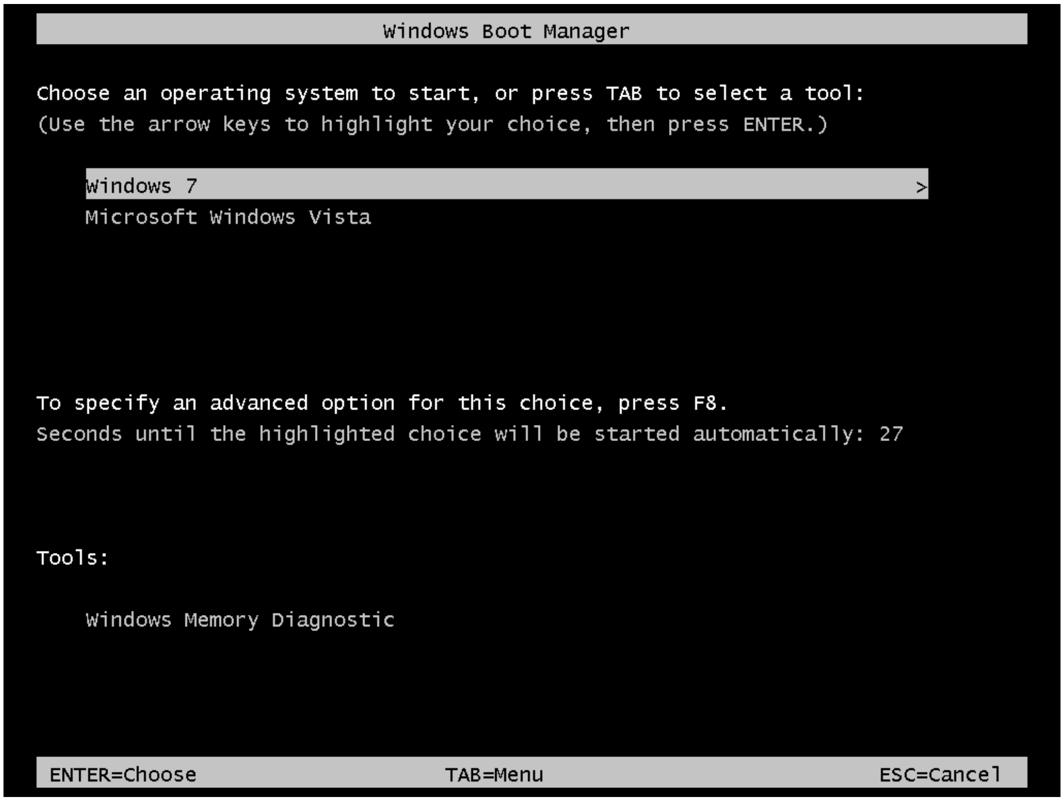
When you reach the **Which type of installation do you want** screen, choose between the **Upgrade** and the **Custom (advanced)** options. In order to continue with the dual-boot setup you would select **Custom (advanced)**.

When the routine continues from here you'll be presented the **Where do you want to install Windows** options, which will show you the available partitions where Windows can be installed.

Once you choose an available partition, or create a new one from available free space, the setup routine will copy the Windows files and begin expanding them. At some point in the "expanding files" sequence, the routine will stop and the system will reboot before continuing.

Once setup comes back online, it will finish expanding all of the files needed before it formally restarts one final time for the final, post-setup configuration of the operating system.

What you should also notice during this startup sequence is that you are now presented with the Windows Boot Manager at start up which allows you the option to choose which operating system you want to boot the system into.



```
                           Windows Boot Manager

Choose an operating system to start, or press TAB to select a tool:
(Use the arrow keys to highlight your choice, then press ENTER.)

    Windows 7                                                       >
    Microsoft Windows Vista




To specify an advanced option for this choice, press F8.
Seconds until the highlighted choice will be started automatically: 27



Tools:

    Windows Memory Diagnostic




 ENTER=Choose                   TAB=Menu                          ESC=Cancel
```

Figure 6: A Dual-Boot Scenario

When you install Windows 7 in multi-boot fashion, it becomes the default operating system in the Windows Boot Manager. Setup designates one operating system (the last to be installed) as the default to start after a 30 second delay. This 30 second delay is a configurable setting that you can make adjustments to, if you wish.

You can make a selection at anytime but if you allow the timer to run out, the default highlighted option will be started automatically.

Once Windows 7 is up and running, you can begin the final stage of setting up the system and complete all of the post installation details, which follow essentially the same course as a normal install.

Using Different Installation Methods

In order to install Windows 7 using a USB drive, you will need to make sure that you have a USB Flash drive that is formatted with the FAT32 file system and contains the installation files for Windows 7.

You'll need to set the USB drive up for this and you do this using the following steps:

1. Connect your USB flash drive to USB port on a system where you can run command line utilities.
2. Open Command Prompt with admin rights by typing "CMD" in the Start menu search box and hitting Ctrl+ Shift+ Enter or by right clicking on the Command Prompt short cut and selecting "Run as administrator".
3. Once the Administrator: Command Prompt window is open type "DISKPART".
4. At the DISKPART> prompt, type "list disk" to make sure you have the USB storage device listed and available.
5. At the DISKPART> prompt, type "select disk" <DRIVE LETTER> where <DRIVE LETTER> is the USB storage device.
6. At the DISKPART> prompt, type "clean" which will clear the existing configuration information and the data off the drive.
7. When the disk is clean, type "create partition primary". The CREATE option will create a volume, partition or virtual disk.
8. Next you will type "format fs=fat32 quick" to create the file system on the USB drive.
9. Once FORMAT is finished you can type "active" which marks the partition active.
10. Type "exit" to leave the DISKPART utility.
11. Copy all the files located on the Windows 7 installation DVD to the USB storage device.
12. Configure the BIOS on the install system to boot from the USB storage device.
13. Attach the USB storage device and then reboot the computer to start installation.

Additional command line options for DISKPART:

Command	**Usage**
ACTIVE	Mark the selected partition as active.
ADD	Add a mirror to a simple volume.
ASSIGN	Assign a drive letter or mount point to the selected volume.
ATTRIBUTES	Manipulate volume or disk attributes.
ATTACH	Attaches a virtual disk file.
AUTOMOUNT	Enable and disable automatic mounting of basic volumes.
BREAK	Break a mirror set.
CLEAN	Clear the configuration information or all information off the disk.
COMPACT	Attempts to reduce the physical size of the file.
CONVERT	Convert between different disk formats.
CREATE	Create a volume partition or virtual disk.
DELETE	Delete an object.
DETAIL	Provide details about an object.
DETACH	Detaches a virtual disk file.
EXIT	Exit DiskPart.
EXTEND	Extend a volume.
EXPAND	Expands the maximum size available on a virtual disk.
FILESYSTEMS	Display current and supported file systems on the volume.
FORMAT	Format the volume or partition.
GPT	Assign attributes to the selected GPT partition.
HELP	Display a list of commands.
IMPORT	Import a disk group.
INACTIVE	Mark the selected partition as inactive.
LIST	Display a list of objects.
MERGE	Merges a child disk with its parents.
ONLINE	Online an object that is currently marked as offline.
OFFLINE	Offline an object that is currently marked as online.
RECOVER	Refreshes the state of all disks in the selected pack. Attempts recovery on disks in the invalid pack and resynchronizes mirrored volumes and RAID5 volumes that have stale plex or parity data.
REM	Does nothing. This is used to comment scripts.
REMOVE	Remove a drive letter or mount point assignment.
REPAIR	Repair a RAID-5 volume with a failed member.
RESCAN	Rescan the computer looking for disks and volumes.
RETAIN	Place a retained partition under a simple volume.
SAN	Display or set the SAN policy for the currently booted OS.
SELECT	Shift the focus to an object.
SETID	Change the partition type.
SHRINK	Reduce the size of the selected volume.
UNIQUEID	Displays or sets the GUID partition table (GPT) identifier or master boot record (MBR) signature of a disk.

Figure 7: DISKPART Command Options

You can also host a network share with the Windows 7 installation files by copying the contents of your Windows 7 DVD and making it accessible for deployments.

You will need to boot client systems into the Windows Preinstallation Environment (WinPE) which is basically a stripped down version of Windows that allows you to access diagnostic and maintenance tools as well as access network drivers. (You can use other network boot loaders as well).

Once the Windows PE environment is booted, you would connect to the network share and begin the installation by running Setup.exe.

There is some additional information on this later in the MegaGuide.

Another installation method for Windows 7 is by using Windows Deployment Services as an installation source for those systems that have a PXE-compliant network card or that are booted from a WDS discover image.

Windows Deployment Services (WDS) enables network deployments of WIM images or virtual hard disks as files used for OS deployments in Active Directory Domain Services (AD DS) networks. This installation method is different than copying the actual installation files from a DVD and placing them on a share for an across the network installation.

WDS in Windows Server 2008 uses multicast for system deployment and Windows Server 2008 R2 now supports the use of multiple stream transfer so that the fastest clients can receive the installation images quicker.

There is some additional information on Windows Deployment Services later in the MegaGuide.

Upgrade to Windows 7

In most cases as a desktop technician, you're going to be working in larger environments, where clean installs and image loads are going to be preferred over in place upgrades of systems. That being said you still may find the occasion where upgrades are necessary.

You first need to understand which prior versions of Windows can be upgraded to Windows 7 and which cannot. You also need to understand other scenarios that might limit or otherwise prevent an in place upgrade to Windows 7.

Microsoft has outlined the **Windows 7 Upgrade Paths** on its website and these are the operating systems that they have listed as not having a supported way of doing an in place upgrade directly to Windows 7:

- Windows 95
- Windows 98
- Windows Millennium Edition
- Windows XP
- Windows Vista RTM
- Windows Vista Starter
- Windows 7 M3
- Windows 7 Beta
- Windows 7 RC
- Windows 7 IDS
- Windows NT Server 4.0
- Windows 2000 Server
- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2

You might notice that Windows NT4 Workstation is not included in the list despite the fact that, for some reason, they included Windows NT Server 4.0. You cannot take a server operating system and perform an in place upgrade, regardless, but for the sake of inclusion, Windows NT4 Workstation should have been listed.

Windows 2000 Professional is also missing from the list as well despite Windows 2000 Server showing up. It is safe to assume that neither of those desktop operating systems can be directly upgraded to any version of Windows 7.

Additional details of other unsupported in place upgrade scenarios:

- Cross-architecture upgrades, such as taking an x86 build and upgrading it to x64 are **NOT** supported.
- Cross-language in-place upgrades (i.e. en-us to de-de) are **NOT** supported.
- Cross-SKU upgrades (i.e. Windows 7 N to Windows 7 K) are **NOT** supported.
- Cross-build type in-place upgrades (i.e. fre to chk) are **NOT** supported.
- Pre-release in-place upgrades across milestones (i.e. Windows 7 RC to Windows 7 RTM) are **NOT** supported.
- Upgrades from Windows Vista to Windows N, Windows K, Windows KN, or Windows E are **NOT** supported.

There are supported in place upgrade scenarios and they are listed there as follows:

From Windows Vista Service Pack 1 or Service Pack 2 you can upgrade the following versions of Windows Vista in place to the corresponding versions of Windows 7:

- Windows Vista Home Basic can be upgraded to:
    - Windows 7 Home Basic Edition
    - Windows 7 Home Premium Edition
    - Windows 7 Ultimate Edition
- Windows Vista Home Premium can be upgraded to:
    - Windows 7 Home Premium Edition
    - Windows 7 Ultimate Edition
- Windows Vista Business can be upgraded to:
    - Windows 7 Professional Edition
    - Windows 7 Enterprise Edition
    - Windows 7 Ultimate Edition
- Windows Vista Enterprise can be upgraded to:
    - Windows 7 Enterprise Edition
- Windows Vista Ultimate can be upgraded to:
    - Windows 7 Ultimate Edition

In a situation where a "lower" SKU version of Windows 7 is already installed and you want to do an in place upgrade to a "higher" SKU, you can do so in a supported fashion by performing an in place upgrade in the following situations:

- Windows 7 Starter (x86) can be upgraded to:
    - Windows 7 Home Premium Edition
    - Windows 7 Professional Edition
    - Windows 7 Ultimate Edition
- Windows 7 Home Basic can be upgraded to:
    - Windows 7 Home Premium
    - Windows 7 Professional
    - Windows 7 Ultimate Edition

- Windows 7 Home Premium can be upgraded to:
    - Windows 7 Professional
    - Windows 7 Ultimate Edition
- Windows 7 Professional can be upgraded to:
    - Windows 7 Ultimate Edition

In order to perform an in place upgrade from Windows Vista to Windows 7 you must have at least Service Pack 1 installed on the Vista systems. You do not have to be at SP2.

Note: if you are running Vista RTM/SP0, you cannot directly upgrade the system to Vista Service Pack 2; Service Pack 1 needs to be installed first.

Windows XP operating systems and earlier cannot be upgraded directly. Migration installations can be performed on XP systems and Custom installations are your only options for most others.

Upgrades can also be performed by using the Windows Anytime Upgrade (WAU) feature.

Windows Anytime Upgrade feature is a method offered by Microsoft for users who want to upgrade their edition of Windows 7 by buying a license online or from a local retail store and buying a Windows Anytime Upgrade key. (It was available for Windows Vista as well). Users would then download and run the Windows 7 Upgrade Advisor in order to determine which features and editions of Windows 7 are supported on their system.

Windows Anytime Upgrade can be used to upgrade from a 32-bit version of Windows 7 to a 32-bit version of Windows 7 or from a 64-bit version of Windows 7 to a 64-bit version of Windows 7. Cross-architecture upgrades, such as taking an x86 build and upgrading it to x64 are NOT supported.

Windows Anytime Upgrade isn't available in all editions of Windows 7 and it is only available for online purchase in a few countries.

If you're running Windows 7 Starter Edition you can use Windows Anytime Upgrade to upgrade to:

- Windows 7 Home Premium Edition
- Windows 7 Professional Edition
- Windows 7 Ultimate Edition

If you're running Windows 7 Home Premium Edition you can use Windows Anytime Upgrade to upgrade to:

- Windows 7 Professional Edition
- Windows 7 Ultimate Edition

If you're running Windows 7 Professional Edition you can use Windows Anytime Upgrade to upgrade to Windows 7 Ultimate Edition.

During the in place upgrade process, if there is a failure or some other issue where the routine cannot complete the system will automatically roll back the attempted update and return the system to the prior operating system.

Performing an In-Place Upgrade

Performing an in place upgrade of a Windows Vista system to Windows 7 begins only slightly differently from a clean install.

1. Insert the Windows 7 DVD to start the installation. Depending on how the auto run parameters are set up on your system you may see the AutoPlay dialog box come up or the installation routine may just begin.
2. Additionally, depending on how your **User Account Control (UAC)** settings are configured for the system, you may be presented with a prompt to allow setup.exe to run.
3. In that situation you would select the **ALLOW** action which would kick off the installation routine.

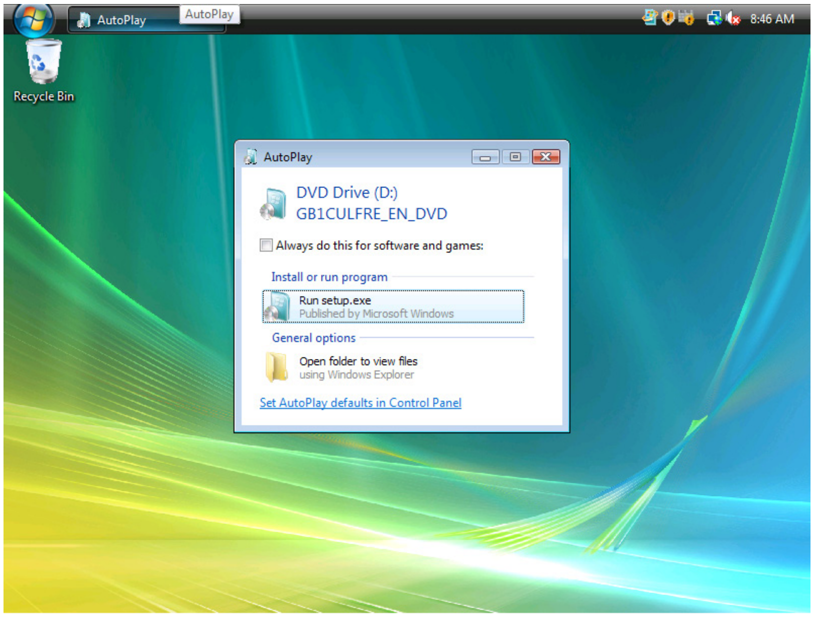


Figure 8: Starting an In-Place Upgrade

4. From there you'd get the **Install Windows** splash screen, where you'd choose **Install now** to continue.
5. Once the file copy is completed, you'll be prompted as to whether or not you'd like to go online to get any needed updates that would be required for the installation.
6. From this point forward the installation routine is pretty much the same as a Custom install.

The same is true for Windows 7 in place upgrades.

In a scenario where you might be running Windows 7 Home Premium and you wanted to go to Windows 7 Ultimate, the steps above are the same and the ending outcome is as well - the installation routine is pretty much the same as Custom (advanced) install once you get beyond the start up and the initial file copy.

Migrating from Windows XP and Migrating User Profiles

When you are updating an XP system to Windows 7 you are effectively performing a Custom installation on the system as an in place upgrade cannot be performed. The new term for these installations, where you are moving user configuration and software settings to a new OS, is called "migrating" the system.

There are two basic migration scenarios: **side-by-side migration and wipe-and-load migration.**

The **User State Migration Tool (USMT)** is used to accomplish either task. The most recent release of the tool, version 4, allows you to migrate user accounts, operating system settings and application settings.

The USMT tool can also be used to migrate access control lists (ACLs) for files and folders that were locally managed on the old system. This allows you to migrate these permissions to the destination computer. Shared folder permissions are not migrated.

Additionally you cannot use the USMT to migrate mapped network drives, local printers, device drivers, passwords, Internet connection sharing settings, hardware-related settings, passwords, application binary files, synchronization files, DLL files, or other executable files.

There are four different .xml migration files used with the USMT:

- **MigApp.xml** - contains rules about migrating application settings like favorites, dial up connection settings, fonts, accessibility settings and so forth.
- **MigUser.xml** - contains rules about user profiles and user data.
    - Folders from each user profile will include My Documents, My Video, My Music, My Pictures, desktop files, Start menu, Quick Launch settings, and Favorites.
    - Folders from the All Users and Public profiles will include Shared Documents, Shared Video, Shared Music, Shared desktop files, Shared Pictures, Shared Start menu, and Shared Favorites.
    - File types migrated by default will include .accdb, .ch3, .csv, .dif, .doc*, .dot*, .dqy, .iqy, .mcw, .mdb*, .mpp, .one*, .oqy, .or6, .pot*, .ppa, .pps*, .ppt*, .pre, .pst, .pub, .qdf, .qel, .qph, .qsd, .rqy, .rtf, .scd, .sh3, .slk, .txt, .vl*, .vsd, .wk*, .wpd, .wps, .wq1, .wri, .xl*, .xla, .xlb, .xls*. (The asterisk (*) stands for zero or more characters.)
- **MigDocs.xml** - contains information on the location of user documents.
- **Config.xml** - used to exclude features from the migration.

The operation of USMT is split into two separate programs:

- **ScanState** – needs to be run from an elevated command prompt and is used to scan the source computer in order to collect the files and settings. ScanState does not modify the source computer. By default, ScanState compresses the files and stores them as an image file.
- **LoadState** – also needs to be run from an elevated command prompt, and is used to migrate the files and settings from the store built by ScanState to the destination computer. LoadState migrates each file one at a time from the store to a temporary location on the destination computer where the files are decompressed and decrypted (if the encryption option was used). LoadState then transfers the file to the correct location, deletes the temporary copy, and begins migrating the next file.

Side-by-side migrations are exactly what they sound like: you need to move user data from one computer to another. This is often performed when you retire an older system in favor of newer hardware. When the install on the new hardware is complete, the new Windows 7 system should have all of the user configuration and software settings that were found on the old system. Additionally, if there is a need, the old system would still be available to go back to until it is retired or otherwise physically removed.

Wipe-and-load migrations are used when you are going to use the old hardware for Windows 7 but cannot directly upgrade the system, such as the scenario where Windows XP is already installed and you want to keep all of the user configuration and software settings.

Using the User State Migration Tool (USMT), you can transfer the collected information to a network share or a USB drive.

Once the clean installation of Windows 7 is complete, you can then import settings stored from the USMT operation back into the OS.

Another way to move user accounts, documents, internet favorites, digitally stored music and images and other similar files and settings would be to use **Windows Easy Transfer**.

Windows Easy Transfer is a utility that comes with Windows 7 and it can be used on systems running Windows XP, Windows Vista, or Windows 7 to new computers running Windows 7.

To use East Transfer, you would perform the following steps:

1. Run Windows Easy Transfer on the destination computer and select the transfer method that you are going to use.
    - **Easy Transfer Cable** – a special USB cable used on the host and destination systems during the migration
    - **Network** – host and destination systems running Windows Easy Transfer and are connected to the same local area network (for Side-by-side migrations only)
    - **External Storage** – run Windows Easy Transfer and specify an external hard drive or USB flash drive
2. Select the **This Is My New Computer** option. Select **No** when prompted as to whether Windows Easy Transfer has already saved your files. If you have chosen the Easy Transfer Cable or Network options you can skip this step.
3. On the **Do You Need to Install Windows Easy Transfer on Your Old Computer** page, select **I Need to Install It Now**.
4. Next, select the storage medium you on which want to install Windows Easy Transfer.

The Windows Easy Transfer application installation file will be copied to this location and this will allow you to install the application on the source computer.

Once Windows Easy Transfer is completely installed on the source computer, you can kick off the migration. If there is only a single user account to migrate all you need to do is can log on with that account. If you need to migrate all accounts on the local system you need to log on with a user account that has local administrator privileges.

When selecting items for migration, you can accept the defaults or you can select the advanced option to modify the selections.

You would use this option when logged in as the Administrator of the system to choose some or all of the local account on the system in addition to other settings and options such as backing up contacts, favorites, My music, My Pictures and so forth.

Domain Two: Deploying Windows 7

Capturing and Deploying a System Image

The Windows Automated Installation Kit (Windows AIK or WAIK) is a collection of tools and best practice information as supplied through included documentation that systems administrators can use to deploy Windows operating systems (including Windows 7) images to target systems as part of a deployment or to virtual machine image files (VHD).

ImageX is a command-line tool that enables you to capture, modify, and apply file-based disk images - the Windows image, .WIM - to target systems within your enterprise.

Windows Setup, Windows Deployment Services (Windows DS), and the System Management Server (SMS) Operating System Feature Deployment Pack are other technologies that can work with WIM files.

DISM.exe is the Deployment Image Servicing and Management (DISM) command-line tool that is available as part of the default installation of Windows 7 as well as version 2.0 of the Windows Automated Installation Kit.

In order to use WAIK tools, you'll need to download the ISO image from the Microsoft website (KB3AIK_EN.iso) and then burn the ISO to a bootable DVD.

Supported Operating Systems include Windows 7 and Windows Server 2008.

System requirements are listed as follows:

- Windows Server 2003 with Service Pack 2
- Windows Vista SP1
- Windows Server 2008 family
- Windows 7 family
- Windows Server 2008 R2 family

Additional tools not mentioned above that are included within the ISO image are:

- **Windows SIM** – opens Windows images, creates answer files, and manages distribution shares and configuration sets.
- **User State Migration Tool (USMT) –** used to migrate user data and is installed as part of the Windows AIK in the %PROGRAMFILES%\Windows AIK\Tools\USMT directory.

The final tool used to capture reference systems and deploy images to target systems is the Windows Preinstallation Environment (WinPE version 3.0).

WinPE is a striped down version of the Windows 7 operating environment and it functions as the replacement for the familiar MS-DOS mode or "real mode" installation boot segment that was present during the installation of legacy operating systems.

WinPE can be booted via the Preboot Execution Environment (PXE), DVD-ROM, UFD, VHD, or hard disk.

It also serves as the recovery platform to run 32-bit or 64-bit recovery tools such as the Windows Recovery Environment (Windows RE).

Preparing the Host System for Image Capture

You need to install Windows 7 on a reference system that will be used to create the image for deployment. You will probably have a need in a large production environment to automate as many of the steps as possible, so you'll need to create an answer file as well.

When you install the Windows AIK a sample answer file called **corp_autounattended_sample.xml** is available for viewing and editing at C:\Program Files\Windows AIK\Samples.

The beginning steps for creating an answer file for BIOS-based systems are:

1. Insert the Windows 7 DVD into the local DVD-ROM drive.
2. Go to the \Sources directory on the DVD and copy the Install.wim file from the Windows product DVD.
3. Navigate to: **Start** → **Programs** → **Windows AIK** to open the **Windows System Image Manager** (WSIM or Windows SIM).
4. In the Windows SIM, right-click **Select a Windows Image or Catalog File** and choose **Select Windows Image.**
5. In the Select a Windows Image dialog box, go to the location where you saved the install.wim file, and then click **Open**.
6. Depending on your setup, you may need to create a .clg file if one does not already exist.
7. If you have more than one Windows image in the .wim file, you will need to select the Windows image to open.
8. On the File menu, select **New Answer File**.
9. An empty answer file appears in the Answer File pane.

From here, add and customize additional Windows settings such as the disk configuration information and Windows Welcome settings; this is done by going into the Windows Image pane of Windows SIM and expanding the Components node to display available settings.

Different parts of the Windows operating system are installed in different configuration passes.

- **WindowsPE –** part of the installation where you are booting the Windows Setup media or starting the installation routine from another Windows installation.
- **OfflineServicing** – used to apply updates, drivers, or language packs to a Windows image. Starts automatically after the **windowsPE** configuration pass completes and before the computer reboots or during servicing scenarios when you specify an answer file with the Deployment Image Servicing and Management tool (DISM.exe).
- **Specialize** – used to create and configure information in the Windows image. Runs automatically when the Windows image boots for the first time or on the next boot after running the sysprep command with the /generalize option.
- **Generalize** – used to remove computer-specific information from the reference Windows installation such as the unique security ID (SID), unique device drivers, and other hardware-specific settings.
- **AuditSystem –** runs when the unattended Setup setting is configured: **Microsoft-Windows-Deployment\ Reseal\ Mode=Audit** while Windows is running in system context, before a user logs onto the computer in Audit mode.

- **AuditUser** – runs when the following unattended Setup setting is configured: **Microsoft-Windows-Deployment\ Reseal\ Mode=Audit** and is used to run custom commands or configure Windows Shell options.
- **OobeSystem** – runs when the following setting is configured: **Microsoft-Windows-Deployment | Reseal | Mode=OOBE** and is used to configure Windows Shell options, create user accounts, and specify language and locale settings.

Once you create all of you settings you'll want to validate them and save them.

1. Click Tools in Windows SIM and then choose Validate Answer File.
2. If there are any error messages or warnings in the Messages pane, you need to review and address them:
    - If you need to address an error, double-click the error message in the Messages pane, bringing you to the setting that is causing the error.
    - Change the setting to fix the error and run the validation again by choosing **Tools** → **Validate Answer File**.
    - You may need to go through this step more than once in order to get the file fully validated so you can save it.
3. Once it is validated you would go to the File menu, choose **Save Answer File**. Save the answer file as **autounattend.xml**.

Creating a WIM file from the Host System

In order to create a WIM file from the host system, you'll need to build up the reference system first. You'll do this by setting up your reference computer with a customized installation of Windows 7 that you'll image and then duplicate onto target systems.

You can create a reference installation by using the Windows installation DVD and inputting all of the required answers to system prompts by using an answer file.

The steps are:

1. You start the process by putting the Windows 7 DVD into the reference system and the media containing the answer file (Autounattend.xml).
    - You may need to restart the computer.
    - You may have to override the default boot order of the system to boot from the CD/ DVD-ROM disk.
2. The Windows Setup / installation routine will start automatically.
3. The installation routine will look in the root directory of all removable media for an answer file called Autounattend.xml.
4. The installation routine will continue through all of the installation steps and the different configuration passes on your system, using Autounattend.xml to answer any setup and configuration prompts.
5. Once Setup completes you can review that all of the system customizations were configured as expected from the Autounattend.xml settings.
6. To prepare the reference system from here you would run the Sysprep utility with the / generalize option to remove hardware-specific information and the /oobe option to configure the computer to boot to the Windows Welcome screen upon next full start up.

7. To do this you would run an elevated command prompt on the reference computer and enter:
    - **c:\windows\system32\sysprep\sysprep.exe /oobe /generalize /shutdown**
8. That command allows Sysprep to prepare the system for capture.
9. The reference installation now is complete and ready to be imaged.

You can store multiple Windows images in a single .wim file. The Windows Image file (.wim) allows you to choose to create architecture-specific .wim files or a single .wim file that contains images for multiple architecture types.

- 32-bit images only – create a .wim file that contains Windows images for just this single architecture type.
- 64-bit images only – create a .wim file that contains one or more of the 64-bit Windows images; due to the differences between x64-based and Itanium-based Windows images, you would need to create separate .wim files for each type of 64-bit image.
- 32-bit and 64-bit images – create a.wim file that contains multiple Windows editions for multiple architecture types as needed.

An outline of the steps for performing both actions is provided below. Where a single architecture is needed, just omit the other architecture steps.

1. Copy the entire 32-bit Windows distribution to a directory on the local computer.
2. Copy the 64-bit Install.wim file to another directory on the local computer.
3. At a command prompt, run the ImageX command to export the 64-bit Windows images to the Install.wim file.
4. Repeat the imagex /export command for each 64-bit Windows image that you want to add.

ImageX command-line options:

imagex /append image_path image_file {"description"} {/boot | /check | /config configuration_file.ini | /scroll | /verify | /logfile }

imagex /apply image_file image_number image_name image_path {/check | /ref | /scroll | /verify | /logfile}

imagex /capture image_path image_file "name" {"description"} {/boot | /check | /compress [type] | /config | /norpfix | /scroll | /verify| /logfile}

imagex /cleanup

imagex /commit mount_path image_name {/logfile}

imagex /commit /append mount_path new_image_name {/logfile}

imagex /delete image_file image_number image_name {/check| /logfile}

imagex /dir image_file image_number image_name {/logfile}

imagex /export src_file src_number src_name dest_file dest_name {/boot | /check | /compress [type] | /ref [splitwim.swm] | /logfile}

imagex /info img_file [img_number | img_name] [new_name] [new_desc] {/boot | /check| /logfile}

imagex /mount image_file image_number image_name image_path {/check| /logfile}

imagex /mountrw image_file image_number image_name image_path {/check| /logfile}

imagex /split image_file dest_file size {/check| /logfile}

imagex /unmount image_path {/commit| /logfile}

imagex /remount image_path {/logfile}

Performing a Manual Image Capture

The above outlined some of the details of performing an automated capture. The steps for performing a manual capture are not much different other than the process is manually performed.

1. The process begins by building a reference installation.
    - This can be done with a system already running with all of the applications installed.
    - You can also choose to build up a new system from the Windows 7 DVD.
    - The recommended way is to work with a new/clean build.
2. Boot the reference system from the DVD.
3. The Windows Setup / installation routine will start automatically.
4. The main steps of the manual install are the same as for a normal installation.
5. To prepare the reference system at this point for imaging you need to decide if you have any other applications that you want to install on the system as part of the base build. Once you do those installs or decide to take just the system as is with the operating system installed you can proceed.
6. The next step would be to run the Sysprep utility with the /generalize option to remove hardware-specific information and the /oobe option to configure the computer to boot to the Windows Welcome screen upon next full start up.
7. To do this you would run an elevated command prompt on the reference computer and enter:
    - **c:\windows\system32\sysprep\sysprep.exe /oobe /generalize /shutdown**
8. That command allows Sysprep to prepare the system for capture.
9. The reference installation now is complete and ready to be imaged.

Prepare a System Image for Deployment

There are a number of tools that allow you to insert an application into a system image, insert a driver into a system image and insert an update into a system image.

The WIM format allows you to make changes to an image offline. This includes adding or removing certain operating system components, applications, product updates, and drivers without having to create a new image.

Microsoft Deployment Toolkit (MDT) 2010 offers system administrators the ability to perform Lite Touch Installations (LTI) of Windows 7 in their environments. Generally MDT 2010 is run from a Windows Server 2008 system but you can run it from Windows 7.

Zero Touch Installation (ZTI) deployment methods using MDT 2010 require Microsoft System Center Configuration Manager 2007 as Zero Touch Installations using MDT 2010 do not work with SMS 2003.

Additionally, administrators can use the Deployment Image Servicing and Management (DISM) command line tool to edit their Windows images to install, uninstall, configure, and update Windows features, packages, drivers and international settings.

In order to run the tool you would need to start up a command interface with elevated permissions and then choose which of the features of the tool you want to run.

The command line options for the tool are shown below:

```
C:\Windows\system32>dism.exe /?

DISM.exe [dism_options] {WIM_command} [<WIM_arguments>]
DISM.exe {/Image:<path_to_offline_image> | /Online} [dism_options]
         {servicing_command} [<servicing_arguments>]
```

DESCRIPTION: DISM enumerates, installs, uninstalls, configures, and updates features and packages in Windows images. The commands that are available depend on the image being serviced and whether the image is offline or running.

WIM Commands	
/Get-MountedWimInfo	Displays information about mounted WIM images.
/Get-WimInfo	Displays information about images in a WIM file.
/Commit-Wim	Saves changes to a mounted WIM image.
/Unmount-Wim	Unmounts a mounted WIM image.
/Mount-Wim	Mounts an image from a WIM file.
/Remount-Wim	Recovers an orphaned WIM mount directory.
/Cleanup-Wim	Deletes resources associated with mounted WIM images that are corrupt.
Image Specifications	
/Online	Targets the running operating system.
/Image	Specifies the path to the root directory of an offline Windows image.
DISM Options	
/English	Displays command line output in English.
/Format	Specifies the report output format.
/WinDir	Specifies the path to the Windows directory.
/SysDriveDir	Specifies the path to the system-loader file named BootMgr.
/LogPath	Specifies the logfile path.
/LogLevel	Specifies the output level shown in the log (1-4).
/NoRestart	Suppresses automatic reboots and reboot prompts.
/Quiet	Suppresses all output except for error messages.
/ScratchDir	Specifies the path to a scratch directory.

Figure 9: DISM Command Line Options

You can get more information about some of the DISM options and their arguments, by specifying an option immediately before /? In order to Modify Images by Using DISM, follow steps similar to the ones outlined below.

1. Log on to the computer with an account that has administrator credentials.
2. Open an elevated command prompt and type md <DESTINATION> to create a destination folder (if you do not already have one).
3. Type DISM /mount-wim /wimfile:<DRIVE LETTER\FOLDER\image.wim> /name:<image_name> /mountdir:<PATH> to mount the WIM file to the mount directory.
4. You can type DISM /get-mountedwiminfo if you want to display information about the mounted image.
5. Once the image is mounted you would type cd <PATH> to go to the mount directory.
6. Once you are in that directory you would find the installation files for Windows 7 and modify them.
7. Next you would change directories by typing cd \ to go to the root directory.
8. You would then type DISM /image:<PATH> /? to display the available options for making changes to the image you've mounted.
9. Next you would type DISM /image:<PATH> /add-driver /driver:<DRIVE LETTER\FOLDER\INF> to add the driver (INF) file to the image in the mount directory.
10. Once you are finished making your changes you would type DISM /unmount-wim /mountdir:<path_to_mount_directory> /discard to unmount the image from the mounted folder and discard changes.

Manual Deployment of a Customized Image

If you need to do a manual deployment of a customized image that is hosted from a network share to a system that does not already have an operating system installed, you will need to configure partitions on the drive and format them so that you can copy the image over.

Microsoft recommends, for image-based deployments, that you use the DiskPart tool to create the partition structures on your destination computers and they recommend the following parameters to be run either manually or from a script.

First, boot the target system from the WindowsPE media and open a command prompt and enter DISKPART.

Once there you can enter each of the lines below manually (each is an individual action) or launch them from a batch file:

- select disk 0
- clean
- create partition primary size=300
- format quick fs=ntfs label="System"
- assign letter="S"
- create partition primary
- format quick fs=ntfs label="Windows"
- assign letter="W"
- exit

The remaining steps for deploying the image manually to the target system are as follows:

1. You would copy the image from the network share to your local hard drive (in this case the W drive). You can install directly from the network location if you wish.
2. Apply the image to the hard drive by using the ImageX tool located on the WindowsPE media: **imagex.exe /apply W:\IMAGE.wim 1 S:**
3. When that step completes you would use BCDboot to initialize the Boot Configuration Data (BCD) store and copy boot environment files to the system partition. In this example it would be W:\windows\system32\bcdboot W:\windows.

Configure a VHD

Windows 7 Enterprise or Ultimate can use Virtual Hard Disk (VHD) booting to use VHD environments even when there isn't a parent operating system present or in the place of the parent operating system in a dual boot configuration.

There are a few configuration steps that you need to take in order to use this feature.

You'll need to create a VHD which you can do with either the DiskPart tool or the Disk Management MMC:

1. From the Disk Management MMC on a system where Windows 7 is already up and running you would go to ACTION on the menu and choose Create VHD:

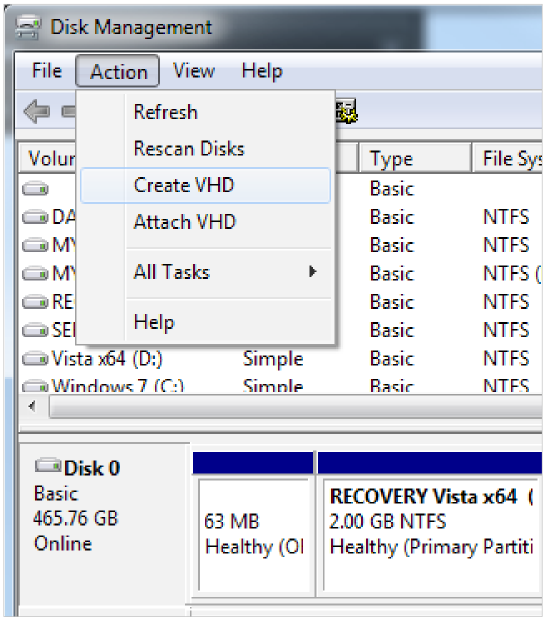
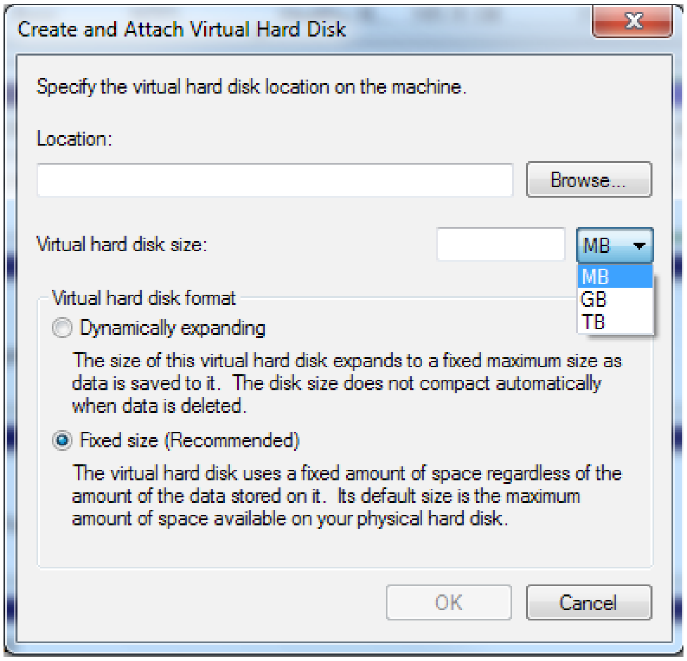


Figure 10: Creating a VHD

2. Next, specify a location for the VHD as well as the initial size of the VHD and whether you wanted it to remain a fixed size or allow it to be a dynamically expanding virtual hard disk.



Create and Attach Virtual Hard Disk

Specify the virtual hard disk location on the machine.

Location:

Virtual hard disk size: MB

Virtual hard disk format

○ Dynamically expanding

The size of this virtual hard disk expands to a fixed maximum size as data is saved to it. The disk size does not compact automatically when data is deleted.

● Fixed size (Recommended)

The virtual hard disk uses a fixed amount of space regardless of the amount of the data stored on it. Its default size is the maximum amount of space available on your physical hard disk.

Figure 11: VHD Options

3. Once the disk is created, you can use the Disk Management MMC to attach the VHD so that it can be accessed as a drive and not as a static file.
4. Initially, the disk is going to be in an unknown state and you'll need to right click the disk in order to bring up the available actions which would allow you to initialize the disk.

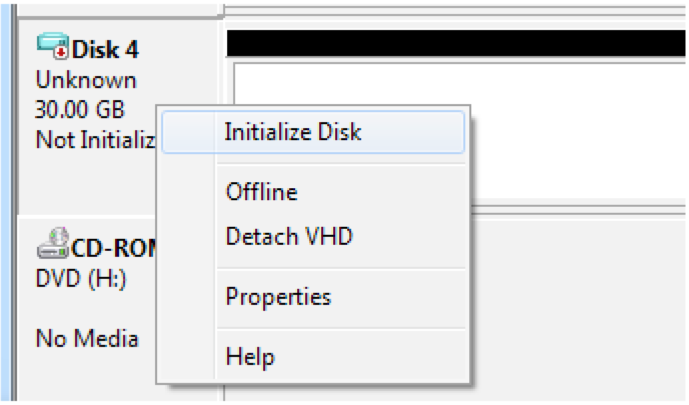


Figure 12: Initializing the VHD

5. Once the disk is initialized, the VHD file can be directly accessed through the host operating system.

Once the VHD has been set up and has an operating system available the VHD can be deployed to run as a virtual machine as a guest or for native boot in place of the host operating system.

The Diskpart command-line utility can be used to create and attach a VHD as follows:

1. Launch an elevated Command Prompt .
2. Type **DISKPART.**
3. Enter **CREATE vdisk file=DRIVE LETTER\FOLDER\FILENAME.vhd maximum=30000.**

Note: This will create a VHD file with a maximum size of 30 GB at the drive letter and folder destination you indicated with the file name you choose.

4. Next type **SELECT vdisk file= DRIVE LETTER\FOLDER\FILENAME.vhd.**
5. From there you would enter **ATTACH vdisk.**
6. The next step would be to enter **CREATE partition primary.**
7. Enter **ASSIGN letter**=**DRIVE LETTER (**for the name of the drive letter you want to assign).
8. The next step is to enter **FORMAT quick label=Windows7VHD.**

If you need to configure native-boot on a system you can use Bcdedit.exe to add a boot entry for the VHD file.

The Boot Configuration Data Store Editor

The Boot Configuration Data Store Editor (BCDEDIT) command-line tool modifies the boot configuration data store which contains boot configuration parameters and controls how the operating system is booted that were previously in the Boot.ini file on Windows XP, Windows Server 2003 and older systems.

In order to do this you would open an elevated command prompt and enter the following:

```
C:\Windows\system32>Bcdedit /copy {current} /d "NEW"
```

That should give you a result similar to the following:

```
The entry was successfully copied to {84ba3e14-0049-11de-8bfb-ec4875b150a8}.
```

Your GUID for the loader object is going to be different for obvious reasons. Use your GUID value in the commands below:

- bcdedit /set <YOUR_GUID> device vhd=[**DRIVE LETTER**]**FOLDER**\ **FILENAME.vhd**
- bcdedit /set <YOUR_GUID> osdevice vhd=[**DRIVE LETTER**]**FOLDER**\ **FILENAME.vhd**

BCDEdit locates the VHD file and Bootmgr locates the partition containing the VHD File to boot from. The next command you need to enter is:

- bcdedit /set <YOUR_GUID> detecthal on

Detecthal forces Windows 7 to automatically detect the Hardware Abstraction Layer (HAL). You can also run **bcdedit /v** to test if your boot entry is successfully created. The **bcdedit /delete <YOUR_GUID> / cleanup** command can be used to delete an existing VHD entry from the Boot menu.

Windows Image to Virtual Hard Disk Converter Tool

The Windows Image to Virtual Hard Disk (WIM2VHD) Converter command-line tool which runs using Cscript (the command-line Windows Scripting Host engine) can be used to create VHD images from any Windows 7 installation source or from an image in a custom WIM file.

By default, the WIM2VHD tool creates VHDs that boot directly to the Out-of-Box Experience (OOBE) environment; that result can be automated by using an Unattend.xml file.

In order to successfully utilize WIM2VHD, you need create a native VHD on your client computer running Windows 7. You will also need to have the Windows AIK installed and an operating system image in a WIM file.

The formal set of requirements to use the tool is:

- A machine running Windows 7 RTM or higher, Windows Server 2008 R2 RTM or higher, or Windows Server 2008 SP2 with Hyper-V RTM enabled.
- Either the Windows 7/Server 2008 R2 Automated Installation Kit (AIK) or the Windows 7/Server 2008 R2 OEM Preinstallation Kit (OPK) needs to be installed.
- Windows 7 or Windows Server 2008 installation media.

So in a scenario like that your entry might look as follows:

```
CSCRIPT WIM2VHD.WSF /WIM:X:\sources\install.wim /SKU:ULTIMATE
/UNATTEND:C:\FOLDER\unattend.xml
```

The Offline Virtual Machine Servicing Tool 2.0.1 allows system administrators to maintain their offline virtual machines in their Microsoft System Center Virtual Machine Manager library.

The tool provides a way to keep offline virtual machines up-to-date with respect to hotfixes and security updates so that once an offline machine is brought online and into service it will not potentially introduce vulnerabilities in the intranet due to missing updates.

The tool uses the following software update management systems:

- Windows Server Update Services (WSUS) 3.0 or WSUS 3.0 SP1
- System Center Configuration Manager 2007, Configuration Manager 2007 SP1, or Configuration Manager 2007 R2

The tool manages the updates based on lists of existing virtual machines stored in the Virtual Machine Manger (VMM) and a set of servicing jobs by running snippets of Windows PowerShell scripts.

For each virtual machine, the servicing job will use the Windows Task Scheduler to determine when to run the servicing job and then perform the following steps:

1. Initialize the virtual machine by deploying it to a host and starting it up.
2. Trigger the appropriate software update cycle (Configuration Manager or WSUS).
3. Shut down the updated virtual machine and returns it to the library.

The servicing job specifies which virtual machines to update, what resources to use for the update process, and when to start the servicing job. This can be configured to setup and schedule jobs to run at VM initialization or during low-traffic maintenance windows.

Domain Three: Configuring Hardware and Applications

Configure Devices

Device drivers are software packages that act as a translator between a hardware device and the operating system. In order for the hardware to function properly on the system the correct device driver for that hardware must be installed.

Generally, Plug and Play devices will install drivers automatically when they are provided within the driver cache; otherwise, you may need to supply the software that came with the device or download updates from Microsoft or the hardware manufacturer.

You can also use Device Manager to install and update drivers as well as change the hardware settings for those devices, and troubleshoot problems.

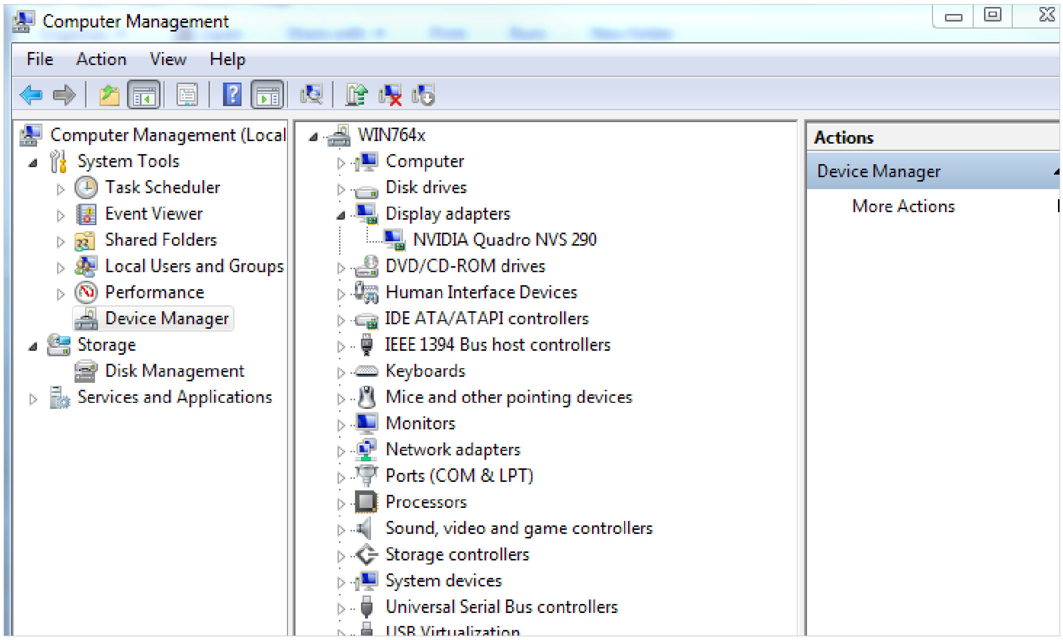
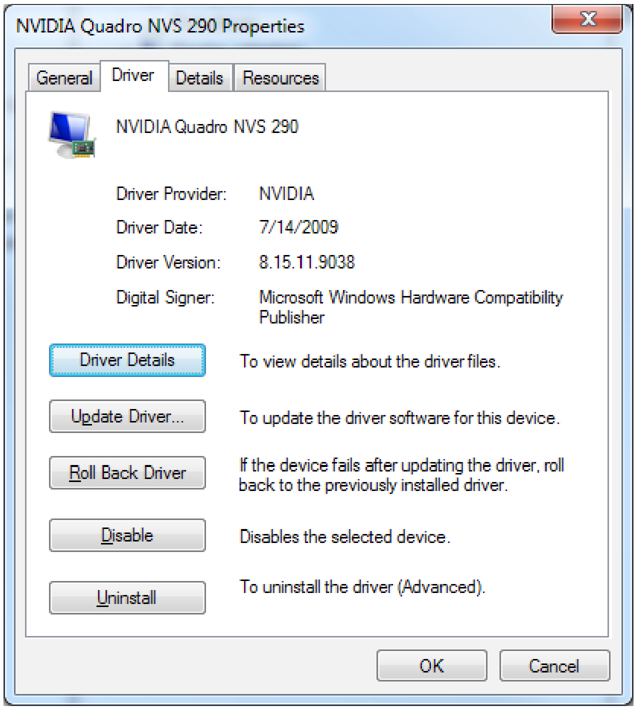


Figure 13: Windows 7 Device Manager in the Computer Management MMC

When using the Device Manager or the Computer Management MMC, all you need to do in order to review the status of a device and the driver configuration is to select the device and right click it to review the property page and the associated tabs.



NVIDIA Quadro NVS 290 Properties

NVIDIA Quadro NVS 290

Driver Provider: NVIDIA

Driver Date: 7/14/2009

Driver Version: 8.15.11.9038

Digital Signer: Microsoft Windows Hardware Compatibility Publisher

Driver Details — To view details about the driver files.

Update Driver... — To update the driver software for this device.

Roll Back Driver — If the device fails after updating the driver, roll back to the previously installed driver.

Disable — Disables the selected device.

Uninstall — To uninstall the driver (Advanced).

Figure 14: A Driver Details tab

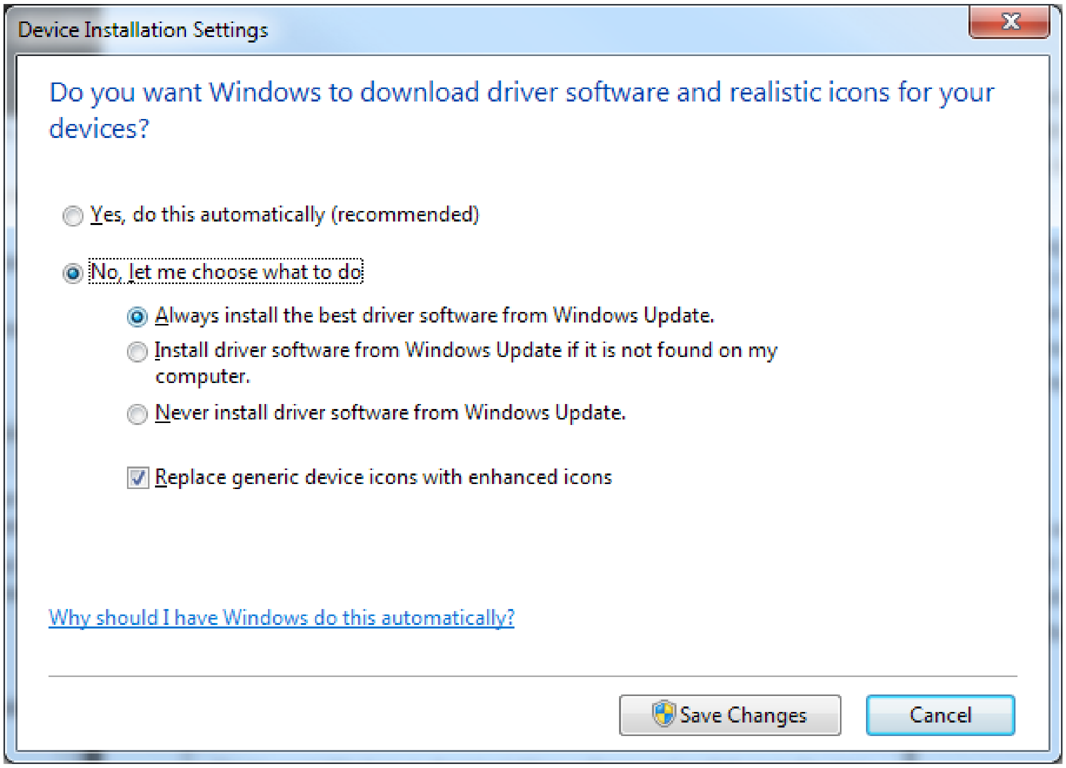
The **General** tab will display basic information about the device and give you the status of the device (whether or not it is working correctly).

The **Driver** tab will provide you with the options to review the **Driver Details** and the files and the different drivers and versions in use for the hardware.

You also have the option right from the **Driver** tab of the properties page to choose the **Update Driver** option which will allow you to start a search for newer software for the hardware device.

You have the option to browse the local system for the driver that you might have manually downloaded or are providing through an installation CD or DVD ROM or you can choose to search automatically for updated drivers. This option will have the Windows operating system search both your local system for new drivers that might already be present as well as the Internet.

You will need to be connected to the Internet in order for the external search to be successful and you'll need to make sure you haven't previously disabled the feature in the device installation settings.



Device Installation Settings

Do you want Windows to download driver software and realistic icons for your devices?

○ Yes, do this automatically (recommended)

● No, let me choose what to do

● Always install the best driver software from Windows Update.

○ Install driver software from Windows Update if it is not found on my computer.

○ Never install driver software from Windows Update.

☑ Replace generic device icons with enhanced icons

Why should I have Windows do this automatically?

Figure 15: Searching for Device Drivers

The default setting is **Yes, do this automatically** but if you make changes to the default behavior, updates will only be performed as you have outlined.

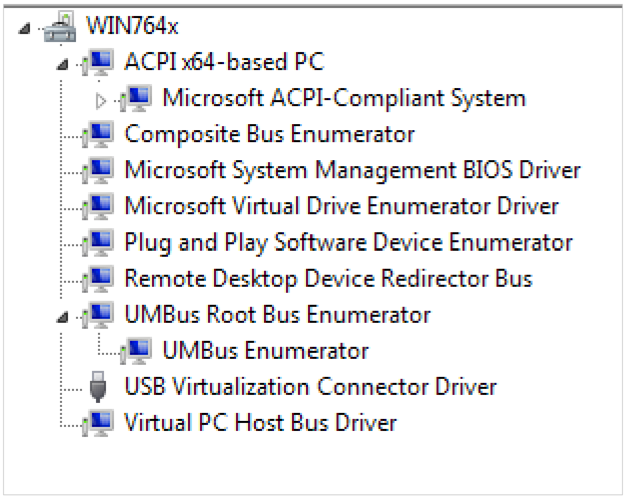
The **Driver** tab also provides the **Roll Back Driver** option if the hardware device fails after updating the driver. This can happen if the driver simply does not install correctly for some reason or in a situation where an update has successfully installed but has cause a new error or some other conflict.

The additional options available on the **Driver** tab allow you to **Disable** the device as well as **Uninstall** the driver.

The Computer Management MMC also allows you to look at the different resources devices are using on your Windows 7 installation.

This is done by changing the default view of the devices (**Devices by type**) to one of the other options.

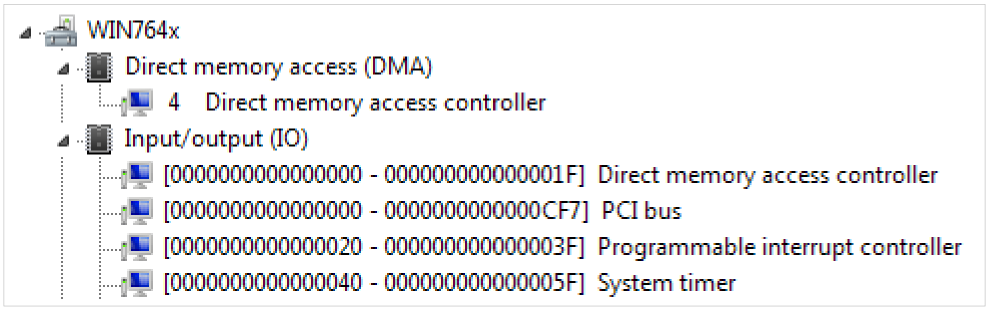
When you view Devices by connection you are able to see how the devices are connected and enumerated.



```
WIN764x
    ACPI x64-based PC
        Microsoft ACPI-Compliant System
    Composite Bus Enumerator
    Microsoft System Management BIOS Driver
    Microsoft Virtual Drive Enumerator Driver
    Plug and Play Software Device Enumerator
    Remote Desktop Device Redirector Bus
    UMBus Root Bus Enumerator
        UMBus Enumerator
    USB Virtualization Connector Driver
    Virtual PC Host Bus Driver
```

Figure 16: Viewing Devices by Connection

When you view **Resources by type** you are presented with the system view of how the hardware is interacting with the system, whether it's through Input/output (I/O), Direct Memory Access (DMA), Interrupt request (IRQ), or through **Memory** space allocation and addressing.



```
WIN764x
    Direct memory access (DMA)
        4    Direct memory access controller
    Input/output (IO)
        [0000000000000000 - 000000000000001F]  Direct memory access controller
        [0000000000000000 - 0000000000000CF7]  PCI bus
        [0000000000000020 - 000000000000003F]  Programmable interrupt controller
        [0000000000000040 - 000000000000005F]  System timer
```

Figure 17: Viewing Resources by Type

When you have situation where you need to install a legacy device that is not plug and play compliant you will need to install the driver directly from the source CD or DVD or from the downloaded installation files.

Also, you may need to use the **Device Manager** to choose the **Add legacy hardware** control in order to start the Add Hardware Wizard in an effort to get the device installed.

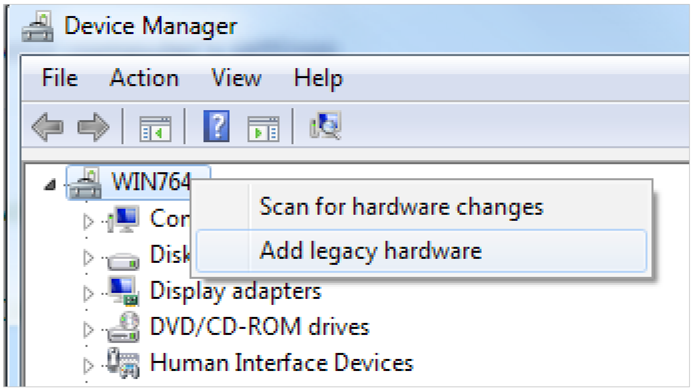


Figure 18: Adding Legacy Hardware

Driver Signing Requirements for Windows are set up to have drivers use digital signatures which allows one to know whether a legitimate publisher has provided the software package.

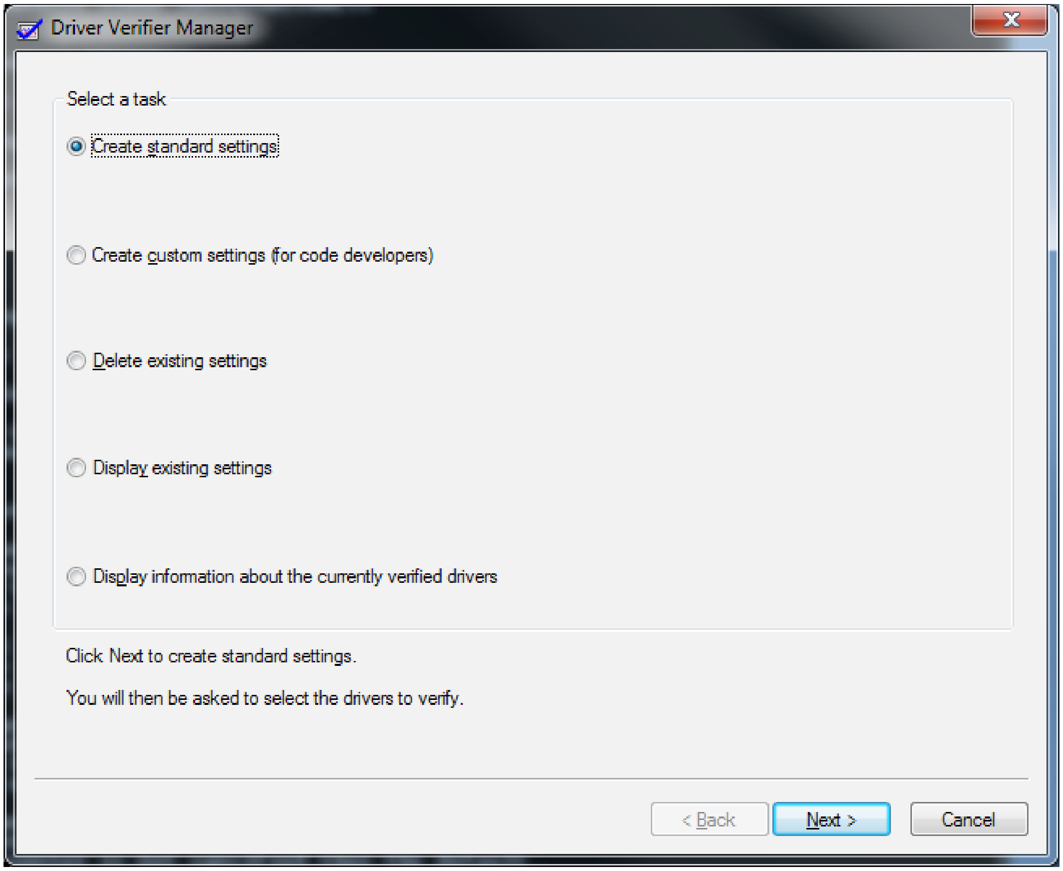
For the newer desktop and server operating systems from Microsoft (Windows Vista, Windows 7 and Windows Server 2008) digital signature requirements are laid out as follows.

- Administrator privilege is required to install unsigned kernel-mode components. This includes device drivers, filter drivers, services, and so on.
- x64 versions of Windows Vista, Windows 7 and Windows Server 2008 require Kernel Mode Code Signing (KMCS) in order to load kernel-mode software.
- Driver binaries that load at boot time ("boot start drivers") must contain an embedded signature, for both x86 and x64 versions of Windows Vista, Windows 7 and Windows Server 2008.
- Installation packages and self-extracting executables that are downloaded must be digitally signed in order to run or install without additional administrative interaction.
- Digital signatures are required for hardware-related drivers and other kernel components submitted for the Windows Logo Program.
- Components must be signed by a certificate that Windows "trusts".

When you encounter issues with drivers such as errors and conflicts you can use the **Driver Verifier Manager** tool to work on a solution.

Driver Verifier Manager is used to detect errors in kernel-mode drivers as it can test and trap conditions that might otherwise go unnoticed in normal operation. The tool verifies that drivers are not making illegal function calls or causing system corruption. It can identify conditions such as memory corruption, mishandled I/O request packets (IRPs), invalid direct memory access (DMA) buffer usage, and possible deadlocks.

It has both a GUI interface as shown below and it can be run from a command line as well.



Select a task

● Create standard settings

○ Create custom settings (for code developers)

○ Delete existing settings

○ Display existing settings

○ Display information about the currently verified drivers

Click Next to create standard settings.

You will then be asked to select the drivers to verify.

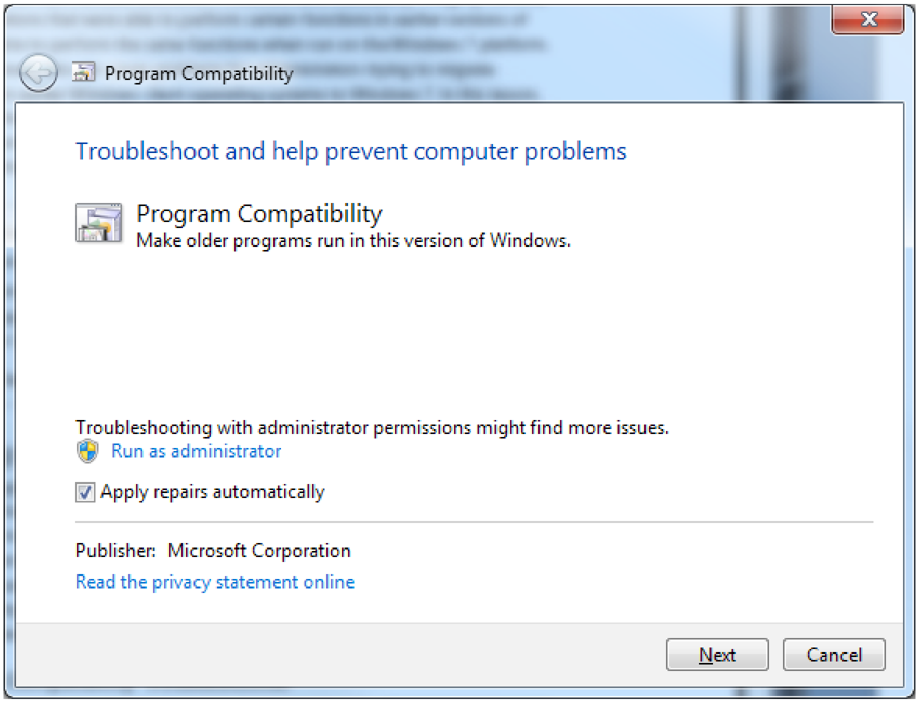
Figure 19: The Driver Verifier Manager

Configure Application Compatibility

Architecture and security improvements in the way that the Windows 7 operating system handles application security with respect to things such as Data Execution Protection and Mandatory Integrity Control is going to cause some issues with application compatibility.

Under legacy operating systems, such as Windows XP and earlier, you're going to have situations where applications were able to perform certain functions but under Windows Vista and Windows 7, they are prohibited. This will cause issues with older applications.

The **Program Compatibility Troubleshooter** is a tool that you can use to configure application compatibility settings based on a set of tests that it performs on an application. When you run the tool and choose the **Apply repairs automatically** option, the tool will attempt to create solutions to compatibility problems. If it can do that, the solution is saved and the application functions without causing problems in the future.



Program Compatibility

Troubleshoot and help prevent computer problems

Program Compatibility
Make older programs run in this version of Windows.

Troubleshooting with administrator permissions might find more issues.
Run as administrator

☑ Apply repairs automatically

Publisher: Microsoft Corporation
Read the privacy statement online

Figure 20: The Program Compatibility Troubleshooter

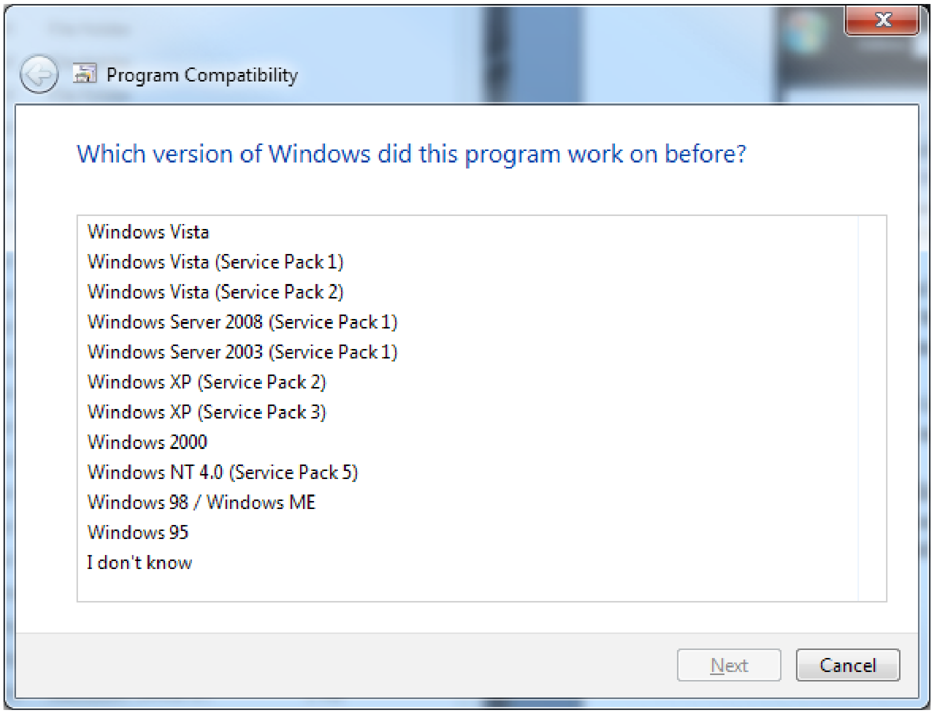
The Program Compatibility troubleshooter works only with executable files and it cannot be used to troubleshoot installations and files in .MSI format.

You can start the tool by right-clicking a problematic application shortcut or file and then selecting Troubleshoot Compatibility from the context menu.

If the issue you're experiencing can't be resolved automatically by the Program Compatibility troubleshooter, you'll need to try to manually specify a built-in **compatibility mode** to resolve the issue.

The compatibility modes are intended to replicate previous operating system environments as much as possible, but configuring the application to run under the previous operating system does not always resolve the issue.

The available compatibility modes are included in the Figure below:



Which version of Windows did this program work on before?

Windows Vista
Windows Vista (Service Pack 1)
Windows Vista (Service Pack 2)
Windows Server 2008 (Service Pack 1)
Windows Server 2003 (Service Pack 1)
Windows XP (Service Pack 2)
Windows XP (Service Pack 3)
Windows 2000
Windows NT 4.0 (Service Pack 5)
Windows 98 / Windows ME
Windows 95
I don't know

Figure 21: Compatibility Modes

Additionally, beyond the defaults provided through the operating system selection that you choose, there are other compatibility options that you can use to configure an application.

- **Run In 256 Colors** – allows you to run applications designed to run with a limited color pallet to display correctly.
- **Run In 640 x 480 Screen Resolution** – allows you to run applications that are designed to run in low resolution and do not support higher resolutions to display properly.
- **Disable Visual Themes** – you configure this setting to resolve issues that are brought out from using visual themes which can cause display problems in some applications.
- **Disable Desktop Composition** – disables features of the Aero user interface such as transparency while the application is active.
- **Disable Display Scaling On High DPI Images** – turns off automatic resizing of applications if large-scale fonts are being used and it addresses issues with large-scale fonts that adversely impact an application's appearance.
- **Run This Program As An Administrator** – addresses the issue of older programs that require administrative privileges as they are not able to prompt for elevation that would generate the User Account Control dialog box for the user to acknowledge. Enabling this option forces the program to run in the Administrator context to get around that limitation. Because of that, only users that have administrative privileges on the computer are able to run the program.
- **Change Settings For All Users** – this setting configures compatibility settings for all users of the computer. When you configure compatibility options, they only apply to the currently logged on user by fault and this setting changes that behavior.

The Application Compatibility Toolkit (ACT) is actually a set of tools you can use to resolve application compatibility issues before deploying a new operating system.

The ACT contains the following components:

- **Application Compatibility Manager** – allows you to resolve a large number of application compatibility issues that might occur when you attempt to deploy an existing application on Windows 7.
- **Compatibility Administrator** – provides compatibility fixes and modes that can resolve problems with existing software. Many existing applications already have compatibility fixes that allow them to run on the Windows 7 platform and the compatibility administrator may already have a default solution for your application problem.
- **Internet Explorer Compatibility Test Tool –** allows you to test existing Web sites to determine if they have compatibility problems that may become evident under Internet Explorer 8 as this is the version of Internet Explorer that ships with Windows 7.
- **Setup Analysis Tool** – monitors the actions taken by application installers and can detect compatibility issues in the installation of kernel mode drivers and 16-bit components as well as the installation of Graphical Identification and Authentication dynamic-link libraries (DLLs). The tool can also handle compatibility issues with respect to the modification of files or registry keys that are guarded by Windows Resource Protection (WRP).
- **Standard User Analyzer** – allows you to test applications for potential compatibility issues caused by User Account Control (UAC).

A software compatibility fix is sometimes referred to as a shim. A **shim** is a is a small piece of code that intercepts an application programming interface (API) call and the parameters passed, either handling the operation itself or redirecting it. The end result of this action is to modify the call so that the result, in Windows 7, is similar to what was experienced in prior versions of Windows operating systems.

Configure Application Restrictions

Software Restriction Policies are a technology managed through Group Policy under Windows 7 for domain managed systems. It is found in the Computer Configuration\Windows Settings\Security Settings\Software Restriction Policies node.

It is also available to use on domain joined systems running Windows XP, Windows Vista, Windows Server 2003, and Windows Server 2008.

It is also possible to set these up as part of a local security policy setting on individual systems.

Software Restriction Policies allows administrators to set the Unrestricted setting to allow an application to run unimpeded and it also has the Disallowed configuration setting which blocks an application from executing.

There are four different types of software restriction policy settings:

- **Hash Rule** – a fingerprint of a specific file.
- **Certificate Rule** – a rule that is set up against a software publisher's digital signature.
- **Path Rule** – a rule that is set to look for a specific local or universal naming convention (UNC) path or path set in the registry.
- **Zone Rule** – a rule that verifies which zone a user is downloading an application from (e.g. Internet Zone or Local Intranet, etc).

Each of these policies has certain limitations.

Hash rules will be broken if the application is changed such as in a situation when it is updated with patches, fixes, security updates, etc. In order for hash rules to remain effective the application needs to stay in a static state or the hash rule needs to be updated when the application is updated.

Path rules are only effective when application installs are made in the default location. The Path rule when used with a Registry path configuration is more difficult to circumvent, but they are also harder to create because you'll need to know exactly which registry keys a specific application creates.

Certificate rules are probably the most effective kind of software restriction policies. They do have some limitations in that not all application publishers use certificates to digitally sign their software.

Zone rules are only effective if an application is run as its downloaded. If an application is saved to disk, then a zone rule has no way of knowing the application's origin.

The Security Levels are the designations that you set in order to put Software Restriction Policies into a default rule. The default rule is used when there is no other designated Software Restriction Policy that applies to an application.

- **Disallowed –** users do not have the rights to execute an application if the application is not explicitly allowed by an existing Software Restriction Policy.
- **Basic User** – users have the rights to execute applications so long as those applications do not require administrative access rights. Users are able to access applications that require administrative access rights only if a rule has been created that covers that application.
- **Unrestricted** – users are able to execute a application unless the application is explicitly blocked by an existing Software Restriction Policy.

Configure Internet Explorer

Internet Explorer **Compatibility View** allows you to set the browser to a state where it can render sites originally designed for previous versions of Internet Explorer. You can enable Compatibility View for a page by clicking the broken page icon at the end of the address bar:

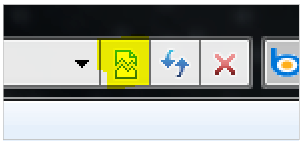
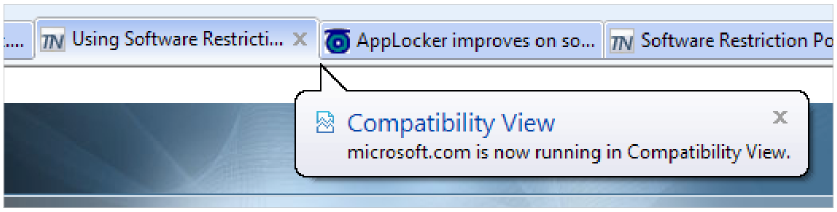


Figure 22: Enabling Compatibility View

Compatibility View settings can be set through the Compatibility View Settings dialog box from the Tools menu of Internet Explorer.

When you are on one tab of the browser and you choose Compatibility View a pop up will appear briefly to let you know that one tab is running under that view.

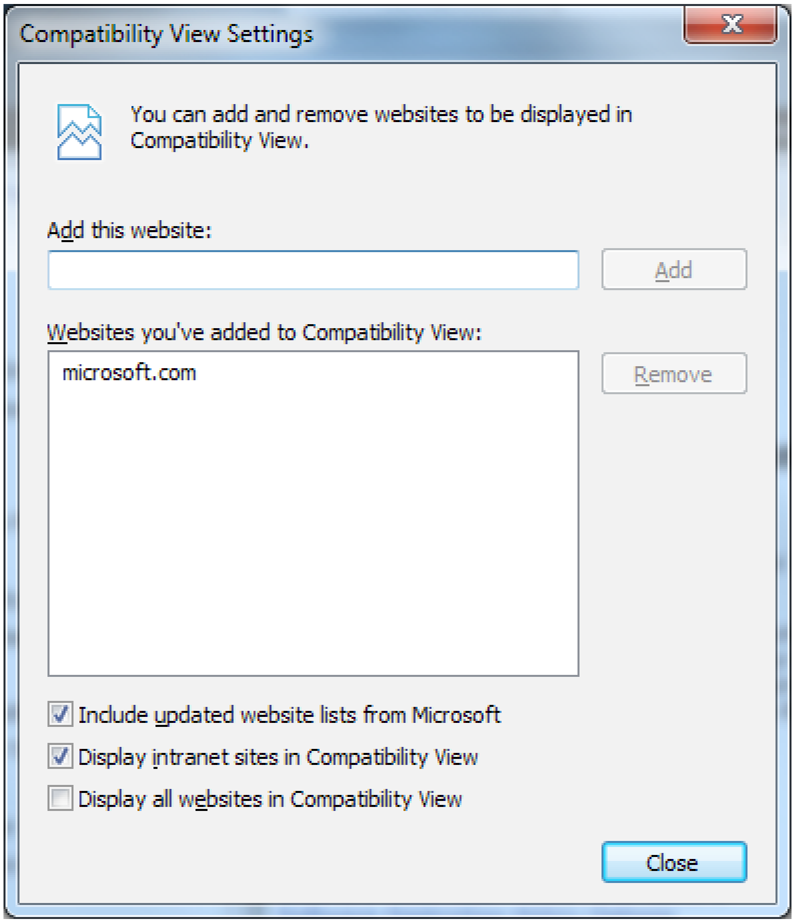


Compatibility View
microsoft.com is now running in Compatibility View.

Figure 23: Compatibility View Enabled

Additionally, if you drop the context menu again from Tools you'll see there is a check mark next to Compatibility View for that tab. You would also notice that the broken page icon at the end of the address bar is now blue in color. When it is not in Compatibility View mode it is clear.

While you can do this on the fly, as needed, you can configure the Compatibility View Settings to always use Compatibility View mode for specific websites by adding them as shown below:



Compatibility View Settings

You can add and remove websites to be displayed in Compatibility View.

Add this website:

Websites you've added to Compatibility View:

microsoft.com

☑ Include updated website lists from Microsoft

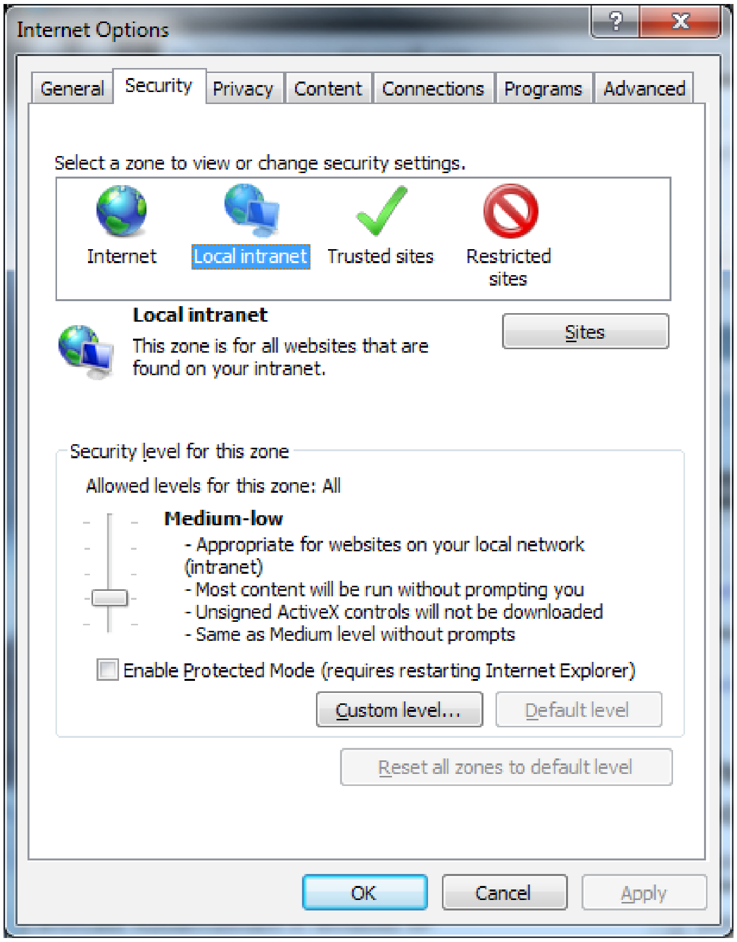
☑ Display intranet sites in Compatibility View

☐ Display all websites in Compatibility View

Figure 24: Adding sites to Compatibility View

When you choose a particular tab to temporarily view it in Compatibility View mode, you'll notice the entire website by DNS name is added to always use Compatibility View mode. You can remove the site by highlighting it and selecting REMOVE or by clearing the Compatibility View setting from the TOOLS context menu.

Internet Explorer can be configured for different levels of security by using built in security zones. These security zones and corresponding settings are on the Security tab of the Internet Options properties page:



Select a zone to view or change security settings.

Local intranet

This zone is for all websites that are found on your intranet.

Security level for this zone

Allowed levels for this zone: All

Medium-low

- Appropriate for websites on your local network (intranet)
- Most content will be run without prompting you
- Unsigned ActiveX controls will not be downloaded
- Same as Medium level without prompts

□ Enable Protected Mode (requires restarting Internet Explorer)

Figure 25: Security Zones

- **Internet –** the default zone for all Web sites not contained in the Local Internet, Trusted Sites, or Restricted Sites zones. This zone is set to Medium-High, by default, and blocks websites from viewing private data from other Web sites. Sites in this zone are unable to make changes to Windows 7. Protected Mode is enabled by default for sites in this zone.
- **Local Intranet** – use this zone setting for computers on your local intranet. Local intranet sites will be automatically detected and you can manually add Web sites to this zone by clicking the Advanced button on the Local Intranet sites dialog box. The default security level of this zone is Medium-Low. Protected Mode is not enabled by default for sites in this zone although you can enable it by selecting the Enable Protected Mode checkbox.

- **Trusted Sites** – this zone contains websites that for one reason or another require elevated privileges during the browsing session. This zone uses fewer security precautions with sites that are contained within the zone so special care should be taken to only add necessary sites and no others. You can add sites through the Trusted Sites dialog box and the default security level for this zone is Medium. Protected Mode is not enabled by default for sites in this zone. The default setting for this site requires that all the sites need to be secured with a Secure Sockets Layer (SSL) certificate.
- **Restricted Sites** – this zone is intended for sites that are potentially dangerous with respect to security or are of a questionable nature as to their design. Sites should be added to this zone as necessary if you have some need to visit them for some intended purpose (e.g. security research). The default security level for this zone is High and Internet Explorer Protected Mode is enabled by default for sites in this zone.

Configuring InPrivate Browsing Mode

The new InPrivate Browsing feature allows you use Internet Explorer 8 to browse sites on the web without effectively leaving any of the details of your activity on the local system and in the browser cache.

This is a new security and privacy option that is useful in situations where you would like to minimize what anyone else might see when they are using your computer on in a scenario where you are using someone else's system or perhaps a public kiosk.

You can start an InPrivate Browsing session from the New Tab page or the Safety button.

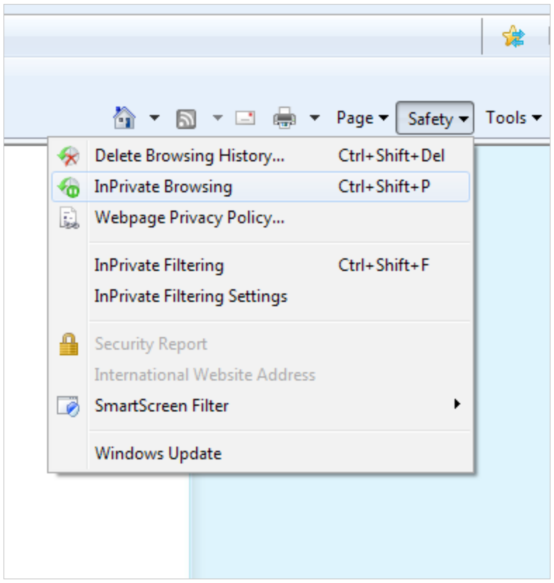

Page
Safety
Tools
Delete Browsing History... Ctrl+Shift+Del
InPrivate Browsing Ctrl+Shift+P
Webpage Privacy Policy...
InPrivate Filtering Ctrl+Shift+F
InPrivate Filtering Settings
Security Report
International Website Address
SmartScreen Filter
Windows Update

Figure 26: Starting InPrivate Browsing

When you choose the option to start an InPrivate Browsing session, Internet Explorer will open a new browser window.

As long as you are using this InPrivate Browsing configured session, you are able to open as many tabs as you want within this open browser window and your activity will be protected by the InPrivate Browsing privacy functionality.

If you open another browser window from the Internet Explorer short cut, that window will not be protected by InPrivate Browsing unless you activate it for that newly launched session.

When you are using your InPrivate Browsing active session, Internet Explorer will store required information such as cookies and temporary Internet files that are required for proper session functionality so that sites your visit will work correctly where a certain amount of data caching is expected and so forth. The privacy features kick in when you finish your InPrivate Browsing session and all of the active data and information is discarded.

The list below outlines the data that InPrivate Browsing with discard when you close the browser and how it is affected during your browsing session:

- **Cookies** – kept in memory so pages work correctly, but cleared when you close the browser.
- **Temporary Internet Files** – stored on disk so pages work correctly, but deleted when you close the browser.
- **Webpage History** – this information is not stored.
- **Form Data and Passwords** – This information is not stored.
- **Anti-Phishing Cache** – temporary information is encrypted and stored so pages work correctly.
- **Address Bar and Search AutoComplete** – this information is not stored.
- **Automatic Crash Restore (ACR)** – ACR can restore a tab when it crashes in an InPrivate session, but if the whole window crashes, data is deleted and the window cannot be restored.
- **Document Object Model (DOM) Storage** – DOM storage is a kind of "super cookie" web developers can use to retain information. Like regular cookies, they are not kept after the window is closed.

InPrivate Browsing sessions cannot manage all aspects of security and confidentiality; while it does handle most of the potential items, there are a few limitations.

InPrivate Browsing will not encrypt your network traffic to the websites that you visit. People who might be using your computer will not be able to look at the history or the cache to see where you were browsing but it wouldn't stop someone on your network that is actively scanning network traffic from seeing the data coming and going to your system.

InPrivate Browsing privacy does prevent websites that purposefully track user access to keep from identifying you through your IP address or other network designation. Additionally, anything you do or enter on that website can be recorded if they do that level of usage monitoring and record keeping. This would again most likely be done through the registration of your IP address which could be back tracked to your ISP if / as needed.

When you make any manual changes such as adding favorites, adding RSS feeds, changing your home page, etc while using an InPrivate Browsing session the changes will be maintained when you close out your InPrivate Browsing session.

Domain Four: Configuring Network Connectivity

Configure IPv4 Network Settings

Before we can cover IPv4 configuration, we need to briefly review IPv4 basics. IPv4 addresses are made up of both the numerical designation of the system (host name) and the numerical designation of the network (network name). IPv4 addresses are 32-bit addresses divided into four octets that are shown in the binary format in dot decimal form such as 192.168.1.100.

The subnet mask is the delineation mark that shows the segment of an address that represents the network and the segment that represents the host. IP addresses were originally set up in five classes:

Class	Range	Notes
A	1.0.0.1 to 126.255.255.254	Supports 16 million hosts on each of 127 networks.
B	128.1.0.1 to 191.255.255.254	Supports 65,000 hosts on each of 16,000 networks.
C	192.0.1.1 to 223.255.254.254	Supports 254 hosts on each of 2 million networks.
D	224.0.0.0 to 239.255.255.255	Reserved for multicast groups.
E	240.0.0.0 to 254.255.255.254	Used only for Testing / Research

Figure 27: IPv4 Address Classes

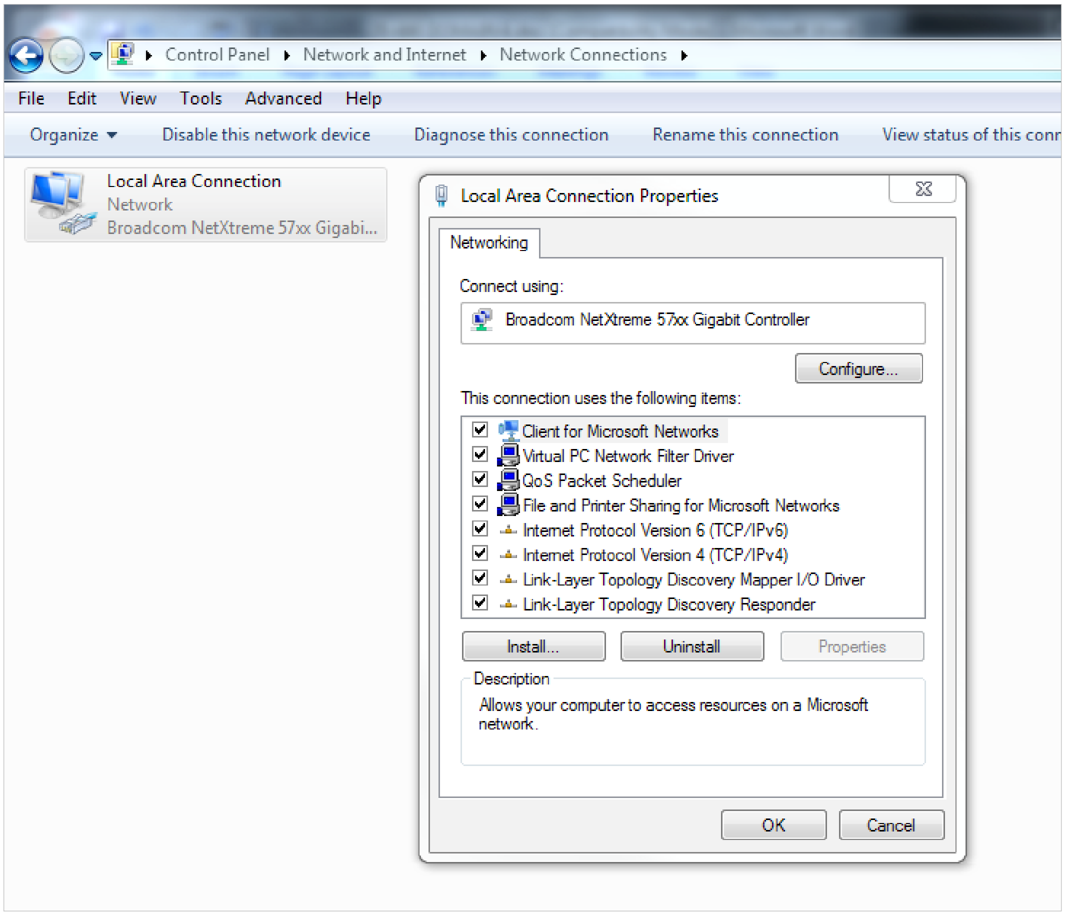
Classless addressing, or **Classless Inter-Domain Routing** (CIDR), allows network administrators to summarize a complicated internal network into a single routing table entry. This is also called "supernetting". CIDR has a special addressing format where the subnet mask is rendered in a number of bits, rather than the dotted decimal notation. So, for instance, the address 192.168.1.1 using the subnet mask 255.255.255.224 would be shown as 192.168.1.0/27.

If a computer needs to communicate with another system on the same subnet, the sending system will reach the target system on its own. If it is outside of the local subnet it will rely on the default gateway and the network node that has that address to forward the packet.

A default gateway is an IP address that is set on a network node. That device forwards network traffic to destination addresses outside of the local subnet. The client system will need to have this default gateway IP address in order to communicate to systems on other remote networks as well as sending network traffic to the internet as applicable.

Connect Systems to the Network

In order to **connect a computer to the network** you'll need to configure the settings for the network adapter you're using. You can find these settings in the **Control Panel** under **Network and Internet** in the **Network Connections** subsection. When you right click the Local Area Connection icon and choose Properties you can see which protocols and services the connection is using.


Control Panel ▸ Network and Internet ▸ Network Connections ▸
File Edit View Tools Advanced Help
Organize ▾ Disable this network device Diagnose this connection Rename this connection View status of this conn
Local Area Connection
Network
Broadcom NetXtreme 57xx Gigabi...
Local Area Connection Properties
Networking
Configure...
Install...
Uninstall
Properties
OK
Cancel

Connect using:

Broadcom NetXtreme 57xx Gigabit Controller

This connection uses the following items:

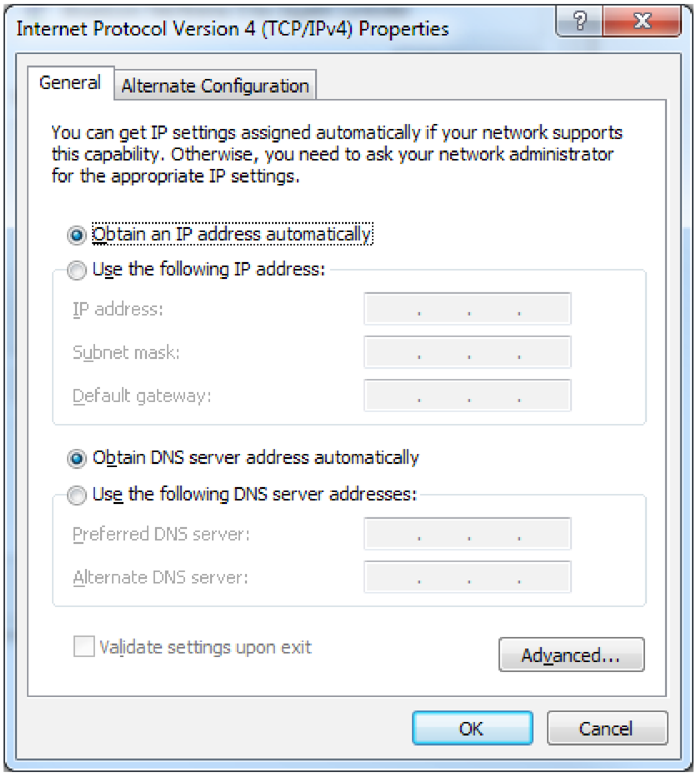
- ☑ Client for Microsoft Networks
- ☑ Virtual PC Network Filter Driver
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

Allows your computer to access resources on a Microsoft network.

Figure 28: Local Area Connection Properties

In order to configure the settings for Internet Protocol Version 4 (TCP/IPv4), highlight it and select **Properties**.



Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

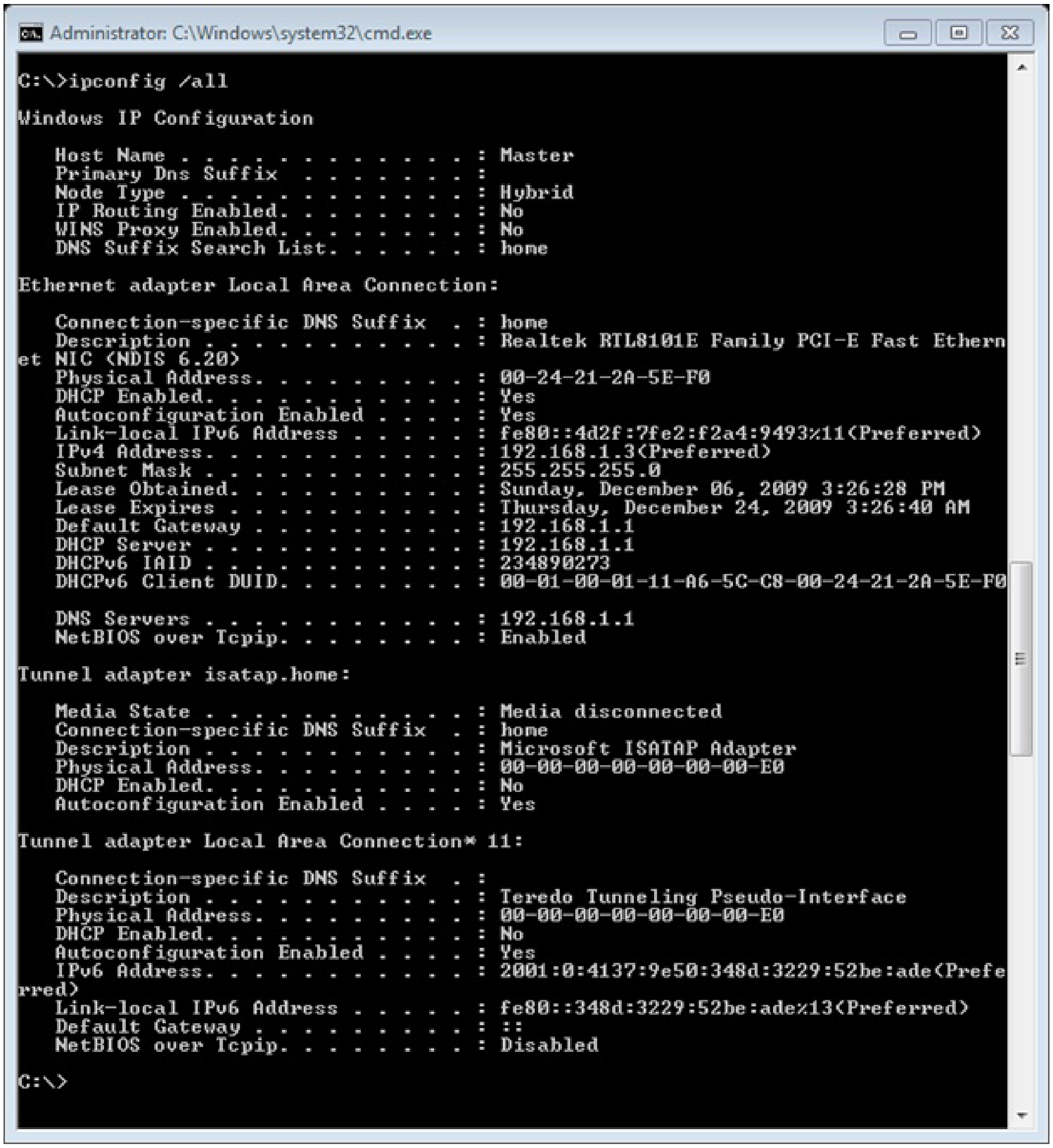
□ Validate settings upon exit

Figure 29: IPv4 Properties

Setting the radio button on **Obtain an IP address automatically** allows the system to use any available Dynamic Host Configuration Protocol (DHCP) server that is supplying dynamic addresses. Usually the DHCP will assign other settings such as DNS and WINS.

If you need to manually set a static IP address for the system you'll need to choose the **Use the following IP address** radio button and manually insert the data. You'll need to do the same to the DNS segment as well. You can select the **Validate settings upon exit** checkbox to make sure you're settings should work correctly.

Additionally, you can use IPCONFIG from the command line to review your settings as shown from the simple output below which resolves the abbreviated information on the adapter for both the IPv4 Address as well as the IPv6 Address information.

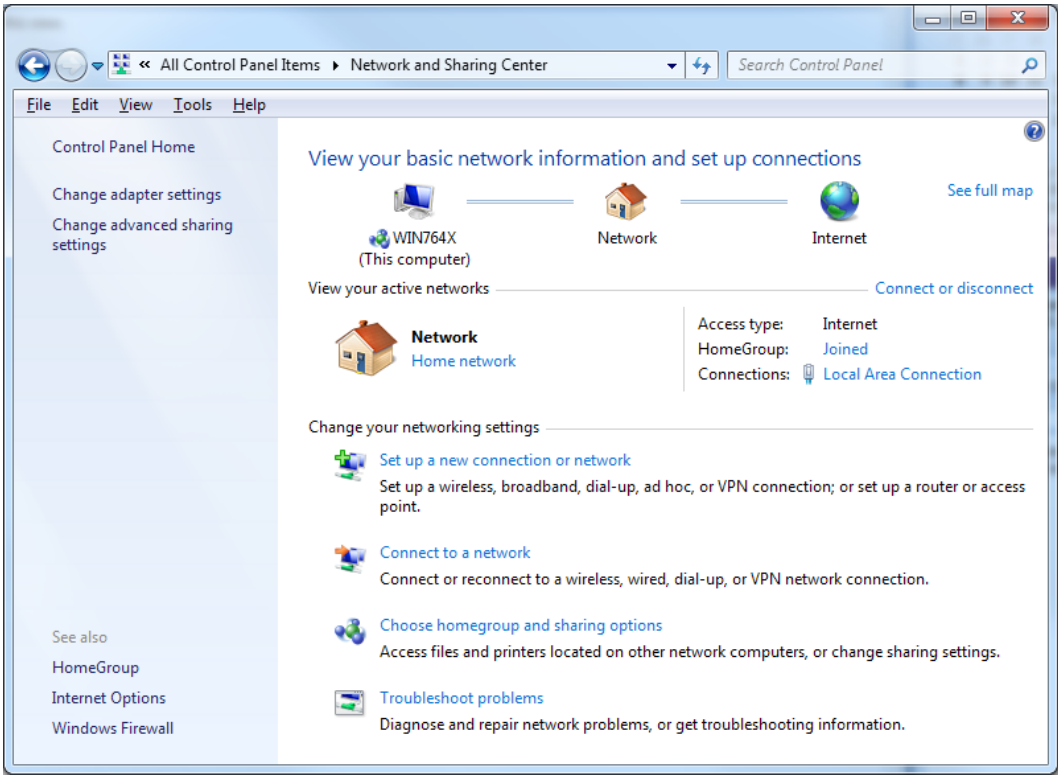


```
C:\>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : Master
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : home

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : home
   Description . . . . . . . . . . . : Realtek RTL8101E Family PCI-E Fast Ethern
et NIC (NDIS 6.20)
   Physical Address. . . . . . . . . : 00-24-21-2A-5E-F0
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::4d2f:7fe2:f2a4:9493%11(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.3(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Sunday, December 06, 2009 3:26:28 PM
   Lease Expires . . . . . . . . . . : Thursday, December 24, 2009 3:26:40 AM
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 234890273
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-11-A6-5C-C8-00-24-21-2A-5E-F0

   DNS Servers . . . . . . . . . . . : 192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Tunnel adapter isatap.home:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : home
   Description . . . . . . . . . . . : Microsoft ISATAP Adapter
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes

Tunnel adapter Local Area Connection* 11:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Teredo Tunneling Pseudo-Interface
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2001:0:4137:9e50:348d:3229:52be:ade(Prefe
rred)
   Link-local IPv6 Address . . . . . : fe80::348d:3229:52be:ade%13(Preferred)
   Default Gateway . . . . . . . . . : ::
   NetBIOS over Tcpip. . . . . . . . : Disabled

C:\>
```

Figure 30: IPConfig /all

Setting up and configuring **Internet Protocol Version 6** (IPv6) network settings is done basically in the same manner: choose the **Properties** option for **IPv6** in **Network Connections**. Similarly, you can either allow a DHCP server to assign the IPv6 address or set one up manually.

If you need to make other settings changes this is done by going into the Control Panel and into the Network and Internet subsection. On this page you can adjust your settings to the default network settings when you select the **View network status and tasks** link.


« All Control Panel Items ▸ Network and Sharing Center
Search Control Panel
File Edit View Tools Help

Control Panel Home

Change adapter settings

Change advanced sharing settings

See also

HomeGroup

Internet Options

Windows Firewall

View your basic network information and set up connections

WIN764X (This computer) — Network — Internet

See full map

View your active networks — Connect or disconnect

Network
Home network

Access type: Internet
HomeGroup: Joined
Connections: Local Area Connection

Change your networking settings

Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

Choose homegroup and sharing options
Access files and printers located on other network computers, or change sharing settings.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

Figure 31: Network and Sharing Center

This page allows you to **view your active networks** and you can change them here as well by selecting the link in the **network** section (in the screen shot above this is "Home network") and then choosing one of the other options.

In order to successfully connect to your intranet network and internet you'll need an understanding of the public IPv4 space assigned by the Internet Assigned Numbers Authority (IANA) where each IP address must be unique and the private ranges that are available to use on a LAN.

Hosts with public IPv4 address that connect directly to the Internet require a public IPv4 address.

When using a proxy device, or other devices like routers that use a Network Address Translation (NAT), it doesn't matter if a public IPv4 address is used or not - generally, a private address will be used.

The Internet Engineering Task Force (IETF) directed the Internet Assigned Numbers Authority (IANA) to reserve the following IPv4 address ranges for private networks, as published in RFC 1918:

RFC1918 name	IP Address Range	Number of Addresses	Classful Description	Largest CIDR Block (subnet mask)	Host ID Size
24-bit block	10.0.0.0 – 10.255.255.255	16,777,216	single class A	10.0.0.0/8 (255.0.0.0)	24 bits
20-bit block	172.16.0.0 – 172.31.255.255	1,048,576	16 contiguous class Bs	172.16.0.0/12 (255.240.0.0)	20 bits
16-bit block	192.168.0.0 – 192.168.255.255	65,536	256 contiguous class Cs	192.168.0.0/16 (255.255.0.0)	16 bits

Figure 32: IPv4 Private Address Ranges

DHCP clients can automatically self-configure an IP address and subnet mask when a DHCP server isn't available by using Automatic Private IP Addressing (APIPA).

When a DHCP client first comes on to the network it attempts to locate a DHCP server in an effort to lease an IP address and any corresponding information (DNS server, WINS server etc).

If the DHCP server fails to respond or is otherwise unavailable the client system will use APIPA to automatically configure itself with an IP address from the reserved APIPA range which is 169.254.0.1 through 169.254.255.254 a default class B subnet mask of 255.255.0.0.

The DHCP client will use the APIPA IP address until a DHCP server becomes available by checking at regular intervals for the presence of a DHCP server. If a DHCP server suddenly becomes available a lease will be obtained, replacing the APIPA address with a dynamically assigned one from the DHCP server's lease pool.

Configure IPv6 Network Settings

IPv6 uses a 128-bit address space as compared to IPv4 which uses a 32-bit space. This will formally resolve the occurring issue of exhausting the address pool under IPv4. Even if you take into consideration that the total number of IPv4 addresses available is 4,294,967,296 (256 x 256 x 256 x 256 or 2^32) and that all of them jumped off of IPv4 and climbed on to IPv6, IPv6 has a total of 3.4x10^38 IP addresses (340 followed by 36 zeros) so it is not likely to be exhausted any time soon. Another way to look at that is if you were to divide the number by the population of the Earth (assuming 6 billion people) that would be 5.666667x10^28 addresses for each person. IPv6 supports DHCPv6 and IPSec, natively.

Native IPSec support means that all hosts encrypt their data transmissions. IPv6 includes a Flow Label in the packet header to provide prioritized delivery support by assigning a priority level to the packet rather than relying on port numbers in use.

Most people are familiar with IPv4 addresses such as 192.168.1.1 which are dotted decimal addresses. Each segment is a 32 bit number which can effectively be from 0 to 255.

IPv6 addresses look like this 2001:0:4137:9e50:3ca3:1b3e:bada:22b2 in which each section consists of a four-digit hexadecimal number where each digit can be from 0 to 9 and from A to F.

Windows 7 uses IPv6 by default and both IPv6 and IPv4 are supported in a dual stack configuration which provides a shared transport and framing layer. This additionally provides shared filtering for firewalls and IPSec security for both IPv6 and IPv4.

IPv6 address types are:

- **Unicast** – one to one communications between systems:
    - **Global Unicast** – routable on the IPv6 portion of the Internet.
    - **Link Local** – used to contact other nodes on the same network; equivalent to Automatic Private IP Addressing (APIPA) IPv4 addresses using the 169.254.0.0/16 prefix.
    - **Unique Local Unicast** – these addresses are comparable to the IPv4 Private IP address ranges; they are not globally routable, and do not provide connectivity with the IPv6 Internet.
- **Multicast** – one-to-many communications between systems using the same multicast address (limited broadcast).
- **Anycast** – network communication used to locate resources; broadcast.

Configure Networking Settings

Adding devices to a network can be as easy as just plugging them into a network cable provided the network has standard settings as opposed to enhanced security.

If the network device is configured to use DHCP and there is a DHCP server available to assign addresses all you need to do to get onto the network is to plug in and allow the network to start up and broadcast to ask for a known DHCP server and once it is located to ask for an IP address lease.

When the address is assigned the system will have the network designation as defined by the subnet mask in use and the host designation. It will also have the supplied default gateway information in order to contact systems outside the local network and receive DNS, WINS and any other settings predefined by an administrator.

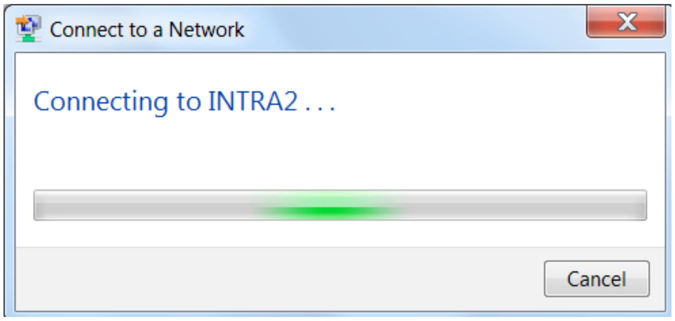
If the system cannot get a DHCP lease it will then configure itself with an APIPA address; this will allow it to connect to some of the resources on the local network. Connecting to a wireless network is a little more involved. Wireless networks operate on radio frequencies as opposed to being connected to Ethernet cabling. The requirements on a system are that there needs to be a wireless adapter on the device and a wireless access point (WAP) within range.

Most modern laptops today have wireless devices built in and they have physical as well as software driven on/off states. When you physically turn the switch on it may interact with the software as well to identify its state.

In a scenario where you are running a notebook computer on batteries and in a power saving mode, it might power off the wireless device if it is detected as not being in use.

When you need to connect a system to a wireless network you would need to turn the hardware switch on for the wireless device in order to allow it to power up. Once it has power, it will seek out any available WAP that is broadcasting its Service Set Identifier (SSID). The purpose of the broadcast is so that wireless clients can find the WAP and connect if they can.

Additionally, if you needed to, you could find the wireless network connection in the Control Panel under the Network and Internet submenu within Network Connections. Then, simply right click the device and choose **CONNECT.**


Connect to a Network

Connecting to INTRA2 . . .

Figure 33: Connecting to a Wireless Network

If there is no wireless encryption setup, then anyone can connect to the WAP, which is discoverable by the SSID broadcast. If the SSID broadcast is turned off, a connecting client would not see it and could not automatically connect to it. A user would then need to know the SSID by name before they could connect. Turning off the SSID broadcast does not prevent users from connecting to the resource; it only prevents automatic connections.

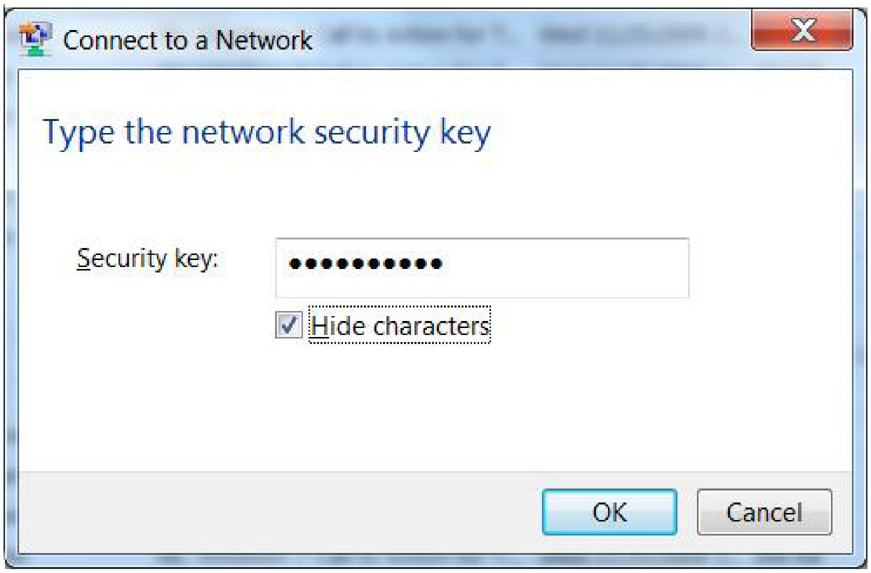
Many WAPs use Wired Equivalent Privacy (WEP) encryption, and usually because they come factory configured with WEP turned on. As it turns out, WEP is not the strongest encryption scheme; it is *easily* cracked.

Wi-Fi Protected Access (WPA and WPA2) security protocols were created to address the inherent weaknesses in WEP.

WPA and WPA2 can be cracked, of course: they are only as strong as their passwords. If administrators use long enough random passwords with numbers, letters and special characters, it makes the pre-shared WPA key virtually uncrackable.

If a WAP that uses WPA broadcasts its SSID, the connecting client will be required to authenticate itself with either a certificate or a password. If this can be done, then access is granted. If a certificate cannot be produced or the password isn't presented, then the client system will not be able to access the network despite being able to "see" the WAP.

You can further enhance the security in this configuration by turning off the SSID. A user connecting wirelessly must to be able to manually enter the nearby SSID name *and* provide a certificate or password to use the WAP.



Connect to a Network

Type the network security key

Security key: ●●●●●●●●●●●

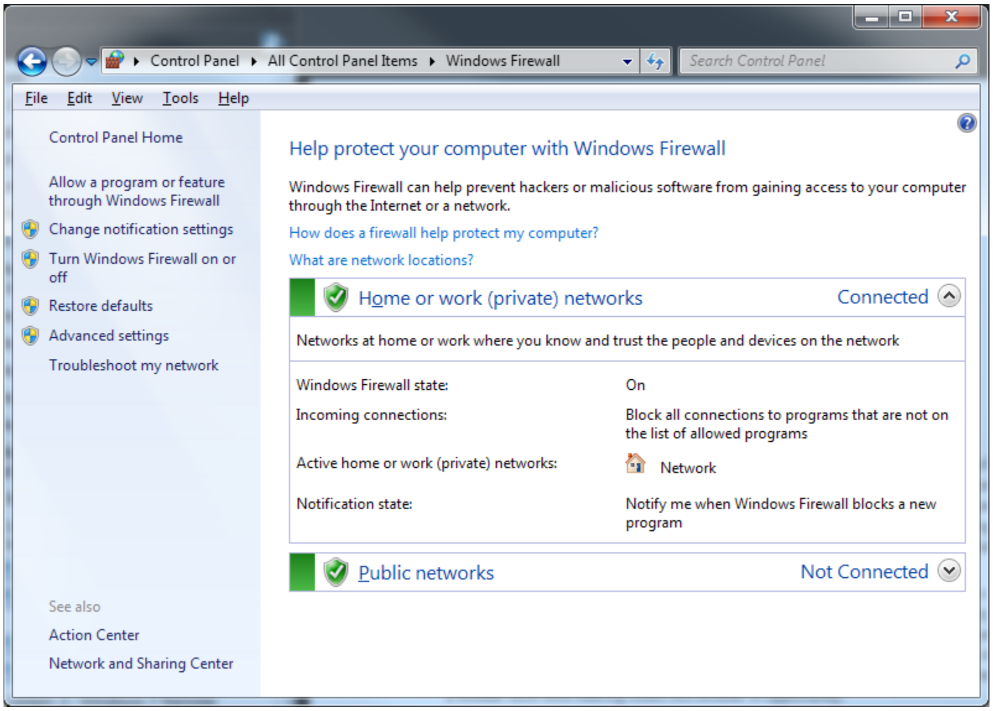
☑ Hide characters

Figure 34: Entering the Security Key for a Wireless Network

You can choose to show the characters as you enter them when using a network security key or hide them by checking the **Hide characters** checkbox.

Configure Windows Firewall

Windows Firewall can be access through the **Control Panel** via the **All Control Panel Items** page. Once you select the applet you have access to the Windows Firewall options in the left side action pane.


Control Panel ▸ All Control Panel Items ▸ Windows Firewall
Search Control Panel
File
Edit
View
Tools
Help
Control Panel Home
Allow a program or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Action Center
Network and Sharing Center

Help protect your computer with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.

How does a firewall help protect my computer?

What are network locations?

Home or work (private) networks — Connected

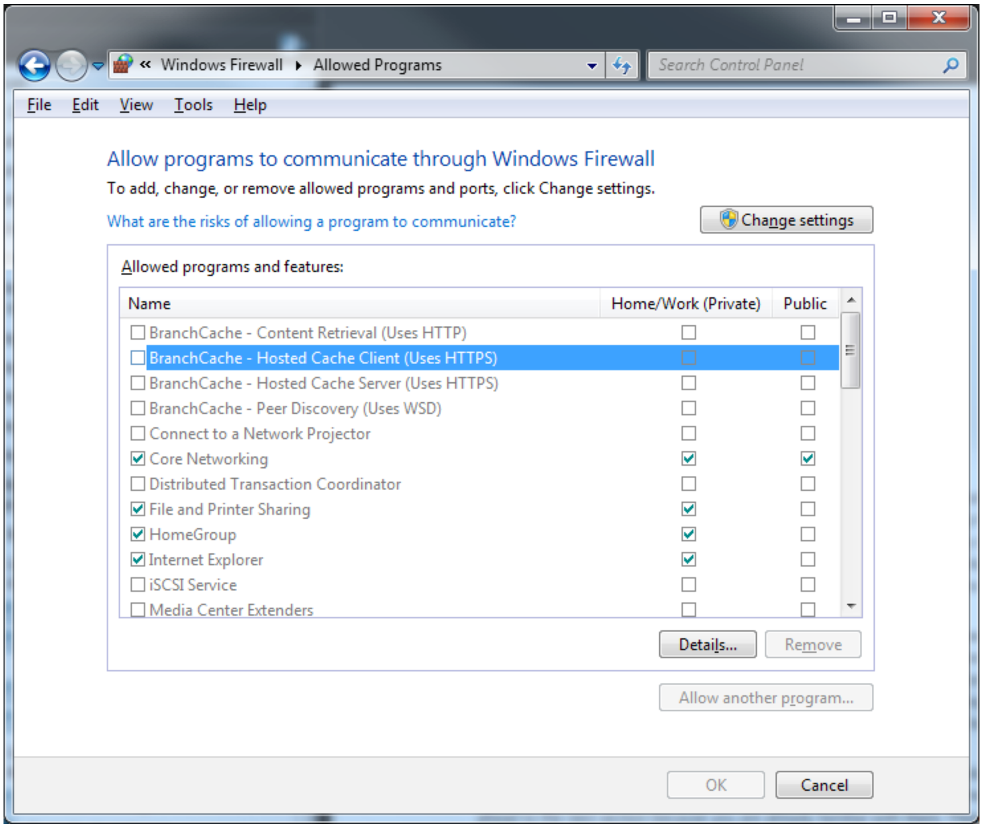
Networks at home or work where you know and trust the people and devices on the network

Windows Firewall state:	On
Incoming connections:	Block all connections to programs that are not on the list of allowed programs
Active home or work (private) networks:	Network
Notification state:	Notify me when Windows Firewall blocks a new program

Public networks — Not Connected

Figure 35: Windows Firewall

If you need to make changes to the settings to open a path for an application you would choose the **Allow a program of feature through Windows Firewall** link. What you see for networks may vary if the system is a domain member.



Allow programs to communicate through Windows Firewall

To add, change, or remove allowed programs and ports, click Change settings.

What are the risks of allowing a program to communicate?

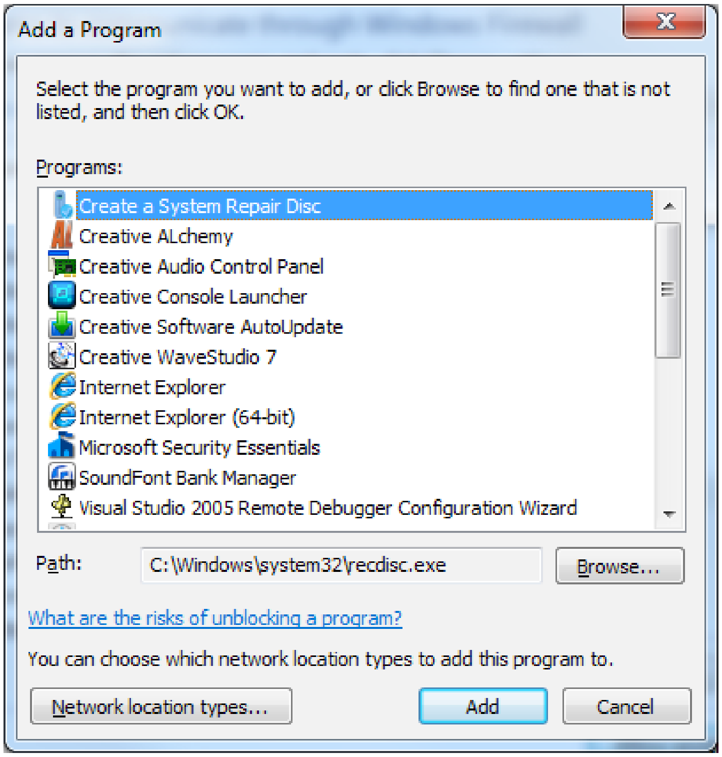
Allowed programs and features:

Name	Home/Work (Private)	Public
□ BranchCache - Content Retrieval (Uses HTTP)	□	□
□ BranchCache - Hosted Cache Client (Uses HTTPS)	□	□
□ BranchCache - Hosted Cache Server (Uses HTTPS)	□	□
□ BranchCache - Peer Discovery (Uses WSD)	□	□
□ Connect to a Network Projector	□	□
☑ Core Networking	☑	☑
□ Distributed Transaction Coordinator	□	□
☑ File and Printer Sharing	☑	□
☑ HomeGroup	☑	□
☑ Internet Explorer	☑	□
□ iSCSI Service	□	□
□ Media Center Extenders	□	□

Figure 36: Allowed Programs

On this page you can choose the Change Settings button in order to elevate your privileges to make the setting changes on either the Home/Work (Private) network or the Public network (or both). This allows you to change the settings of any currently listed program.

If you need to make an exception for another program you would select the **Allow another program** button.



Select the program you want to add, or click Browse to find one that is not listed, and then click OK.

Programs:

- Create a System Repair Disc
- Creative ALchemy
- Creative Audio Control Panel
- Creative Console Launcher
- Creative Software AutoUpdate
- Creative WaveStudio 7
- Internet Explorer
- Internet Explorer (64-bit)
- Microsoft Security Essentials
- SoundFont Bank Manager
- Visual Studio 2005 Remote Debugger Configuration Wizard

Path: C:\Windows\system32\recdisc.exe

What are the risks of unblocking a program?

You can choose which network location types to add this program to.

Figure 37: Adding an Exception

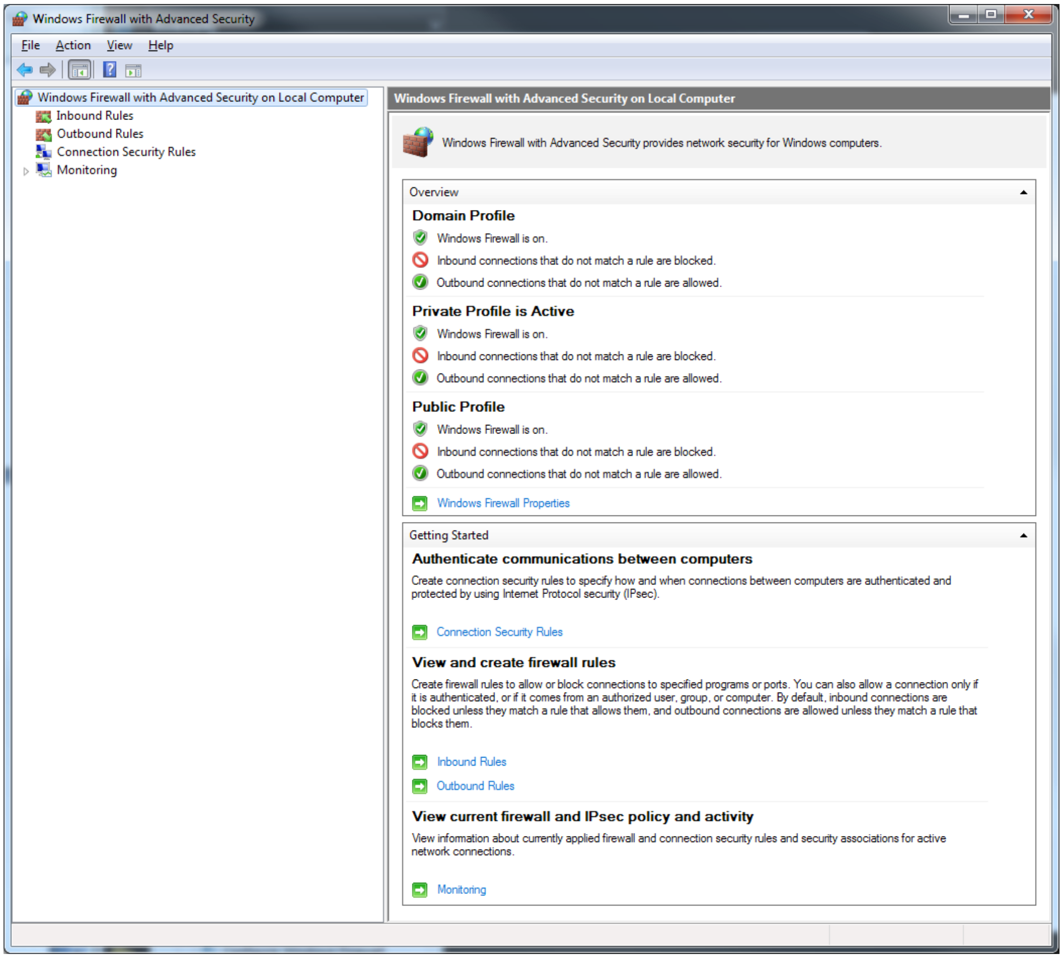
Once you highlight a program you want to configure you would select the **Network location types** button before you click **ADD** in order to choose the desired network.

Once you configure these settings this new application will be permitted to run in pass through fashion at the firewall to communicate as needed on the network or over the internet.

Select the **Change notification settings** option if you needed to turn off the firewall on one of the two networks (or both) as well as make changes to the notifications that you receive. It is not recommended to turn off Windows Firewall unless you are using another software firewall on the local system.

If you make changes to different settings and you are not sure of all of the actions you've taken, you can choose the **Restore default** option which will automatically undo all of the changes to the Windows Firewall and bring it back to its default state.

A more granular approach to Windows Firewall settings can be accessed through the Advanced Security MMC snap-in.


Windows Firewall with Advanced Security
File Action View Help
Windows Firewall with Advanced Security on Local Computer
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring

Windows Firewall with Advanced Security on Local Computer

Windows Firewall with Advanced Security provides network security for Windows computers.

Overview

Domain Profile

- Windows Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Private Profile is Active

- Windows Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Public Profile

- Windows Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Windows Firewall Properties

Getting Started

Authenticate communications between computers

Create connection security rules to specify how and when connections between computers are authenticated and protected by using Internet Protocol security (IPsec).

Connection Security Rules

View and create firewall rules

Create firewall rules to allow or block connections to specified programs or ports. You can also allow a connection only if it is authenticated, or if it comes from an authorized user, group, or computer. By default, inbound connections are blocked unless they match a rule that allows them, and outbound connections are allowed unless they match a rule that blocks them.

Inbound Rules

Outbound Rules

View current firewall and IPsec policy and activity

View information about currently applied firewall and connection security rules and security associations for active network connections.

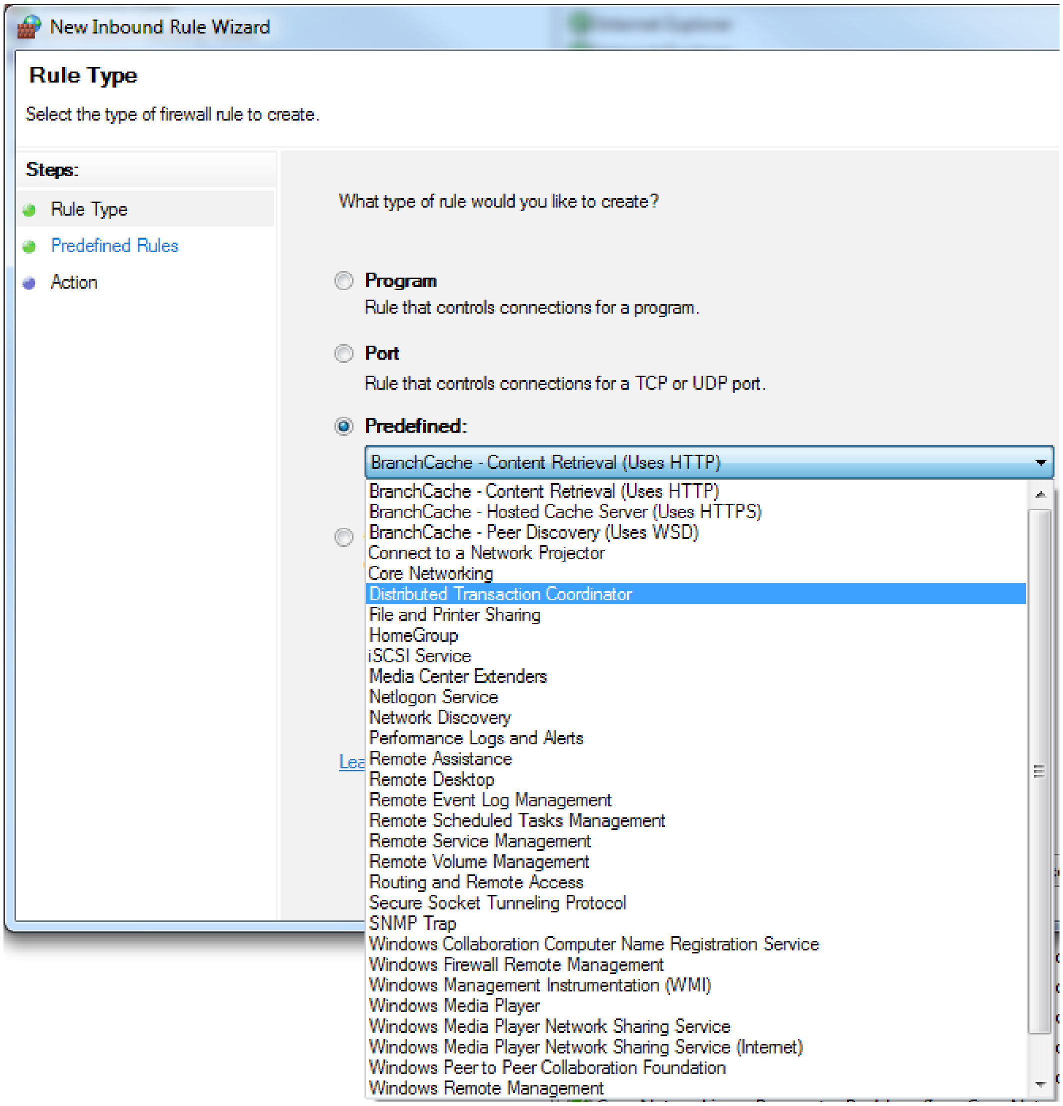
Monitoring

Figure 38: Advanced Firewall Settings

This allows you to review each of the profiles in the overview section as well as choose different options from the Getting Started section. Windows Firewall with Advanced Security allows you to configure inbound and outbound rules. Windows Firewall with Advanced Security also makes available these additional features:

- Set rules that apply for a specific protocol type and port address.
- Set rules that apply for specific traffic that addresses specific services, rather than just specific applications.
- Set limits for the scope of rules to be applied to the traffic source or destination address.
- Set rules that allow traffic only if it is authenticated.
- Set connection security rules.

To create a new Inbound Rule, start the wizard by going to the **Action** menu and choosing **New Rule.** From there, you can create a rule based on a port or a program. You may also choose from a list of Predefined rules that would control connections for a Windows experience.



New Inbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

Steps:

- Rule Type
- Predefined Rules
- Action

What type of rule would you like to create?

○ **Program**
Rule that controls connections for a program.

○ **Port**
Rule that controls connections for a TCP or UDP port.

● **Predefined:**
BranchCache - Content Retrieval (Uses HTTP)

- BranchCache - Content Retrieval (Uses HTTP)
- BranchCache - Hosted Cache Server (Uses HTTPS)
- BranchCache - Peer Discovery (Uses WSD)
- Connect to a Network Projector
- Core Networking
- Distributed Transaction Coordinator
- File and Printer Sharing
- HomeGroup
- iSCSI Service
- Media Center Extenders
- Netlogon Service
- Network Discovery
- Performance Logs and Alerts
- Remote Assistance
- Remote Desktop
- Remote Event Log Management
- Remote Scheduled Tasks Management
- Remote Service Management
- Remote Volume Management
- Routing and Remote Access
- Secure Socket Tunneling Protocol
- SNMP Trap
- Windows Collaboration Computer Name Registration Service
- Windows Firewall Remote Management
- Windows Management Instrumentation (WMI)
- Windows Media Player
- Windows Media Player Network Sharing Service
- Windows Media Player Network Sharing Service (Internet)
- Windows Peer to Peer Collaboration Foundation
- Windows Remote Management

○

Lea

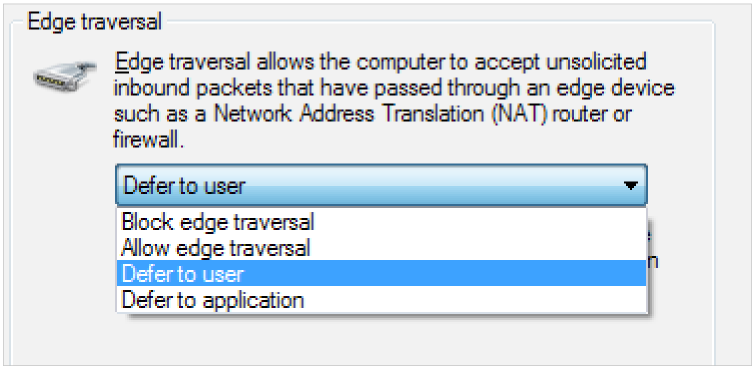
Figure 39: Creating a New Firewall Rule

The various options available to you through the wizard as steps in the left pane of the active window will change based on your rule selection.

- If you are going to create a program rule you would specify a program for which the rule applies.
- If you are going to create a port rule you would specify whether the rule applies to the TCP or the UDP protocol as well as specify the port numbers. You would also need to specify what action the firewall needs to take when it encounters network traffic that matches the rule conditions.
- Allow the connection if the traffic meets the rule conditions for allowing the network traffic.
- Block the connection if the traffic meets the rule conditions for blocking the network traffic.
- Allow the connection if the traffic meets the rule conditions and is authenticated using one of the methods specified in the connection security rules.

Once a rule is set up you can configure additional settings on the property page of the rule itself by right clicking the rule and choosing **Properties** from the context menu.

- On the **General** tab you can see the name and description of the rule as well as if it is enabled and what the action is for the rule.
- On the **Programs and Services** tab you can set the parameters for all programs that meet the specified conditions or a specific program as outlined by its path.
  - In the services section you can specify whether the rule applies to all programs and services, services only or to specific services.
- On the **Computers** tab you can set up authorized computers, which allow connections from only the computers specified.
  - There is a section on this tab to outline exceptions to the rule on a machine by machine basis as well.
- On the **Protocols and Ports** tab you can define the settings as narrow or a wide as you need in order to allow the application to function correctly on the rule.
- On the **Scope** tab you would set up the local and remote IP addresses for the rule; it can be any IP address (all) or it can be set for specific IP addresses as defined.
- On the **Advanced** tab you can set the network profile that this rule applies to as well as the interface type for the network card.
  - There is also a section to configure settings based on traversing firewalls and routers and how to handle the traffic response.



Edge traversal

Edge traversal allows the computer to accept unsolicited inbound packets that have passed through an edge device such as a Network Address Translation (NAT) router or firewall.

Defer to user

Figure 40: Edge Traversal Settings

- The **Users** tab allows you to set authorized users and allow connections as well as set up exception rules for specific users.

Configure Remote Management

Remote Desktop allows administrators and other users with the granted permissions to log on to the Windows 7 system remotely. This remote access to the system from another machine would deliver a desktop session within the Remote Desktop window to the remote system as if the user were sitting locally at the machine. The screen shot below shows the session established from a Windows XP Media Center 2002 Edition system to a Windows 7 Ultimate Edition system:

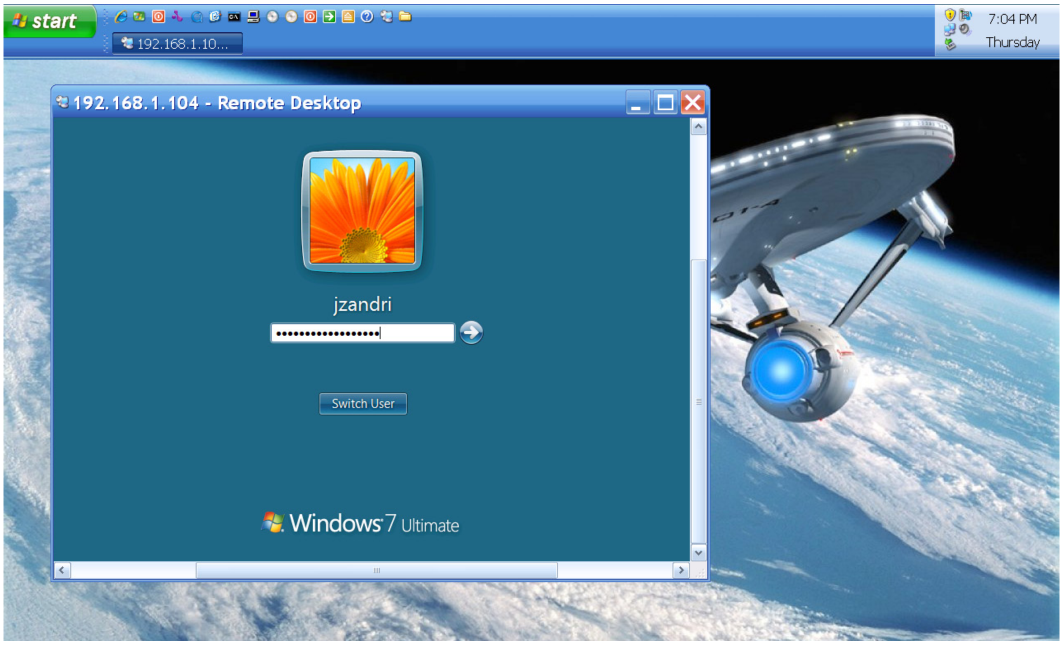


Figure 41: A Remote Desktop Session

Remote Desktop can be set on a machine on the Remote tab of the System Properties page. By default, it is not enabled. Once you do enable it, you are able to assign user rights to remote into the system. Members of the Administrators group have the access rights to do so by default.

When you enable the Remote Desktop option you can choose to allow connections from computers running any version of Remote Desktop or you can choose the more secure option of permitting only those computers running Remote Desktop with Network Level Authentication.

Network Level Authentication is used to enhance Remote Desktop Session Host server security by requiring that the user be authenticated to the Remote Desktop Session Host server before a session is created. This process occurs before a remote desktop connection can be established and before the logon screen appears.

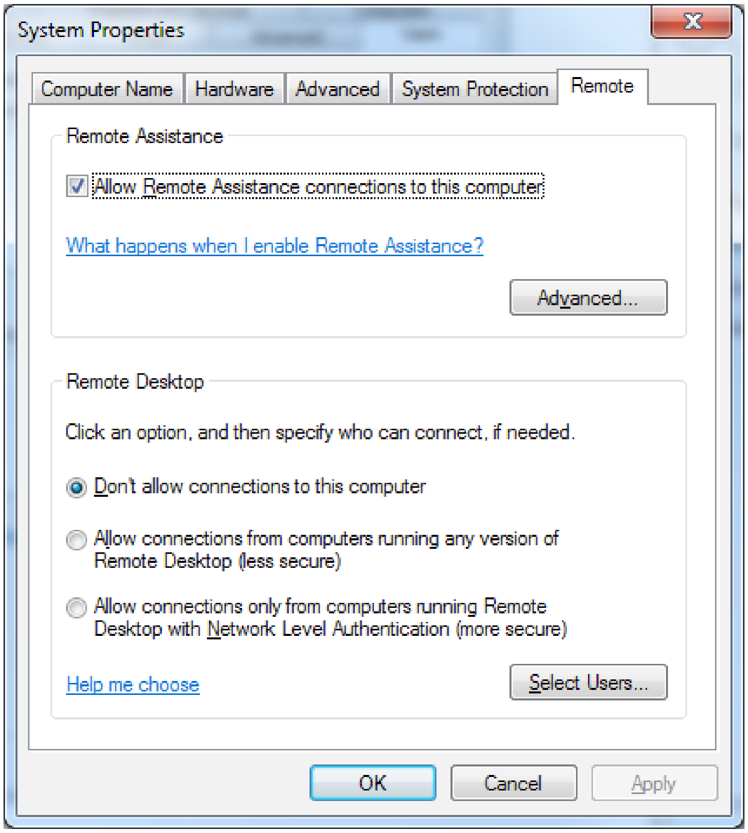
Network Level Authentication:

- Requires fewer remote computer resources initially as the remote computer uses a limited number of resources before authenticating the user.
- Provides better security by reducing the risk of denial-of-service attacks because the target system’s resources are not used until after authentication is successful.

In order to successfully enable this setting and allow all permitted users to connect using Network Level Authentication, the following system requirements must be met:

- The client computer must be using at least Remote Desktop Connection 6.0.
- The client computer must be using a supported version of Windows:
    - Windows 7
    - Windows Vista
    - Windows XP with Service Pack 3, which supports the Credential Security Support Provider (CredSSP) protocol.
- The Remote Desktop Session Host server must be running Windows Server 2008 R2 or Windows Server 2008.

Remote Assistance is a remote support tool which allows a person the ability to view the screen of the person to whom they are providing assistance. Remote Assistance can be used only with the permission of the person that is logged on to the remote computer.



Remote Assistance

☑ Allow Remote Assistance connections to this computer

What happens when I enable Remote Assistance?

Remote Desktop

Click an option, and then specify who can connect, if needed.

● Don't allow connections to this computer

○ Allow connections from computers running any version of Remote Desktop (less secure)

○ Allow connections only from computers running Remote Desktop with Network Level Authentication (more secure)

Help me choose

Figure 42: Enabling Remote Assistance

There have been a number of improvements to Remote Assistance from the earlier Windows XP version:

- Connectivity improvements using Network Address Translation (NAT) traversal using Teredo and IPv6
- Improved user interface
- A stand-alone executable (Msra.exe) that is scriptable and can use command-line options
- Performance improvements including a smaller footprint, quicker startup and connect times
- Enhanced security with mandatory password and integration with User Account Control (UAC)
- Additional Group Policy settings for improved manageability in a domain environment

A few features have been removed:

- The Windows 7 version no longer supports the MAILTO method of solicited Remote Assistance
- Voice sessions through the application are no longer supported
- The file transfer feature that was available in Windows XP and Windows Vista is no longer supported

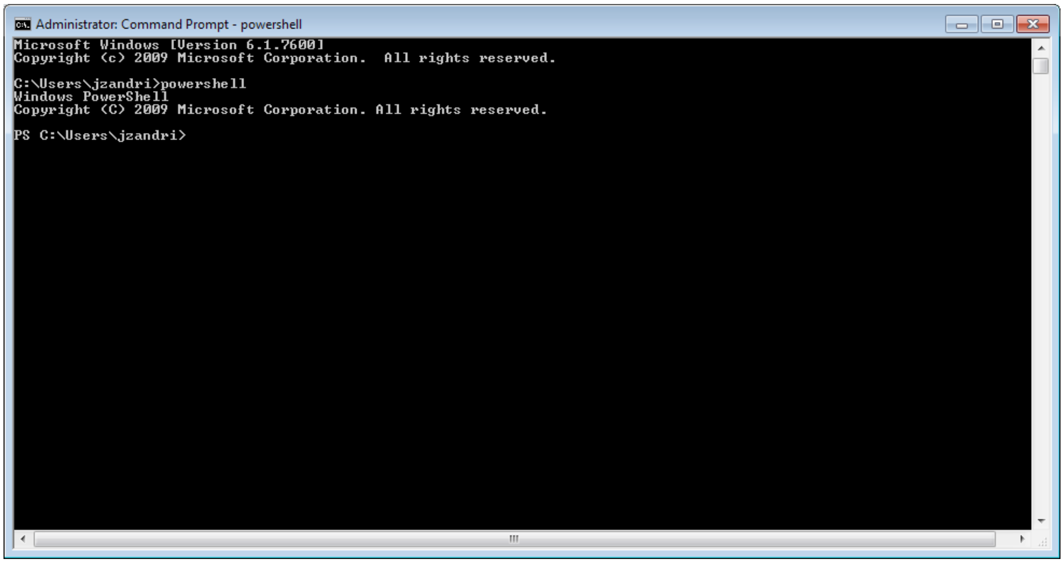
Compatibility with earlier versions is still supported so if a file transfer is initiated from a Windows XP or Windows Vista computer, Windows 7 will accept the transfer.

Remote Assistance has three operational states:

- **Waiting For Connect** – occurs when the person offering the help has offered a Remote Assistance session to the user but they have not yet agreed to allow them to connect the remote system. This state will also occur when the user has sent the an invitation to connect but they have not yet responded by opening the invitation.
- **Screen Sharing** – occurs when the user has agreed to allow the person offering to help the permission to connect to the remote system. In this state the Remote Assistance session is enabled and the person offering the help can view the screen of the user's system only - they do not have the ability to take any type of control of the remote system.
- **Control Sharing** – occurs after the Screen Sharing state when the person offering to help has requested control of the user's system and that user grants the permission to the helper to have shared control of his computer. In this state the person offering the help has the same level of access control to the system that the user has.

Windows PowerShell Remote Management

Windows PowerShell is included with Windows 7 and you can initialize it by running the command from within an open command window. Windows 7 includes version 2 of the management utility, by default. Enter **C:\powershell** in the run window to start PowerShell.



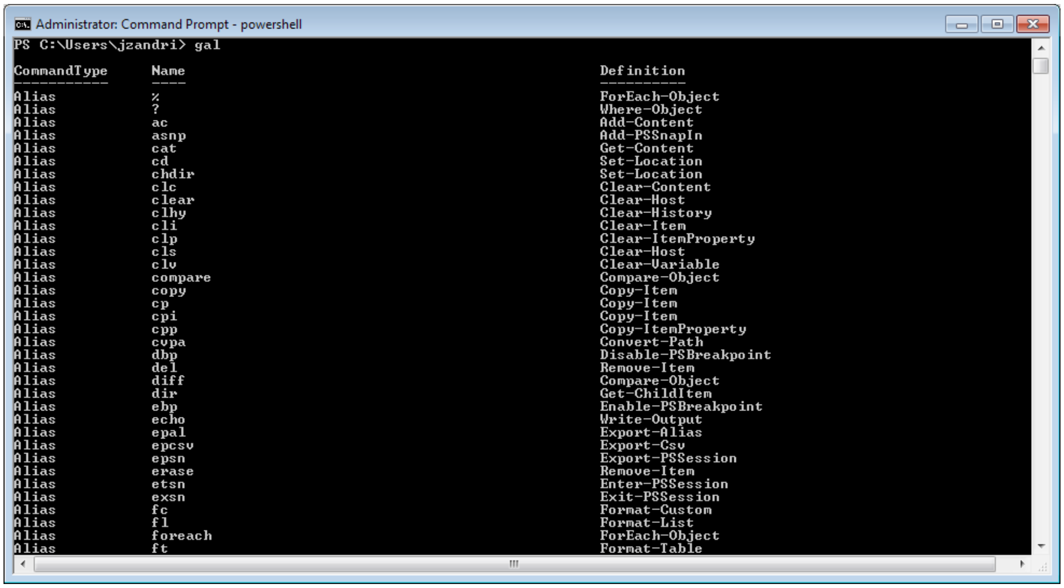
```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\jzandri>powershell
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Users\jzandri>
```

Figure 43: A PowerShell Command Window

Run commands one at a time, just as you would in a normal CLI interface. For a deeper selection of PowerShell commands one PowerShell command, type:

```
C:\Users\jzandri>powershell Get-Help
```

PowerShell also allows you to abbreviate some commands (also called commandlets or **cmdlets**) into aliases. Type **get-alias** or **gal** to return a list of aliases for PowerShell commands.



```
PS C:\Users\jzandri> gal

CommandType     Name                                                Definition
-----------     ----                                                ----------
Alias           %                                                   ForEach-Object
Alias           ?                                                   Where-Object
Alias           ac                                                  Add-Content
Alias           asnp                                                Add-PSSnapIn
Alias           cat                                                 Get-Content
Alias           cd                                                  Set-Location
Alias           chdir                                               Set-Location
Alias           clc                                                 Clear-Content
Alias           clear                                               Clear-Host
Alias           clhy                                                Clear-History
Alias           cli                                                 Clear-Item
Alias           clp                                                 Clear-ItemProperty
Alias           cls                                                 Clear-Host
Alias           clv                                                 Clear-Variable
Alias           compare                                             Compare-Object
Alias           copy                                                Copy-Item
Alias           cp                                                  Copy-Item
Alias           cpi                                                 Copy-Item
Alias           cpp                                                 Copy-ItemProperty
Alias           cvpa                                                Convert-Path
Alias           dbp                                                 Disable-PSBreakpoint
Alias           del                                                 Remove-Item
Alias           diff                                                Compare-Object
Alias           dir                                                 Get-ChildItem
Alias           ebp                                                 Enable-PSBreakpoint
Alias           echo                                                Write-Output
Alias           epal                                                Export-Alias
Alias           epcsv                                               Export-Csv
Alias           epsn                                                Export-PSSession
Alias           erase                                               Remove-Item
Alias           etsn                                                Enter-PSSession
Alias           exsn                                                Exit-PSSession
Alias           fc                                                  Format-Custom
Alias           fl                                                  Format-List
Alias           foreach                                             ForEach-Object
Alias           ft                                                  Format-Table
```

Figure 44: PowerShell CMDlet Aliases

The Windows PowerShell Quick Reference guide to commonly used Windows PowerShell commands can be downloaded from the Microsoft website for review. You can also download the Windows PowerShell Graphical Help File (Version 2.0).

Windows Remote Management Command Line Tool

You can configure your Windows 7 system to be managed remotely by using the Windows Remote Management Command Line Tool. From an elevated command line, type:

```
C:\Users\jzandri>winrm
```

Windows Remote Management (WinRM) is the Microsoft implementation of the WS-Management protocol, which provides a secure way to communicate with local and remote computers using web services.

Usage: winrm operation resource_uri [-*switch:value* [-*switch:value*] ...] [@{*key=value*[;*key=value*]...}]

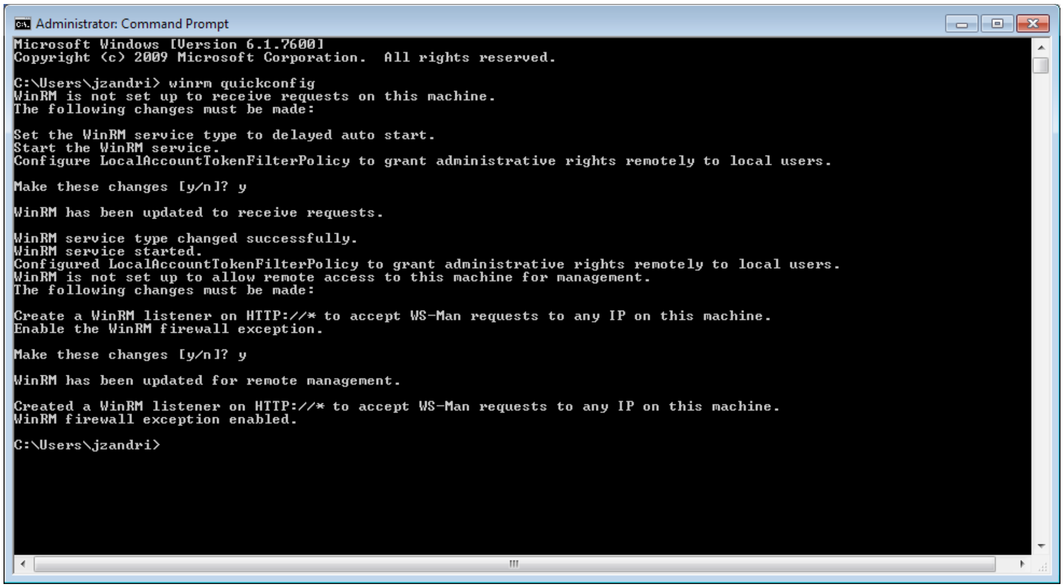
Command	**Description**
winrm g[et]	Retrieving management information.
winrm s[et]	Modifying management information.
winrm c[reate]	Creating new instances of management resources.
winrm d[elete]	Remove an instance of a management resource.
winrm e[numerate]	List all instances of a management resource.
winrm i[nvoke]	Executes a method on a management resource.
winrm id[entify]	Determines if a WS-Management implementation is running on the remote machine.
winrm quickconfig	Configures this machine to accept WS-Management requests from other machines.
winrm configSDDL	Modify an existing security descriptor for a URI.
winrm helpmsg	Displays error message for the error code.

Figure 45: WinRM Commands

You can also call help on specific WinRM topics with **winrm** help *[topic]*.

You need to run **WinRM Quickconfig** from an administrative command prompt on the client you want to manage remotely using either WinRS or Windows PowerShell in order to configure the Windows Remote Management service, set appropriate firewall rules and enable the WinRM listener.

- The first time you run this on your system, you will receive a message that WinRM is not set up to receive requests on your system and you will be prompted to set the WinRM service type to delayed auto start.
- Once you answer the prompt, a message will be displayed that WinRM has been updated to receive requests and that the service type has been changed successfully.
- Once the WinRM service is started, you will also see the message that the system will also configure the LocalAccountTokenFilterPolicy to grant administrative rights remotely to local users.
- An additional message will be displayed indicating that WinRM is not set up to allow remote access to the machine for management and the next prompt will require you to set the WinRM listener on HTTP://* to accept WS-Man requests to any IP on the local system by enabling the WinRM firewall exception.
- Once you answer **Yes** to that prompt, WinRM will be correctly updated for remote management and the WinRM firewall exception will be enabled.



```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\jzandri> winrm quickconfig
WinRM is not set up to receive requests on this machine.
The following changes must be made:

Set the WinRM service type to delayed auto start.
Start the WinRM service.
Configure LocalAccountTokenFilterPolicy to grant administrative rights remotely to local users.

Make these changes [y/n]? y

WinRM has been updated to receive requests.

WinRM service type changed successfully.
WinRM service started.
Configured LocalAccountTokenFilterPolicy to grant administrative rights remotely to local users.
WinRM is not set up to allow remote access to this machine for management.
The following changes must be made:

Create a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine.
Enable the WinRM firewall exception.

Make these changes [y/n]? y

WinRM has been updated for remote management.

Created a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine.
WinRM firewall exception enabled.

C:\Users\jzandri>
```

Figure 46: Configuring WinRM for the First Time

Only Windows PowerShell V2 and later support remote Windows PowerShell.

Domain Five: Configuring Access to Resources

Configure Shared Resources

Configure and Administer Folder Virtualization

There are going to be situations where you will need to allow non-administrators to be able to make low impact configuration changes on the system without changing their access control or permissions on the system. One example is where standard users in Windows 7 have the right to change the time zone on their computers; this is an allowed action that they can perform and it will not fire off User Account Control (UAC).

On Windows XP systems these user accounts do not have this right by default and this has always been an issue for administrators that had to handle road warriors' accounts as they would need to be set as administrators on their systems in order to make these changes.

Windows 7 standard users can now connect to encrypted wireless networks and add VPN connections; a change over how previous operating systems handled the rights requirements for these activities.

While standard users in Windows 7 have the right to change the time zone on their computers they do not have the right to change the system time because many applications and services rely on a precise system clock that needs to be managed automatically. As one example, Kerberos authentication between systems must have time settings synchronized with a common time service within five minutes or authentication fails. Windows operating systems should be set up to automatically update their current time using the domain controller as a network time service.

Any standard user who attempts to change the time will be prompted for administrative credentials.

Certain Windows XP programs will not run without administrative privileges because the application needs to perform file write actions or needs to make changes to file and registry locations that can affect the entire system (for example, in folders like C:\Program Files and C:\Windows or in HKEY_LOCAL_MACHINE in the registry). User accounts that do not have administrative control would lack the necessary privileges to do that and the applications would fail to operate properly.

Registry and file virtualization in Windows 7 allows the operating system to redirect many of these per-machine file and registry write calls to per-user locations where a standard user actually has the permission to write and make changes. This makes it so more legacy applications will function properly as enterprises make the move to shore down the number of administrator level accounts in use and set more of them up with standard user level access.

This is done to allow system administrators to change the habits of needing to make users local administrators of their systems in order for applications to function properly.

Both Windows Vista and Windows 7 includes folder and registry virtualization so that applications that are not UAC compliant can still run correctly without requiring the user to have administrative privileges.

When a non-UAC-compliant application attempts to write to a protected directory that would otherwise require administrative privileges, UAC uses folder virtualization to give the application a virtualized view of the resource it is attempting to change. The virtualized copy of the folder location is maintained under the user's profile and not as part of the actual "physical" file system. This makes it so there is a separate copy of the virtualized file created for each user that runs the non-compliant application.

This same technique would be used if the application needed to write to a protected part of the registry. UAC would use registry virtualization to the same extent and effect.

Configure and Administer Shared Folder Permissions

Permissions are set on local and network resources so that only specific users and security groups have the proper authorization to access and use those resources. They are often set by the resource owner or by anyone with the ability to grant permissions; generally that would be an administrator of some level (local, domain, etc).

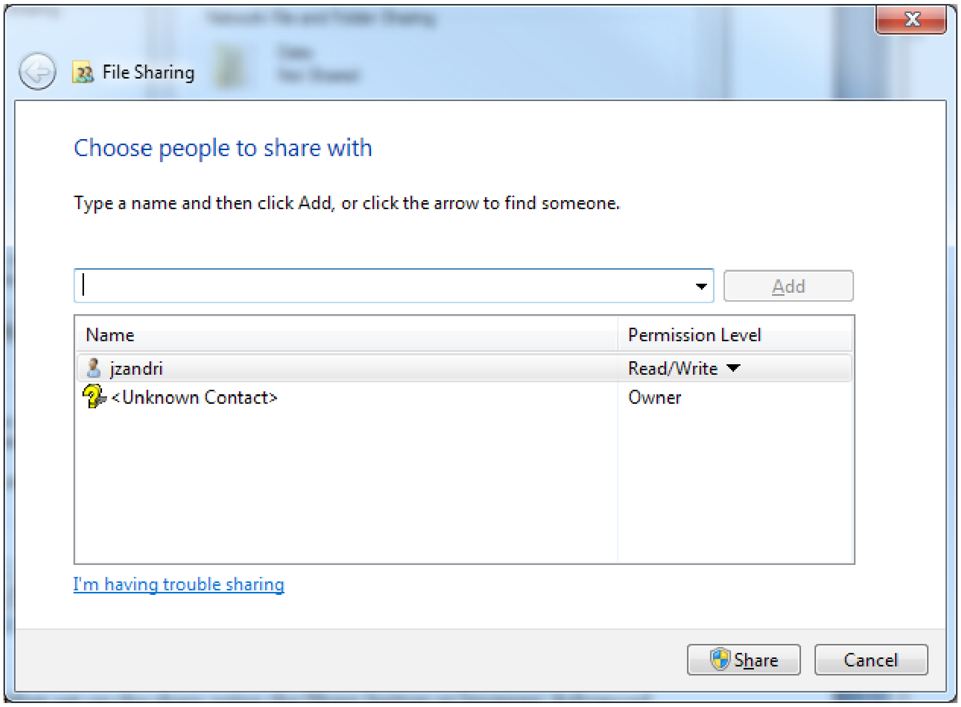
If you are the owner of a resource (e.g. a word document that you created) you are the one that generally grants the users or security groups the appropriate permission to access the resource. Every local or domain resource has access control information, called a security descriptor, associated to it.

The access control information defines the level of access granted to or denied from users and security groups and permissions are defined within an object's security descriptor and allocated to specific users and security groups.

There are two types of permissions that can be set on resources: NTFS file system permissions and Shared folder permissions.

Shared folder permissions will only affect users as they access the resources from a remote system; they have no bearing on a user logged in interactively at the local console. When you need to set up sharing on a folder, right click it and go to the properties page and access the **Sharing** tab.

From this tab you can either set up the share using the Share button or use Advanced Sharing. Advanced Sharing requires an elevated privilege. When using simple file sharing, you'll be presented with a dialog box as shown below:



Choose people to share with

Type a name and then click Add, or click the arrow to find someone.

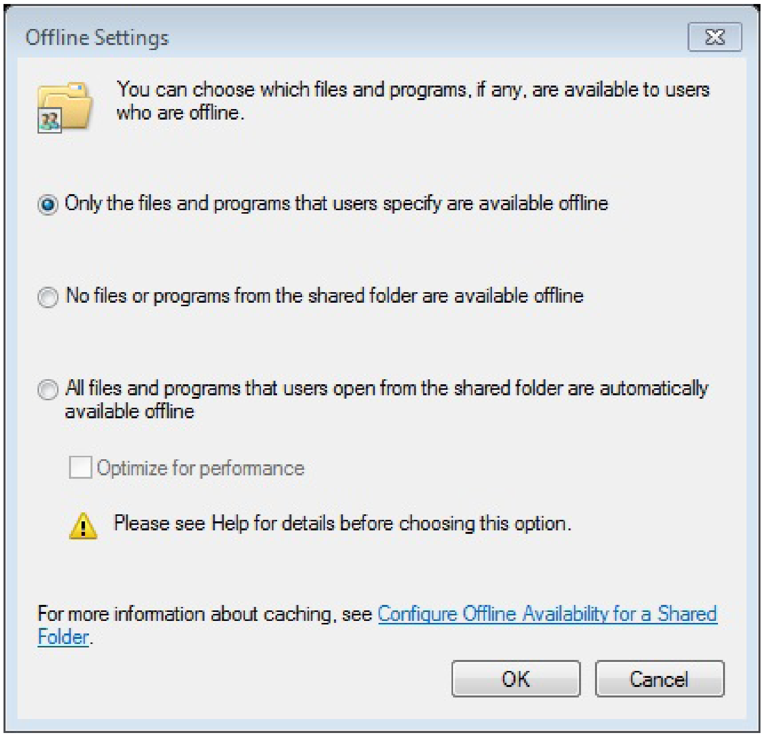
Name	Permission Level
jzandri	Read/Write
<Unknown Contact>	Owner

I'm having trouble sharing

Figure 47: Simple File Sharing

This allows you to set the Permission Level that you want to choose for any user with a profile on the system. You may also add additional users, as well.

Advanced Sharing provides a more granular approach to file sharing. You can change the name of the share, limit the number of users and create very specific permissions per user. Advanced file sharing also provides the ability to adjust how Windows 7 handles caching of shared files offline.



Offline Settings

You can choose which files and programs, if any, are available to users who are offline.

● Only the files and programs that users specify are available offline

○ No files or programs from the shared folder are available offline

○ All files and programs that users open from the shared folder are automatically available offline

□ Optimize for performance

Please see Help for details before choosing this option.

For more information about caching, see Configure Offline Availability for a Shared Folder.

Figure 48: Offline File Settings

You have a few options available to you:

- **Only the files and programs that users specify are available offline** is the default option. No files or programs are available offline, by default, and users will need to decide which files and programs they want to access when they are not connected to the network.
- **No files or programs from the share are available offline** option blocks Offline Files completely.
- **All files and programs that users open from the share are automatically available offline** will automatically cache any file, folder or program in the share so that it may be accessed when the user is offline. Changes are synchronized automatically when the user logs back into the network. Files and programs are held until the cache is full or the user deletes files.
- The **Optimized for performance** check box automatically caches executable files that are run from the shared folder so that the file will be accessed from the local cache instead of the original source location.

You can also make all of these settings from a command prompt. Open an elevated command prompt and enter any of the following commands:

- net share <sharename> /cache:manual
- net share <sharename> /cache:documents
- net share <sharename> /cache:programs
- net share <sharename> /cache:none

You can also use the /cache:BranchCache command line switch when a system is set up with the **BranchCache for network files** role service (this is installed through Server Manager in Windows Server 2008). The setting allows computers in a branch office to cache files downloaded from a shared folder and then securely serve the files to other computers in the branch office.

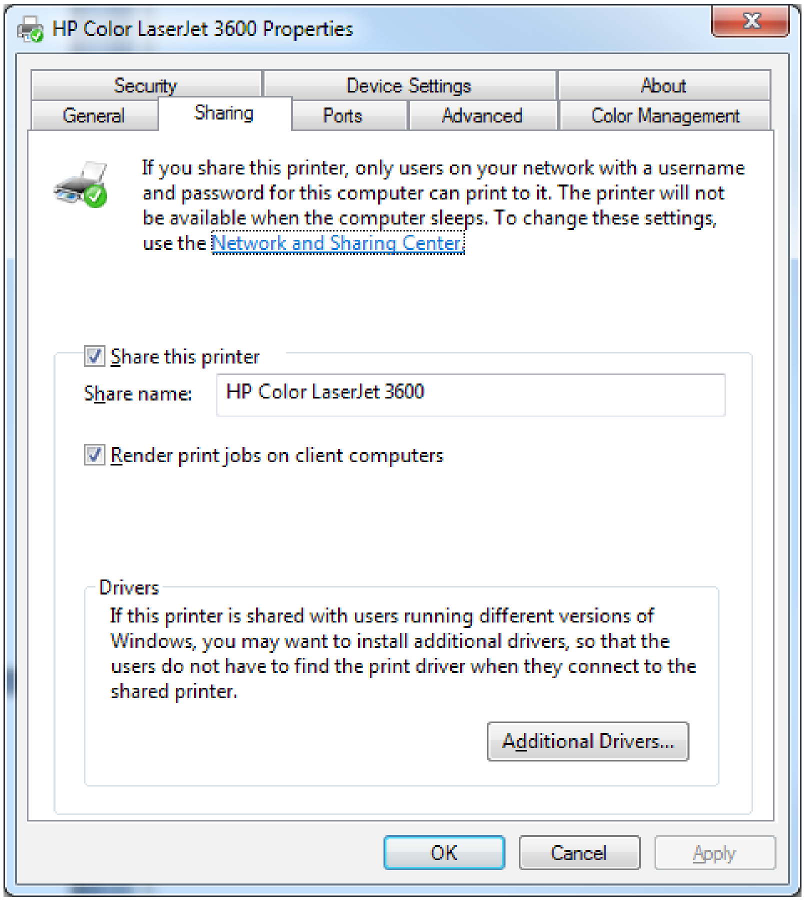
With respect to permissions, you have the option to give users READ access, CHANGE access or FULL CONTROL access to the resources across the share. You can assign the following types of access permissions to shared folders or drives:

- **READ** is the default permission that is assigned to the Everyone group and it allows:
    - Viewing file names and subfolder names
    - Viewing data in files
    - Running program files
- **CHANGE** allows all **READ** permissions, plus:
    - Adding files and subfolders
    - Changing data in files
    - Deleting subfolders and files
- **FULL CONTROL** is the default permission that is assigned to the Administrators group on the local computer. Full Control allows all **READ** and **CHANGE** permissions, plus:
    - Changing permissions (NTFS files and folders only)

Configure and Administer Printers and Queues

Shared printers allow you to offer a singly connected printer over the network to other, authorized computers. You can enable printer sharing in either HomeGroup or Advanced Sharing Settings. Locate the printer within Control Panel\All Control Panel Items\Devices and Printers.

To set up the print device: **Right-click** the printer that you wish to share, and click **Printer Properties** in the context menu. Go to the **Sharing** tab and click the **Share This Printer** checkbox.



If you share this printer, only users on your network with a username and password for this computer can print to it. The printer will not be available when the computer sleeps. To change these settings, use the Network and Sharing Center.

☑ Share this printer

Share name: HP Color LaserJet 3600

☑ Render print jobs on client computers

Drivers

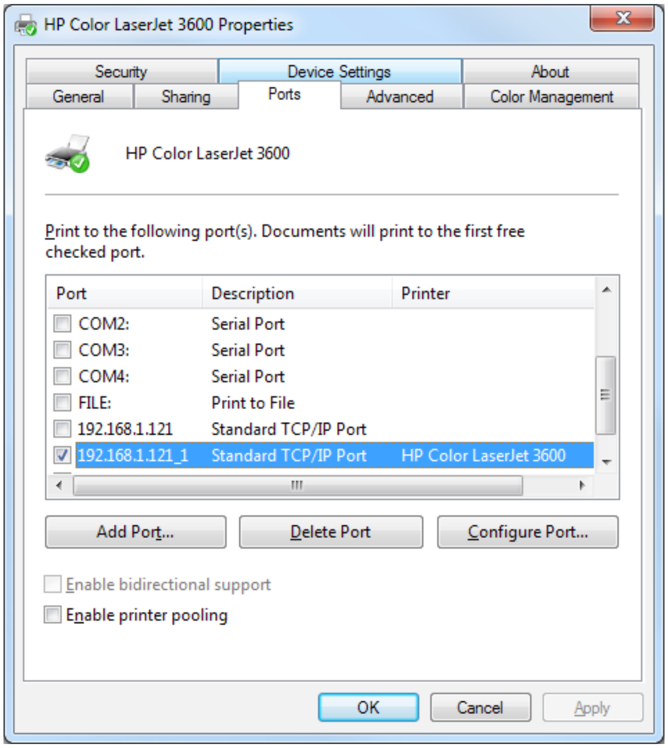
If this printer is shared with users running different versions of Windows, you may want to install additional drivers, so that the users do not have to find the print driver when they connect to the shared printer.

Figure 49: Sharing a Printer

You have the ability to set up additional drivers for network users that are connecting to use the device by choosing the Additional Drivers button.

When you select the Additional Drivers option, other computers on the network that do not have the printer drivers installed for the shared print device are able to download them from the computer that is sharing the printer rather than having to go to the internet to download them.

The **Ports** tab allows you to set up which ports are configured to allow printing. These could include any of the COM ports (serial), LPT printer ports or setting up the device to print to file as well. Additionally, you can set the device up for TCP/IP printing, provided the printer is connected directly to a network. You also have the options available to you to manually add a port, delete a port or configure an existing port.



Print to the following port(s). Documents will print to the first free checked port.

Port	Description	Printer
☐ COM2:	Serial Port	
☐ COM3:	Serial Port	
☐ COM4:	Serial Port	
☐ FILE:	Print to File	
☐ 192.168.1.121	Standard TCP/IP Port	
☑ 192.168.1.121_1	Standard TCP/IP Port	HP Color LaserJet 3600

☐ Enable bidirectional support

☐ Enable printer pooling

Figure 50: Printer Port Settings

On the **Advanced** tab, you are able to set whether the device is always available to be printed to or if it will only be available during a certain range of hours. You can also make configuration settings that include which driver to be used by default as well as to whether to spool print documents or to print directly to the printer. These settings are detailed as follows:

- **Spool print documents so program finishes printing faster** option has two related options that you must choose between.
    - **Start printing after last page is spooled** option sets the print device so that it does not print a document until it is completely spooled.
    - **Start printing immediately** option sets the print device so that it starts printing a document before it is completely spooled which allows the application you are printing from to release control back to you in a shorter period of time.
- **Print directly to the printer** option sets the print device so the document does not spool, which decreases printing time. It is not recommended to use this option on a shared printer.
- **Hold mismatched documents** option sets the print device to hold documents that do not match the configuration of the printer which prevents errors resulting from documents that use paper sizes different from the default loaded paper size.
- **Print spooled documents first** option sets the print device to print out a spooled before a partially spooled document.

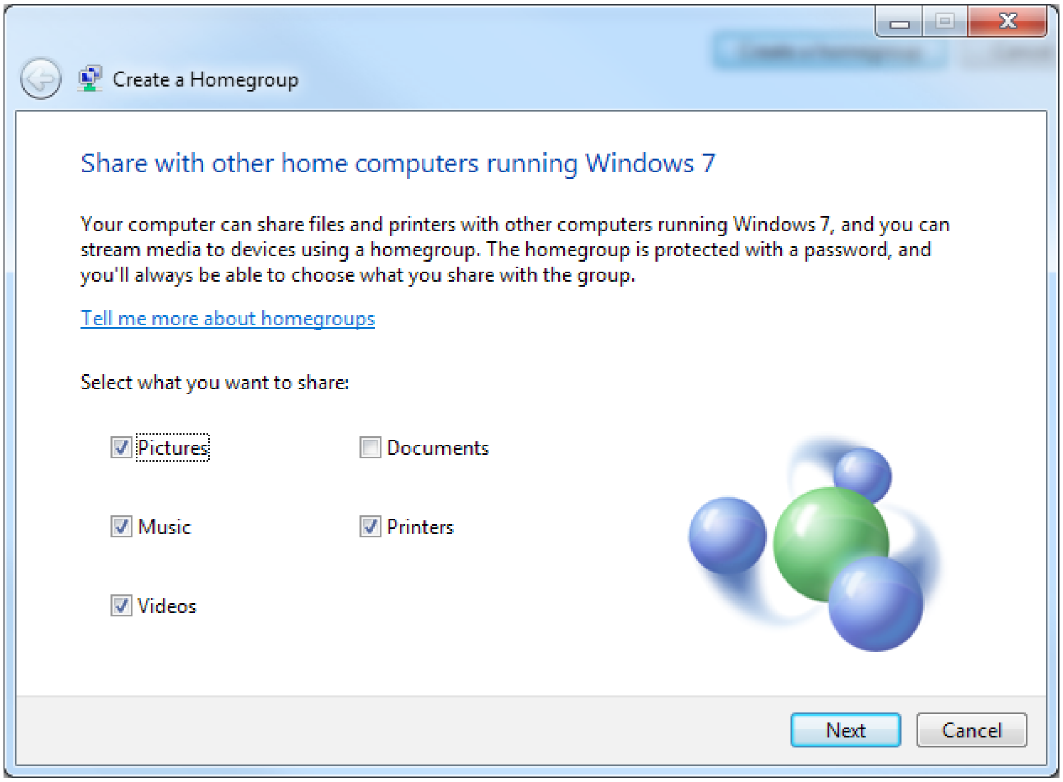
- **Keep documents after they are printed** option sets the print device to retain documents in the print spooler after they are printed which allows them to be quickly resubmitted for printing if needed. In order for this feature to work correctly you must have adequate free disk space available to store all the documents in the spooler.
- **Enable advanced printing features** option should be enabled when documents are rendered using metafile data type (EMF) and other advanced features such as Page Order, Booklet Printing, and Pages Per Sheet.

Configure and Administer HomeGroup Settings

HomeGroup is a network settings configuration wizard for systems on a home network, allowing users to quickly and easily share files and printers and other network attached devices across a password protected setup.

By requiring the use of password, the user making the configuration settings and administrative changes can limit who can gain access to network resources, which systems and devices can gain access to that HomeGroup configuration, and which resources are actually shared on the network.

When you start the Create a HomeGroup Wizard, you are presented with the screen shown below (**Figure 51**). You can make changes to these settings at any time. You'll notice that the Documents setting is not selected by default.



Create a Homegroup

Share with other home computers running Windows 7

Your computer can share files and printers with other computers running Windows 7, and you can stream media to devices using a homegroup. The homegroup is protected with a password, and you'll always be able to choose what you share with the group.

Tell me more about homegroups

Select what you want to share:

☑ Pictures ☐ Documents

☑ Music ☑ Printers

☑ Videos

Figure 51: Creating a HomeGroup

Click **Next** and you'll be given the prompt to write down a randomly generated password, which you'll need to add other computers to the HomeGroup. Other computers may be added by opening the HomeGroup applet in the Control Panel on other PCs and running the wizard, where you'll be prompted for the password.

Systems running Windows 7 Starter and Windows 7 Home Basic can join an existing HomeGroup but one cannot be created from those systems.

If you need to make changes to the advanced settings of the HomeGroup, this can be done by navigating to: **Control Panel** → **All Control Panel Items** → **Network and Sharing Center** → **Advanced sharing settings** on each network discovered on the system.

Configure File and Folder Access

Encrypting Files and Folders Using EFS

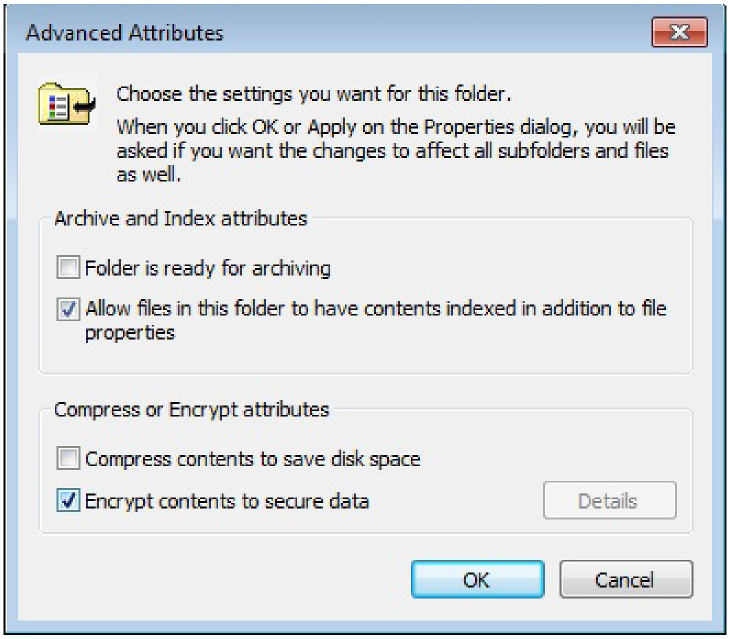
Encrypting File System (EFS) is available on Windows 7 Professional Edition as well as Enterprise and Ultimate editions.

While EFS is not fully supported on Windows 7 Starter, Windows 7 Home Basic, and Windows 7 Home Premium you are able to work with encrypted files, to a certain extent, if you have the encryption key or certificate.

On these systems you can do the following, provided you have either the encryption key or certificate:

- Decrypt files by running Cipher.exe in the Command Prompt window (advanced users)
- Modify an encrypted file
- Copy an encrypted file as decrypted to a hard disk on your computer
- Import EFS certificates and keys
- Back up EFS certificates and keys by running Cipher.exe in the Command Prompt window (advanced users)

Encrypting files and folders on a system is as easy and going to the file or folder, right clicking it and selecting the **Advanced** button on the **General** tab. This will bring up the advanced attributes window, shown below:


Advanced Attributes

Choose the settings you want for this folder.

When you click OK or Apply on the Properties dialog, you will be asked if you want the changes to affect all subfolders and files as well.

Archive and Index attributes

□ Folder is ready for archiving

☑ Allow files in this folder to have contents indexed in addition to file properties

Compress or Encrypt attributes

□ Compress contents to save disk space

☑ Encrypt contents to secure data

Figure 52: Advanced Folder Attributes

EFS under Windows 7 includes the following features:

- Support for Storing Private Keys on Smart Cards
- Encrypting File System Rekeying Wizard
- New Group Policy Settings for EFS
- Encryption of the System Page File
- Per-User Encryption of Offline Files

Smart card key storage support allows for EFS encryption keys and certificates to be stored on smart cards, providing stronger protection for the encryption keys. This is an added level of protection for laptop computers or systems with important data that might be stored in remote locations. Using smart cards to store encryption keys keeps those keys off of the local hard drive of the system which means that they cannot be used by skilled attackers that escalate their privilege level on a system or find a way to physically obtain the box.

The Encrypting File System rekeying wizard allows users the ability to choose which certificate to use for EFS and to select and migrate existing files that will use the newly chosen certificate.

The wizard can also be used to migrate users in existing installations from software certificates to smartcards and administrators or users themselves can use the wizard in recovery situations.

Configure and Administer NTFS Permissions

You can apply NTFS file and folder permissions to individual user accounts or security groups and these access permissions will be relevant regardless of whether someone is accessing the resource remotely or at the local system.

You will only be able to set file and folder permissions on data that is hosted on NTFS volumes; file and folder permissions are not available for data stored on FAT or FAT32 volumes.

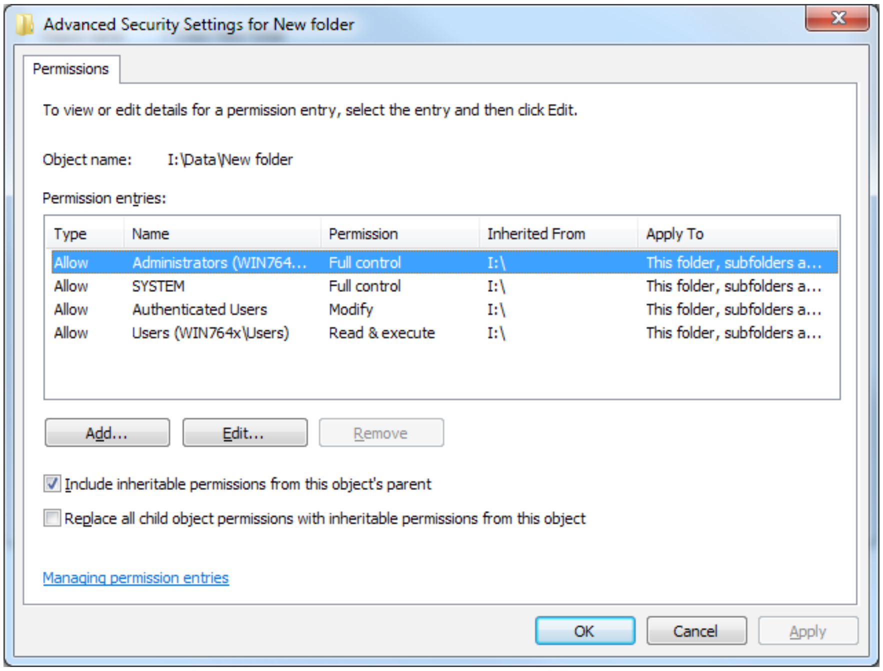
There are six standard permissions that can be assigned to a file or a folder:

- **Full Control –** when this permission is applied to folders it allows for full control of the folder and the contents which includes reading, writing, changing, and deletion of files and subfolders. When this permission is applied to a file it permits the same type of total control over the file as outlined above in the folder description. It permits reading, writing, changing, and deletion of the file as well as modifying the permissions on file.
- **Modify –** when this permission is applied to folders it allows for the reading, writing, changing, and deletion of files and subfolders. When this permission is applied to a file, it permits reading, writing, changing, and deletion of the file. It does not allow the user to modify the permissions on files and folders; if it did that is effectively full control at that point as the user could elevate their rights if they could modify their own permissions.
- **Read & Execute –** when this permission is applied to folders it allows for all of the content of the folder to be read and / or executed as applicable. When this permission is applied to a file it allows the specific file to be read and / or executed. This permission also includes List Folder Contents by default.
- **List Folder Contents –** this permission can only be applied only to folders as it allows the contents of the folder to be viewed.
- **Read –** when this permission is applied to folders it allows the content to be accessed and read. If there is an EXE or DLL or some other file in a fold that needs execute permissions **READ** is not enough permissions; you would need to set **READ & EXECUTE**. When the **READ** permission is applied to a file it allows the contents of the file to be read.
- **Write –** when this permission is applied to folders it allows for the adding of files and subfolders to the parent folder. When this permission is applied to a file it allows for the modification of a file. You do not have the permission to entirely delete the file itself (e.g. right click the file and delete it) but you do have the permission to select all the data inside the file and erase the contents and then resave it as an empty file.

Additionally, there are special NTFS permissions that you can set directly to files and folders if you have a need for this level of granular control to the resources. As files and folders are created they will inherit the permissions that are assigned to the parent folder unless inheritance has been turned off.

Changing those default settings on a file or folder's inherited permissions is done by editing the permissions:

1. Right-click the object you want to edit and click **Properties**.
2. Go to the **Security** tab and select **Advanced**.
3. You'll arrive at the Advance Security Settings for whatever folder you're adjusting.
4. Select the **Change Permissions** button in order to clear the Include inheritable permissions from this object's parent setting.



Advanced Security Settings for New folder

Permissions

To view or edit details for a permission entry, select the entry and then click Edit.

Object name: I:\Data\New folder

Permission entries:

Type	Name	Permission	Inherited From	Apply To
Allow	Administrators (WIN764...	Full control	I:\	This folder, subfolders a...
Allow	SYSTEM	Full control	I:\	This folder, subfolders a...
Allow	Authenticated Users	Modify	I:\	This folder, subfolders a...
Allow	Users (WIN764x\Users)	Read & execute	I:\	This folder, subfolders a...

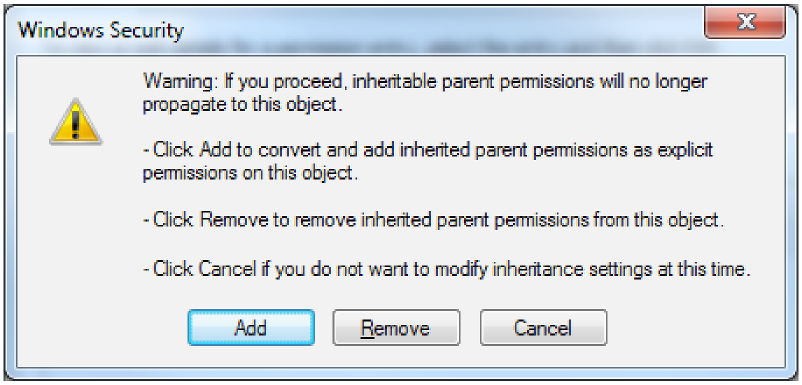
☑ Include inheritable permissions from this object's parent

☐ Replace all child object permissions with inheritable permissions from this object

Managing permission entries

Figure 53: Changing Advanced NTFS Permissions

When you do this the Windows Security dialog box appears letting you know that the action you are taking will remove inheritance of permissions to this folder from the parent folder.



Windows Security

Warning: If you proceed, inheritable parent permissions will no longer propagate to this object.

- Click Add to convert and add inherited parent permissions as explicit permissions on this object.

- Click Remove to remove inherited parent permissions from this object.

- Click Cancel if you do not want to modify inheritance settings at this time.

Figure 54: Security Warning

In order to continue from here you'll need to make one of the choices of adding or removing the permissions or canceling to continue without making any changes.

Troubleshoot and Resolve Effective Permissions Issues

All of the files and folders on your Windows 7 system will contain user and group permissions as set from NTFS. The effective permissions for a user or a security group are determined by combining all of the permissions.

When a user has Read permission and a group the user is a member of is assigned Modify permission and if they are a member of another group that has Full Control, their ultimate effective permission is Full Control. This is always the case with the exception of any Deny permissions as a Deny permission takes precedence and will override any corresponding Allow permissions.

If a user account is in a group that is assigned the Read permission to a folder and that user is also a member of another group that is assigned the Modify permission for the same folder but there is a Deny Read permission set to the user account itself for that folder then the user would be denied Read access.

All of the user's direct explicit settings on their account are calculated into factoring effective permissions as well as their group memberships and any local privileges and permissions they might have as outlined below:

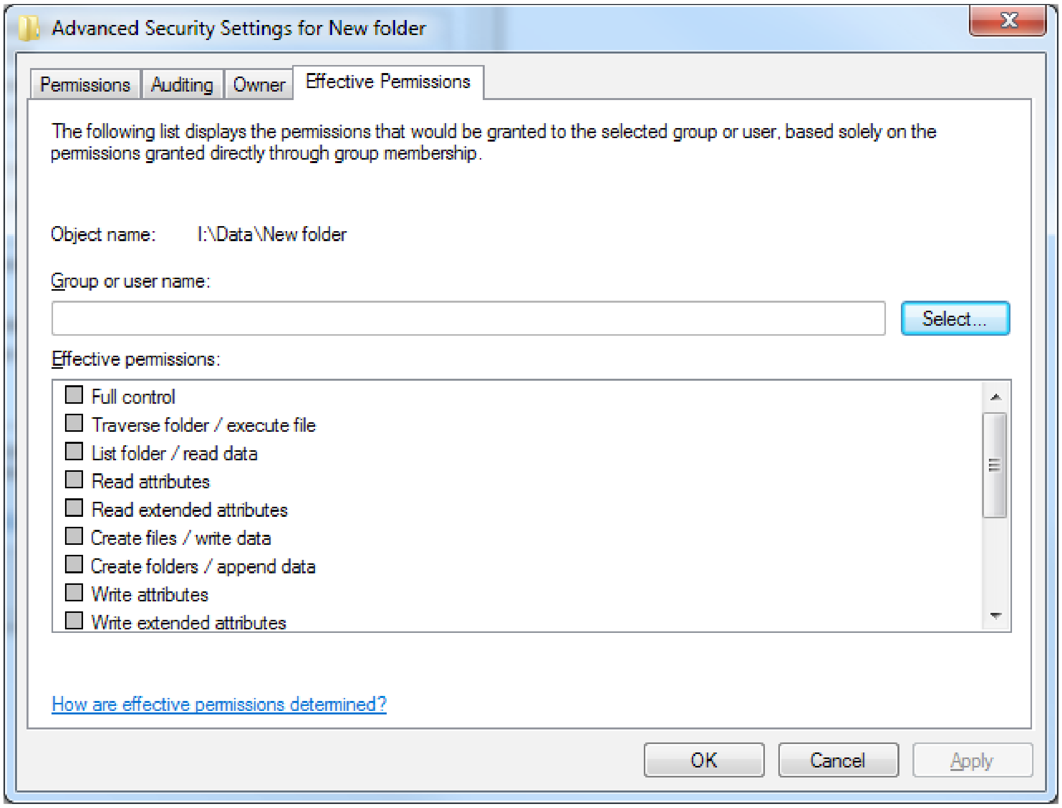
- Universal group membership
- Global group membership
- Local group membership
- Local permissions
- Local privileges

Effective permissions are based on a local evaluation of the user's group membership, user privileges, and permissions. When a given resource is being used, the effective permissions displayed will not include permissions granted or denied to the user through the use of a local group on the remote computer including:

- Local group membership
- Local privileges
- Share permissions

You can use the **Effective Permissions** tab of the object's property page when you're trying to figure out the effective permissions for a user, understanding that the results are an approximation of the permissions that a user has.

The actual permissions a user account may have can be different because permissions can be granted or denied based on how a user logs on such as when they log on locally or when they attempt to use the resources over the wire.



The following list displays the permissions that would be granted to the selected group or user, based solely on the permissions granted directly through group membership.

Object name: I:\Data\New folder

Group or user name:

Effective permissions:

- ☐ Full control
- ☐ Traverse folder / execute file
- ☐ List folder / read data
- ☐ Read attributes
- ☐ Read extended attributes
- ☐ Create files / write data
- ☐ Create folders / append data
- ☐ Write attributes
- ☐ Write extended attributes

How are effective permissions determined?

Figure 55: Effective Permissions

NTFS Permissions: Copying Files vs. Moving Files

Windows 7 regards permission inheritance differently when files are moved or copied on the same volume or across volumes.

Files that are copied or moved to FAT or FAT32 volumes do not retain any of their prior NTFS permissions in the new location. This is because FAT and FAT32 volumes do not have the ability to set any type of permission through the file system to files and folders so any data that is coming from an NTFS volume and going to a FAT or FAT32 volume will be created without any of these settings.

Files that are moved to a folder on the same NTFS volume keep their original NTFS permissions; they will not inherit the permissions of their new parent folder. This is because the files and folders are not physically moved on the disk. Only their reference pointers are changed. There is no actual copy to a new folder and a deletion from the old; this is why you'll notice that you can move many gigabytes of data on the same volume in literally no time.

Files that are copied from one folder to a different folder on the same NTFS volume inherit the NTFS permissions of the destination location/folder. This is because you are creating new files (copies of the old ones) in a new location.

Files that are moved from one location or folder to a folder on a different NTFS volume inherit the NTFS permissions of the destination location or folder. This is because, across volumes, the operating system cannot simply realign NTFS reference pointers. In order to move across partitions you are actually performing a copy action into the new location ahead of a deletion action from the original location. Because this is a create/delete scenario, these are new files being created and they will therefore inherit the permissions of the new parent folder.

If you need to copy files or move them and keep their existing NTFS permissions you can use **robocopy**.

Robocopy.exe is a command-line utility included with Windows 7 that allows you to keep file and folder permissions when copying or moving the data. Robocopy has many command switches that can be used (too many to list here) but, since it is now standard on Windows operating systems, you can type robocopy /? to review the available command line parameters.

In order to keep existing NTFS permissions and other information when copying files across volumes, the command syntax is as follows:

```
robocopy [DRIVE LETTER]:\SOURCE [DRIVE LETTER]:\ DESTINATION /copyall /e
```

The /COPYALL parameter copies the NTFS security information and is equivalent to /COPY:DATSOU, where D=Data, A=Attributes, T=Timestamps, S=Security, O=Owner info, U=Auditing info.

Configure User Account Control (UAC)

User Account Control (UAC) is a security feature of Windows 7 that is designed to inform a user of a need of privilege elevation when a proposed action to be taken on the system cannot be performed within the current privilege level.

Legacy versions of Windows operating system (Windows XP and Server 2003 and earlier) were set up where the administrator account automatically was running at the highest authorization level on the system for all things - from having the ability to install software and drivers and to write to protected areas of the system registry all the way to just reading email and writing a Word doc.

The main issue with this was that this ends up being a security problem because any program run by a user logged on with an administrative account runs with the rights and privileges of that user. So when that user was reading their e-mail message as an administrator and the attachment was malicious and used a known vulnerability that the system was not patched for, the application would run in the context of the logged on user - in this case, administrator.

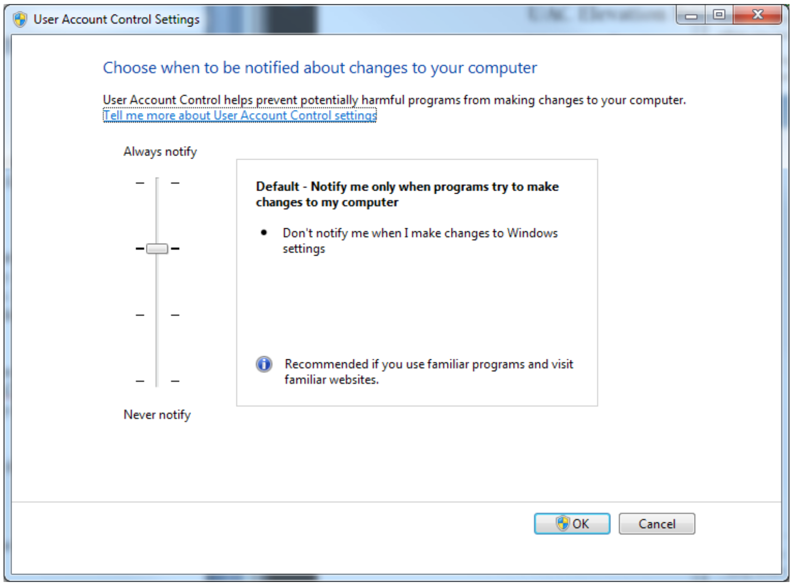
UAC resolves this problem by allowing a user that is a member of the local Administrators group to run as a standard user most of the time and then escalate their privileges for a needed function and that function only in order to so carry out those specific administration-related tasks at the time they are attempting them. Once that one task is complete, that one privilege escalation is dismissed and the remainder of the user session for the admin account is continued as a standard user.

When UAC is enabled and a standard user needs to perform a task that requires administrative permissions (e.g. moving the system time up two minutes), UAC prompts the user for credentials with administrative privileges. If the user has them they can provide them otherwise the task cannot be performed.

The default UAC settings under Windows 7 allow a standard user to perform the following tasks without receiving a UAC prompt:

- Install updates from Windows Update;
- Install drivers from Windows Update or those that are included with the operating system;
- View Windows settings;
- Pair Bluetooth devices with the computer; and
- Reset the network adapter and perform other network diagnostic and repair tasks.

The default UAC setting notifies you when programs try to make changes to your computer, but you can control how often you are notified by UAC by adjusting the settings.



User Account Control Settings

Choose when to be notified about changes to your computer

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

Always notify

Default - Notify me only when programs try to make changes to my computer

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

Recommended if you use familiar programs and visit familiar websites.

Never notify

Figure 56: User Account Control Settings

There are four available settings for UAC:

- **Always notify** – this setting will cause the system to notify you before programs make changes to your computer or to Windows settings that require the permissions of an administrator. When this occurs, your desktop will dim, and you must then either approve or deny the request in the UAC dialog box before you can do anything else on your computer. The dimmed desktop is referred to as the secure desktop mode.
- **Notify me only when programs try to make changes to my computer** – this setting will set up UAC so that it will notify you before programs make changes to your computer that require the permissions of an administrator. Because this setting is a little more permissive than **Always notify** UAC will not notify you if you are making changes to Windows settings that otherwise require the permissions of an administrator. However if a program outside of the Windows operating system tries to make changes to a Windows setting, UAC will send up a notification and place the system into the secure desktop state.

- **Notify me only when programs try to make changes to my computer (do not dim my desktop)** – this setting is essentially the same as the previous one and UAC will send up a notification but it will not place the system into the secure desktop state, making it significantly less secure.
- **Never notify** – this setting shuts UAC off and you will need to restart the computer to complete this action. Once UAC is off, people that log on as administrator will always have the permissions of an administrator at all times and for all sessions and actions. When you are logged in as an administrator you will not be notified before any changes are made to the local system. If you are logged on as an administrator, programs can make changes to the system in the context of the local user which is " administrator" with all rights elevated at all times. If you are logged on as a standard user, any changes that require the permissions of an administrator will automatically be denied and there will be no prompts for elevation to perform any actions as UAC is off.

Configure Authentication and Authorization

In order to configure user rights on a system, it is important to get a complete understanding of what the built-in user groups can do on your Windows 7 system.

- **Administrators** – user accounts that are a part of this group have unrestricted access to the system.
- **Backup Operators** – user accounts that are a part of this group are granted the permission to override file and folder access restrictions for the purpose of backing up data.
- **Cryptographic Operators** – user accounts that are a part of this group are able to perform cryptographic operations when Windows 7 is deployed in 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** – user accounts that are a part of this group are able to manipulate Distributed COM objects on the local system.
- **Event Log Readers** – user accounts that are a part of this group can read data stored in the event logs.
- **Network Configuration Operators** – user accounts that are a part of this group can change TCP/IP address settings on the local system.
- **Performance Log Users** – user accounts that are a part of this group can schedule the logging of performance counters, enable trace providers, and collect event traces.
- **Performance Monitor Users** – user accounts that are a part of this group can access performance counter data on the local system and from remote systems over the wire.
- **Power Users** – this group is included in Windows 7 for backward compatibility and there are no users assigned to the group by default. UAC basically changed the actual need for user account membership for this group.
- **Remote Desktop Users** – user accounts that are a part of this group are able to log on to the system remotely through Remote Desktop.
- **Replicator** – this group is used to support file replication in domain environment.

Authentication Issues

Smart Cards

Smart cards store digital certificates within the card itself and provide an additional security layer to login in to a system and a network over authenticating by just using user names and passwords alone.

While it might be possible for someone to somehow acquire your username and your current password, they still would not be able to log in without also having obtained your smart card and the Personal Identification Number (PIN) that accompanies.

Think of an ATM. If I took your ATM card from you, I would need to have at least that card and your PIN in order to steal money from you. If I was standing in front of the ATM with the card in my possession and the PIN information and the ATM asked me for a user name and a password too, I would not be able to use the card as I probably wouldn't have this information as well. Using smart cards for logging into workstations is similar to this. When more than one set of authentication standards is used, this is called multifactor authentication. Multifactor authentication is stronger than any individual standard alone and makes breaking into a system with this setup highly unlikely.

Multifactor authentication could also be the smart card and PIN along with using a biometric ID, such as a fingerprint (many laptop systems today come with a fingerprint reader embedded into the chassis).

Biometric authentication is generally used on stand-alone systems running Windows 7 - this authentication type cannot be integrated into Active Directory Domain Services (AD DS) without using third-party products at the present time.

There are some group policies contained in the Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options node that you can configure on your Windows 7 system:

- **Interactive Logon: Require Smart Card** – users are forced to log onto the computer using a smart card when this policy is enabled. When the policy is in the default disabled state users can log on using any method.
- **Interactive Logon: Smart Card Removal Behavior** – allows administrators to determine how the system responds when a user removes the smart card from the smart card reader. The default setting is for no action to be taken if a smart card is removed.

Other settings options include:

- **Lock Workstation** - when this setting is enabled the Windows 7 system will respond by locking the screen if the user removes the smart card. The user can only unlock the screen by reinserting the smart card.
- **Force Logoff** - when this setting is enabled the user is forcibly logged off if the user removes the smart card.
- **Disconnect If A Remote Desktop Services Session** - when this setting is enabled it will apply to users connected via Terminal Services sessions hosted on Windows Server 2008 systems and Remote Desktop Services in Windows Server 2008 R2. This policy forces a disconnection from the Remote Desktop Services session when the user removes his smart card.

Configure BranchCache

BranchCache uses peer-to-peer networking to reduce file sharing and HTTP traffic across the WAN. When BranchCache is enabled in your environment, all client systems running Windows 7 will keep a local cached copy of any data that they copy from a file or Web server running Windows Server 2008 R2.

This allows a computer running Windows 7 on the same LAN or branch office that needs the same data to pull it locally from the cache of another Windows 7 machine on the LAN, rather than going over the network for the same information. This reduces bandwidth usage and improves performance. BranchCache supports file sharing using Server Message Block (SMB) and HTTP.

In order to successfully use BranchCache in your environment your systems must be running Windows 7 with the BranchCache feature enabled and the Web / file servers must be running Windows Server 2008 R2 with the BranchCache feature enabled.

For example, let's say you're the first person to arrive in the office and you read an email about a new business strategy that has been posted in a ZIP file to the company's SharePoint site hosted on a Windows Server 2008 R2 system. You decide to download it. If it's 15MB in size, it may take a minute or two for the copy to completely download to your system, depending on the available bandwidth and current usage.

If a co-worker comes in and reads the same email and they take the same actions, then they too will be downloading this same compressed archive over the wire. With Distributed Cache BranchCache enabled, the co-worker's download would be re-directed to come from your cache instead of from the SharePoint site.

While this is can be an advantage, there are two drawbacks:

- You trade improved network bandwidth for decreased performance in each individual machine, especially for the first Windows 7 computer to access a given remote resource.
- Branch Cache only works when a given resource is available on the branch network. If someone with sole access to the resource turns their system off, the next machine needing the data would need to go over the wire as normal; then they would be the Distributed Cache holder for the next person requesting that data.

BranchCache is either set up in a Hosted Cache configuration, which is the preferred configuration with a Windows Server 2008 R2 system deployed to each regional office; or, in the Distributed Cache fashion, as described above.

BranchCache clients can be managed using either Group Policy or the Netsh command-line tool. If you decide to configure BranchCache using Group Policy you can do so by navigating to **Computer Configuration → Policies → Administrative Templates → Network → BranchCache**.

You can define the following settings:

- **Turn On BranchCache** – this setting turns on BranchCache when it is enabled.
- **Set BranchCache Hosted Cache Mode –** this setting turns on Hosted Cache mode when you enable it and you can specify the location of the Hosted Cache server. Each of your branch offices will have different Hosted Caches so you will need to define different GPOs for each of the branch offices.
- **Set BranchCache Distributed Cache Mode** – this setting turns on Distributed Cache mode when it is enabled. You would configure these settings when you choose to use the peer to peer configuration on a local LAN or when Hosted Cache cannot be used due to a lack of an available Windows Server 2008 R2 system in the remote office.

- **Configure BranchCache For Network Files** – this setting changes the default latency required before BranchCache stores a copy of data retrieved from a file server when the setting is enabled. BranchCache will cache data only if latency is greater than 80 milliseconds (ms) by default as data travels on a LAN in less than 20 ms in most cases.
- **Set Percentage Of Disk Space Used For Client Computer Cache** – this setting is used to set the amount of local disk space that Distributed Cache clients will reserve for the BranchCache data store. BranchCache will use 5 percent of the total disk space by default when you enable the setting.

You can use a command line session and the Netsh tool to view or change BranchCache settings. Below is a small list of the more widely used commands:

- **Netsh BranchCache Show Status** – shows BranchCache status (enabled / disabled).
- **Netsh BranchCache Show HostedCache** – displays the location of the Hosted Cache server if Hosted Cache mode is enabled.
- **Netsh BranchCache Show LocalCache –** displays the location and maximum size of the local cache if Distributed Cache mode is enabled.
- **Netsh BranchCache Set Service HostedClient <hosted_cache_server> –** configures a Hosted Cache client and defines the location (using a host name) of the Hosted Cache server.
- **Netsh BranchCache Set Service Distributed** – enables BranchCache in Distributed Cache mode.
- **Netsh BranchCache Set Service Disabled** – disables BranchCache on the client if it was previously enabled.

Domain Six: Configuring Mobile Computing

Configure BitLocker and BitLocker To Go

BitLocker Drive Encryption is available on Enterprise and Ultimate editions of Windows Vista as well as Enterprise and Ultimate editions of Windows 7. Windows Server 2008 also features BitLocker.

BitLocker uses the Trusted Platform Module (TPM) version 1.2 hardware component found in most notebook systems sold today. Desktop motherboard hardware vendors are also providing Trusted Platform Module enabled system boards in order to directly support BitLocker.

BitLocker, under Windows 7, can encrypt operating system drives, fixed data drives, and removable data drives.

Without TPM 1.2 present on a system itself, you can use BitLocker to encrypt the Windows operating system drive by using a USB startup key to boot the computer or to bring a system out of hibernation.

Systems that do not have TPM available cannot use the pre-startup system integrity verification offered by BitLocker with a TPM. When BitLocker is used with data drives, it can handle the following file system types:

- exFAT
- FAT16
- FAT32
- NTFS

When BitLocker is used with operating system drives, the drive must be formatted with the NTFS file system.

BitLocker encrypts entire volumes using the Full Volume Encryption Key (FVEK) and a Volume Master Key (VMK). The FVEK always uses AES encryption to protect the volume.

You can make changes to BitLocker's encryption settings by navigating to:

Computer Configuration → Administrative Templates → Windows Components → BitLocker Drive Encryption → Choose Drive Encryption Method And Cipher Strength Group Policy.

There, you can make changes to the AES encryption strength to a different value than the AES 128 bit with Diffuser default. All the available choices are:

- AES 128 bit with Diffuser (default)
- AES 256 bit with Diffuser (strongest setting; may negatively affect performance)
- AES 128 bit
- AES 256 bit

The system requirements to use Bitlocker include:

- The system integrity check requires TPM 1.2. Otherwise, BitLocker will require you to save a startup key on a removable device such as a USB flash drive.
- Systems with a TPM must also have the Trusted Computing Group compliant BIOS which allows for the required chain of trust for the initialization process before the operating system loads. Systems without a TPM do not require a TCG-compliant BIOS.
- The system BIOS for TPM and non-TPM systems must support the USB mass storage device class, including reading small files on a USB flash drive before an operating system is loaded.
- You need to have a primary partition that is at least 1.5 gigabytes (GBs) in size and it needs to be marked as the active partition. This is used by bootmgr to boot the system. The boot files are also found on this partition as well.
- You'll need at least one other primary partition to be used for the operating system and for data storage.

BitLocker uses TPM to validate the integrity of a system by performing a check of the boot components and boot configuration data to verify that the system is still in the checked state it is expected to be in.

If the data appears to have been altered Bitlocker leaves the system locked before the operating system is loaded to prevent access to the information that is encrypted.

The potential changes that could affect the expected condition of the system might be:

- Unauthorized software (e.g. Trojans, root kits, etc) that have or attempted to change the state of the system.
- Malicious users with physical access to the system that attempt to boot to the system from an alternate operating system with the intention of gaining unauthorized access to the data on the system.

The following are some examples of situations where the user or an administrator would need to recover the system / unlock a hard drive because the security has denied access; these include (but are not limited to):

- Attempting to access a hard drive with BitLocker enabled in a different system.
  - Includes attaching it via external Firewire / USB ports to another system.
- Changing/replacing motherboard with a new TPM.
- Changing the status of the TPM (turning it off, temporarily disabling, and / or clearing the TPM.
- Updating the system BIOS and or any of the other ROM on the motherboard.
- Intentional or unintentional changes to the initialization routine / boot components that cause system integrity validation to fail.
- Entering the wrong PIN information when PIN authentication has been enabled.
- Loss of (or damage to) the USB flash drive that has the information for the startup key when startup key authentication has been enabled.

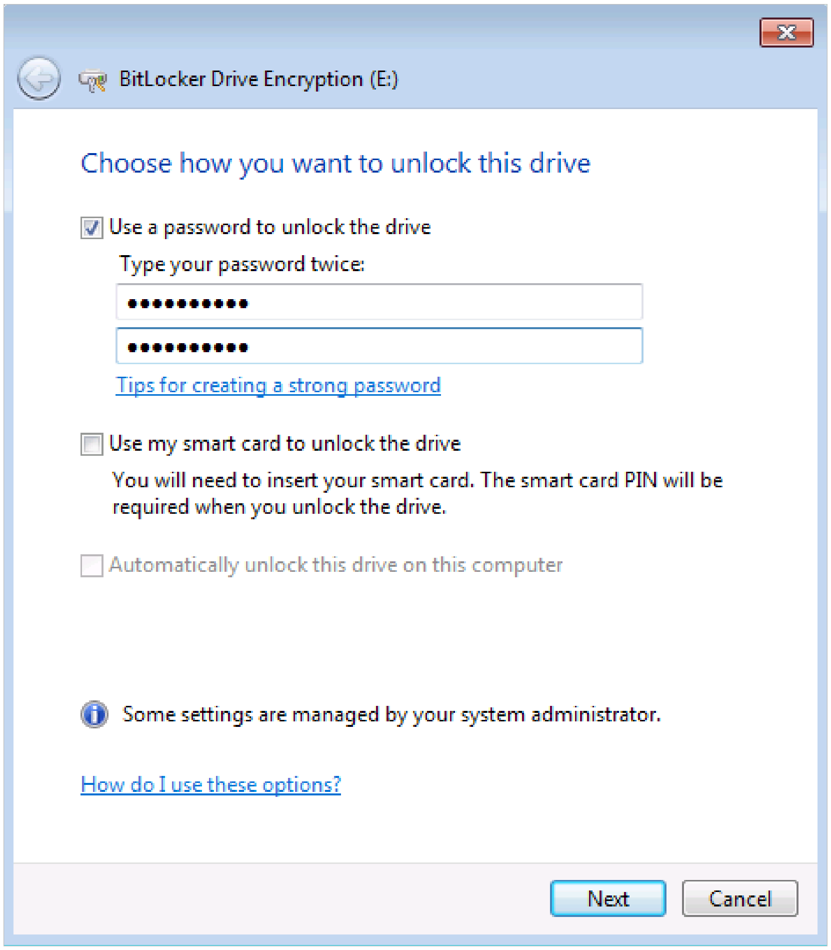
There may be a few scenarios where you might need to temporarily disable Bitlocker Drive Encryption to perform changes or maintenance to a system so the changes would be properly incorporated into the system as part of an authorized change. Temporarily disabling Bitlocker before making these types of changes would keep the system from going into a state at start up that might require it to be recovered.

Some examples of these scenarios where you may need to temporarily disable Bitlocker:

- Updating the BIOS on the motherboard or other ROM that might be present.
  - This includes installing a hardware component that has its own ROM available.
- Making other major system changes on the hardware side (replacing motherboard, adding devices that affect system initialization, etc).
- Making intentional changes to the initialization routine / boot components.
  - Installing a different version of the operating system.
  - Changing the system startup to allow for dual booting.
  - Making desired / required changes to the master boot record (MBR).
  - Changing the disk partitions when these changes affect the partition table.
- Moving a BitLocker-protected drive to another computer.

BitLocker To Go works very much like the base BitLocker that is found on the internal system drives.

Users can choose a method to unlock the drive such as using a Password which is the standard use of letters, symbols, and numbers that can be entered to unlock the drive as needed.



BitLocker Drive Encryption (E:)

Choose how you want to unlock this drive

☑ Use a password to unlock the drive

Type your password twice:

●●●●●●●●●●

●●●●●●●●●●

Tips for creating a strong password

□ Use my smart card to unlock the drive

You will need to insert your smart card. The smart card PIN will be required when you unlock the drive.

□ Automatically unlock this drive on this computer

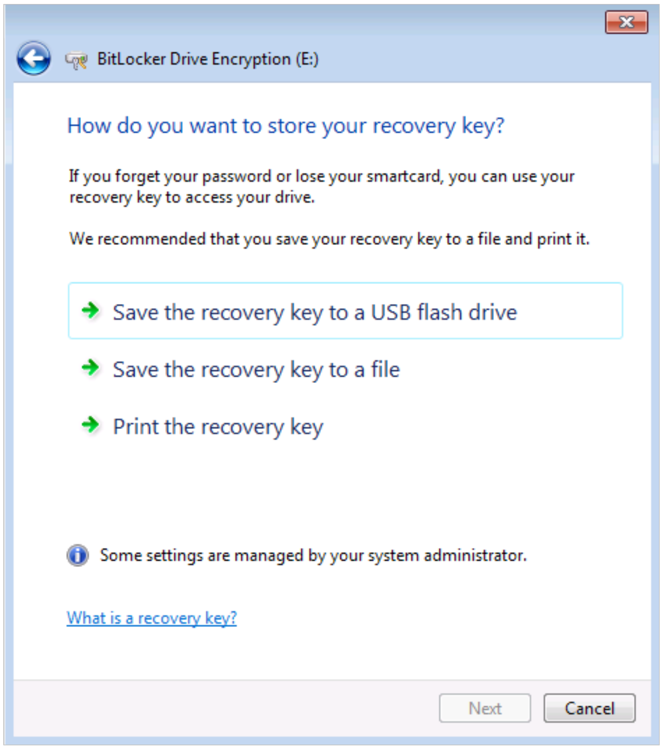
Some settings are managed by your system administrator.

How do I use these options?

Figure 57: Unlocking a Drive with BitLocker

The other method is using a Smart card and a PIN to unlock the drive. Usually Smart cards are used in a corporate environment and are very much like ATM cards. You insert the ATM card, enter the Personal Identification Number (PIN) that you set and you get access to your account. With BitLocker, you insert your Smart card into the reader attached to the system and enter the PIN and this allows you to seamlessly access the BitLocker encrypted data.

Once you choose one of the methods to unlock your protected drives you will be asked to print or save the recovery password which is a 48-digit password and used if other unlock methods fail (e.g. forgotten password).


BitLocker Drive Encryption (E:)

How do you want to store your recovery key?

If you forget your password or lose your smartcard, you can use your recovery key to access your drive.

We recommended that you save your recovery key to a file and print it.

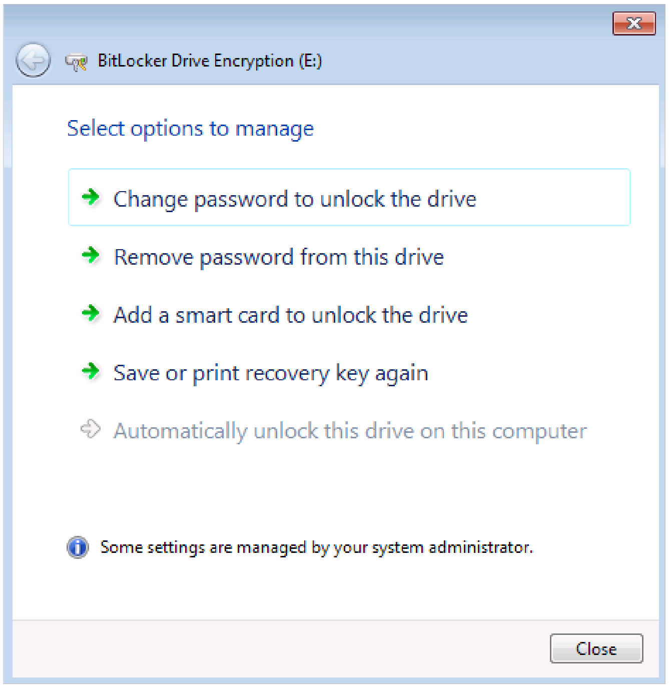
Save the recovery key to a USB flash drive
Save the recovery key to a file
Print the recovery key

Some settings are managed by your system administrator.

What is a recovery key?
Next
Cancel

Figure 58: Storing a Recovery Key

You can manage the BitLocker Drive encryption settings by navigating to **Control Panel** → **All Control Panel Items** → **BitLocker Drive Encryption**. You can manage all the settings for your BitLocker drives, including the ones secured using BitLocker To Go.


BitLocker Drive Encryption (E:)

Select options to manage

Change password to unlock the drive
Remove password from this drive
Add a smart card to unlock the drive
Save or print recovery key again
Automatically unlock this drive on this computer

Some settings are managed by your system administrator.

Figure 59: Managing BitLocker Drive Encryption

The steps to unlock and use a removable drive when you encrypt one with BitLocker To Go are actually pretty simple and transparent.

1. When the drive is inserted and detected, Windows 7 will prompt the user to enter the correct password to unlock the drive.
2. Once this is successfully done, the drive will be unlocked for use for the entire session. If the user removes the drive it will be locked again and in order to use it they would need to supply the password again.
3. Once a drive is unlocked, having access to it is as seamless as any other Windows Explorer or command line activity that is taken on non-encrypted drives.
4. Group Policy settings can be configured for BitLocker To Go. Navigate to:

   Computer Configuration → Policies → Administrative Templates → Windows Components → BitLocker Drive Encryption → Removable Data Drives.

The policies that you can configure are:

- **Control Use Of Bitlocker On Removable Drives** – when enabled, this setting is used to control whether or not BitLocker To Go can be used and how (e.g. block users from suspending encryption, decrypting BitLocker To Go drives).

- **Configure Use Of Smart Cards On Removable Data Drives** – when in use, you can require the use of a smart card to protect a drive with BitLocker To Go. There is also a setting that prevents users from using smart cards.

- **Deny Write Access To Removable Drives Not Protected By BitLocker** – when this policy is enabled you are requiring that BitLocker To Go encryption is on a removable drive before allowing users to save files to it.

- **Allow Access To Bitlocker-Protected Removable Data Drives From Earlier Versions Of Windows** – this policy is used to control whether the BitLocker To Go Reader is installed on BitLocker To Go protected drives for use on legacy versions of Windows operating system.

- **Configure Use Of Passwords For Removable Data Drives** – this is used to require passwords for BitLocker To Go encrypted drives. It also is used to enable password complexity requirements.

- **Choose How Bitlocker-Protected Removable Drives Can Be Recovered** – this policy sets recovery agents (as applicable) and is also used to determine whether recovery agents, 48-digit recovery passwords, or 256-bit recovery keys can be used to recover a BitLocker-protected drive. This policy setting is also used to save BitLocker To Go recovery information to Active Directory Domain Services (AD DS) when the client system is a member of a domain.

Using Data Recovery Agents with BitLocker

Data Recovery Agents are special accounts that are configured to recover data from BitLocker-protected drives when other methods of retrieval fail. This is done by using smart card certificates and public key information.

As the system or enterprise administrator for your environment, you will need to 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 and this is done as follows:

1. Either run the GPMC or the Local Group Policy Editor.
2. Navigate to the console tree under **Computer Configuration\Windows Settings\Security Settings\Public Key Policies.**
3. Right-click BitLocker Drive Encryption.
4. Select **Add Data Recovery Agent** to start the Add Recovery Agent Wizard and chose **Next** to continue.
5. On the **Select Recovery Agents** page, browse to the certificate file that will be used for the data recovery agent.
6. Select the .CER file, importing it.
7. Review the information in the Recovery agents list.
8. As needed, you can configure multiple data recovery agents. If you are done, choose **Next** to continue.
9. The last screen is the **Completing the Add Recovery Agent** page of the wizard which will show the summary information of the data recovery agents that will be added.

There are four categories of Group Policy settings available for BitLocker Drive Encryption:

- Global settings that affect all BitLocker-protected drives
- Operating system drive settings
- Fixed data drive settings
- Removable data drive settings

BitLocker Group Policy settings available in the Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption container are outlined in some detail below and review some of the Group Policy settings that can be used to control BitLocker.

With the **All Drives (GLOBAL setting)** you can configure the following settings;

- Choose default folder for recovery password
- Choose drive encryption method and cipher strength
- Choose how users can recover BitLocker-protected drives
- Prevent memory overwrite on restart
- Provide the unique identifiers for your organization
- Store BitLocker recovery information in Active Directory Domain Services
- Validate smart card certificate usage rule compliance

With the **Operating system drive** settings you can:

- Allow enhanced PINs for startup
- Choose how BitLocker-protected operating system drives can be recovered
- Configure minimum PIN length for startup
- Configure TPM platform validation profile
- Require additional authentication at startup
- Require additional authentication at startup

With the **Fixed data drive** settings you can:

- Allow access to BitLocker-protected fixed data drives on earlier versions of Windows
- Choose how BitLocker-protected fixed drives can be recovered
- Configure use of passwords for fixed data drives
- Configure use of smart cards on fixed data drives
- Deny write access to fixed data drives not protected by BitLocker

With the **Removable data drive** settings you can:

- Allow access to BitLocker-protected removable data drives on earlier versions of Windows
- Choose how BitLocker-protected removable drives can be recovered
- Configure use of passwords for removable data drives
- Configure use of smart cards on removable data drives
- Control use of BitLocker on removable drives
- Deny write access to removable data drives not protected by BitLocker

Configure DirectAccess

DirectAccess is new to the Windows operating system in Windows 7 and Windows Server 2008 R2 and it allows remote users to access to internal network resources whenever they are connected to the Internet without having to use a Virtual Private Network (VPN) connection.

It also allows domain or other system administrators to manage their remote assets like notebook/laptop systems when the user otherwise is not connected through VPN, as was the case with many remote users in the past.

Because of the seamless and bi-directional nature of DirectAccess, when a user is connected to the Internet and DirectAccess is enabled, the user's system is virtually connected to the corporate environment as much as if they were sitting on the corporate LAN.

This allows systems to respond to software inventorying requests and it allows administrators to keep the systems up to date with security updates.

Direct Access supports the following additional features:

- Multifactor authentication methods are supported.
- Uses IPv6 for remote access.
- Uses IPsec Encryption methods; DES, which uses a 56-bit key, and 3DES, which uses three 56-bit keys.
- Uses Network Access Protection (NAP) for system compliance checking on client computers before allowing them to remotely access intranet resources.
- DirectAccess servers can be configured to restrict which servers, users, and individual applications are accessible to remote access clients.

There are two different methods available for accessing internal resources using DirectAccess: **Selected Server Access** and **Full Enterprise Network Access**.

Selected Server Access allows network administrators the ability to limit the access of DirectAccess clients to a specific set of intranet application servers and deny access to all other locations on the intranet.

By using IPsec protection from the DirectAccess client to the specified servers this setup allows the sessions to be established directly between the DirectAccess client and the designated servers while providing an additional layer of IPsec peer authentication and data integrity for end-to-end traffic so that DirectAccess clients can verify that they are communicating with specific servers.

Basically the traffic is going from the DirectAccess clients and those specified servers only so the access to intranet resources is limited to just those servers.

Full enterprise network access differs in that you need to deploy IPv6 and IPSec across your entire enterprise and, rather than having access to just specified servers, you are provided a virtual gateway into your intranet through the specified system to all of the systems that you might otherwise have access to on the LAN. Enterprise access provides two types of protection: end-to-end and end-to-edge.

With end-to-end protection in use, your Windows 7 DirectAccess clients can establish an IPsec session through the DirectAccess server (which must be running Windows Server 2008 or Windows Server 2008 R2 and use both IPv6 and IPsec) to each application server. This configuration provides the highest level of security because you can configure access control on the DirectAccess server.

In an end-to-edge protection configuration, your Windows 7 DirectAccess clients establish an IPsec session to an IPsec gateway server that will forward unprotected traffic to application servers on the intranet. This configuration does not require IPsec on the intranet and works with any IPv6-capable application servers.

The entire connection process that the Windows 7 DirectAccess clients use to connect to intranet resources happens automatically without requiring user intervention.

Below is an example of a standard connection process:

1. The network connected Windows 7 DirectAccess client attempts to connect to an intranet resource.
2. The DirectAccess client attempts to connect to the DirectAccess server using native IPv6 and IPsec. Since a native IPv6 network probably isn't available (Internet connections today are still running IPv4), the client establishes an IPv6-over-IPv4 tunnel using 6to4 or Teredo.
3. If a firewall or proxy server prevents the client system using 6to4 or Teredo from connecting to the DirectAccess server, the client automatically attempts to connect using the IP-HTTPS protocol using Secure Sockets Layer (SSL).
4. The DirectAccess client and DirectAccess server authenticate each other using computer certificates for authentication which is part of the process for establishing the IPsec session.
5. The DirectAccess server verifies that the computer and user are authorized to connect using DirectAccess through Active Directory.
6. If you are using Network Access Protection (NAP) for health validation, the DirectAccess client obtains a health certificate from a Health Registration Authority (HRA) located on the Internet prior to connecting to the DirectAccess server.
7. The next step of the that process has the HRA forwarding the DirectAccess client health status information to a NAP health policy server which processes the policies defined within the Network Policy Server (NPS) and determines whether the client is compliant with system health requirements.
8. If the connecting DirectAccess client is compliant with system health requirements, the HRA obtains a health certificate for the DirectAccess client so that is can connect to the DirectAccess server and submit its health certificate for authentication.
9. The DirectAccess server allows the connection and begins forwarding traffic from the DirectAccess client to the intranet resources based on permissions and access controls as defined for the user of the system from their user and group memberships.

Some of the requirements for DirectAccess include the following:

- One or more DirectAccess servers must be a member of an AD DS domain and they must be running Windows Server 2008 R2.
- The server that will be running DirectAccess will need to have two network adapters with one that connected directly to the Internet and one connected to the intranet.
- The server will also need to have at least two consecutive, public IPv4 addresses assigned to the network adapter that is connected to the Internet.
- DirectAccess clients must be members of an AD DS domain and will need to be running Windows 7 Enterprise or Windows 7 Ultimate.
- There needs to be at least one domain controller and one DNS server that is running Windows Server 2008 SP2 or Windows Server 2008 R2.
- A public key infrastructure (PKI) will need to be in place in order to issue computer certificates and / or smart card certificates for smart card authentication and health certificates for NAP.

Configure Mobility Options

Configure and Administer Offline File Policies

The Offline Files feature in Windows has been around since Windows 2000 and even earlier when you consider the prior iteration Windows Briefcase. The Windows 7 release of the feature allows users to locally cache files from network shared folders so that those resources are accessible from the client when the computer is not directly to the network share. Offline Files is available on Windows 7 Professional, Enterprise, and Ultimate Editions.

When you enable a network resource to be available for offline access, the operating system will store a copy of the data from the share within a local cache. When the remote resource is no longer available, (e.g. client no longer connected to the LAN), the user can continue to work with the data that is the stored copy of the network location within its local cache.

When the file server that hosts the original source location becomes available such as when you get back onto the corporate network, Windows 7 will synchronize the data from the local cache with the source copy; this will allow any changes to the data at the cache level of the client to be replicated automatically back up to the original share source location.

Data owners can make a source location available to offline cache by right-clicking the folder and going to the Sharing tab and choosing the Advanced Sharing option. Refer to the discussion on Offline Files in Domain 4.

When you are accessing a remote resource that someone else has shared out you can elect to dynamically access that data remotely by choosing to set the specific file to always be available offline.

Right-click the file and choose **Always available offline.**

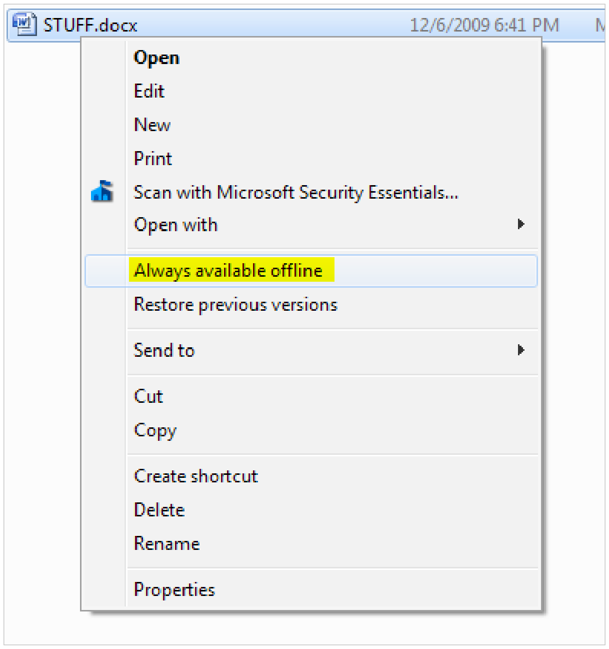
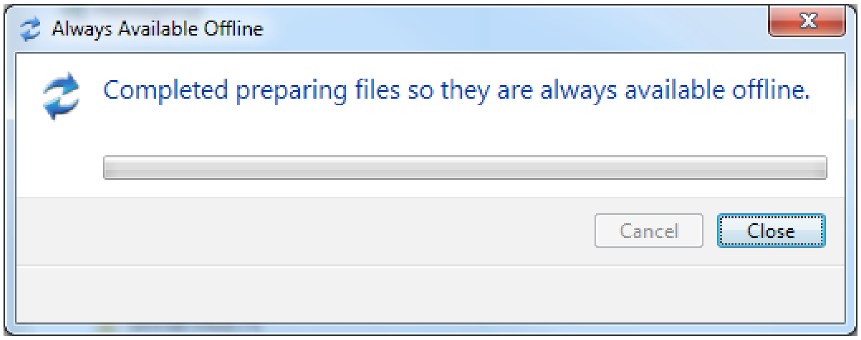


Figure 60: Configuring Individual Files for Offline Access

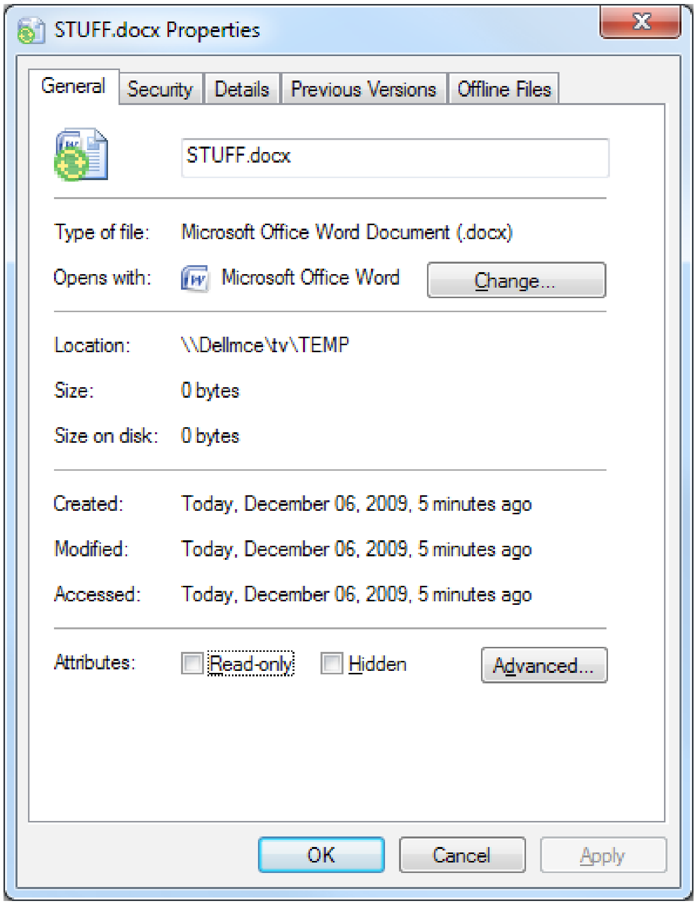
A dialog box appears, as shown below:


Always Available Offline

Completed preparing files so they are always available offline.

Figure 61: A File Caching for Offline Access

Once this is complete you'll notice that the icon for the file (a Word doc in this case) changes to include the green caching symbol added:


STUFF.docx Properties

STUFF.docx

Type of file: Microsoft Office Word Document (.docx)

Opens with: Microsoft Office Word

Location: \\Dellmce\tv\TEMP

Size: 0 bytes

Size on disk: 0 bytes

Created: Today, December 06, 2009, 5 minutes ago

Modified: Today, December 06, 2009, 5 minutes ago

Accessed: Today, December 06, 2009, 5 minutes ago

Attributes: □ Read-only □ Hidden

Figure 62: Cached File Properties

You can sync this file manually by right clicking it and choosing sync from the context menu.

You can also perform this action from the properties page of the file on the Offline Files tab that is available once you select the option to make the files available offline.

Generally there is little need to perform a manual sync as this is done automatically for you. The Offline Files feature in Windows 7 has the four following modes of operation:

- **Online Mode (Default Setting)** – when this setting is configured all changes made to files are applied to the remote source location and then to the local cache. Read requests are made from the local cache. Synchronization occurs automatically.
- **Auto Offline Mode –** Windows 7 will transition settings to auto offline mode if a sudden loss to the network is detected. At that point required access will come from the local cache and the operating system will attempt to reconnect to the network source location automatically every two minutes. Once reconnection is successful, Offline Files automatically transitions back to online mode.
- **Manual Offline Mode** – offline mode is forced when user selects the Work Offline item in Windows Explorer as shown below.
- **Slow-link Mode** – enabled by default in Windows 7 this setting becomes available when the link speed falls below 64,000 bits per second. When this mode is activated as the bits per second slows below the threshold, all file operations are performed against the local cache. Users can synchronize manually, but automatic synchronization does not occur. Windows 7 will automatically convert back to online mode when link speed returns to a point higher than the set threshold. 64,000 bits per second is the default setting but it is configurable along with many other settings through group Policy.

Configure and Administer Transparent Caching

Windows 7 transparent caching allows client computers to cache remote files in a proactive manner, reducing the frequency the client needs to access a remote source location.

When a user first opens a file in a shared folder at the remote source, Windows 7 reads the file and then stores a local copy of it on the local hard drive. Each time the user needs to access this cached file, Windows 7 retrieves it from the local cache, rather than the remote source location.

Windows 7 will **always** check the original source data to make sure the local cache is the most recent copy (e.g. the user may not have made any changes to the data but another user might have, rendering the cached copy out-of-date and in need of a refresh from the original source location). If this integrity check is attempted and the original source location cannot be reached, the cache can't be accessed.

When transparent caching is enabled, updates to the cached file(s) are always written directly to the original source location. Transparent caching is not enabled by default on fast networks.

Windows 7 Background synchronization for offline files occurs automatically; the user does not need to choose between online and offline operating options.

If users choose to take manual actions to sync the files they can do this on a file by file or share by share basis or they can take this action from the Sync Center from the Control Panel.

Administrators can enable the Exclude Files From Being Cached Policy to prevent certain file types from being available offline. File types are designated in the policy by their file name extension.

If there is a situation where you have a sync conflict with respect to offline files you can resolve the issue by selecting Resolve within the View Sync Conflicts area and selecting one of the three available actions:

- **Keep the local version** – choosing this option means that you are going to be overwriting the conflict version of the file on the original network source location in order to keep the local cached version on the computer.
- **Keep the server version** – choosing this option means that you are going to keep the version of the file that is stored on the original network source location and effectively deleting the changes made to the local cached version.
- **Keep both versions** – choosing this option means the local cached copy of the data on the computer is going to be kept but renamed and then saved to the original source location on the network. The version of the file in the original source location on the network keeps the original name.

Creating and Migrating Power Policies

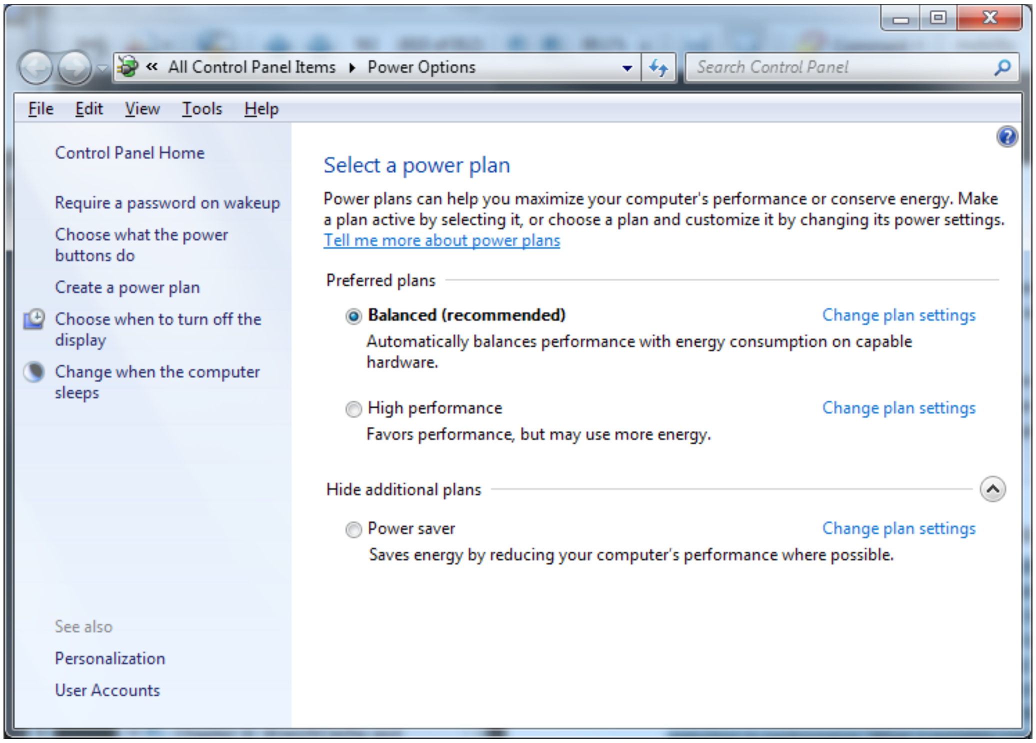
Power plans are a number of different settings that detail how a Windows computer runs, as it pertains to power management. In most cases, these are used to control the battery life for portable systems. The settings, however, can be manipulated on desktops and workstations as a way to maintain and mange your electrical consumption.

Windows 7 comes with three power plans, by default: **High Performance**, **Balanced**, and **Power Saver**.

The High Performance power plan allows the system hardware to run at 100% without reducing any of the settings or allowing any built in power management to reduce consumption.

Most of the default settings of the Power Saver plan configure the system hardware devices to use less energy as applicable by scaling back the amount of electricity consumed. This reduction of power consumption has an equivalent reduction in peripheral and overall system performance.

Generally speaking, users with PCs that spend the majority of their running time plugged directly into the wall running under the Power Saver plan. PCs intended for portability are better candidates. The default power plan for a newly installed client running Windows 7 is **Balanced**.


« All Control Panel Items ▸ Power Options
Search Control Panel
File
Edit
View
Tools
Help
Control Panel Home
Require a password on wakeup
Choose what the power buttons do
Create a power plan
Choose when to turn off the display
Change when the computer sleeps
See also
Personalization
User Accounts

Select a power plan

Power plans can help you maximize your computer's performance or conserve energy. Make a plan active by selecting it, or choose a plan and customize it by changing its power settings.
Tell me more about power plans

Preferred plans

● **Balanced (recommended)** Change plan settings
Automatically balances performance with energy consumption on capable hardware.

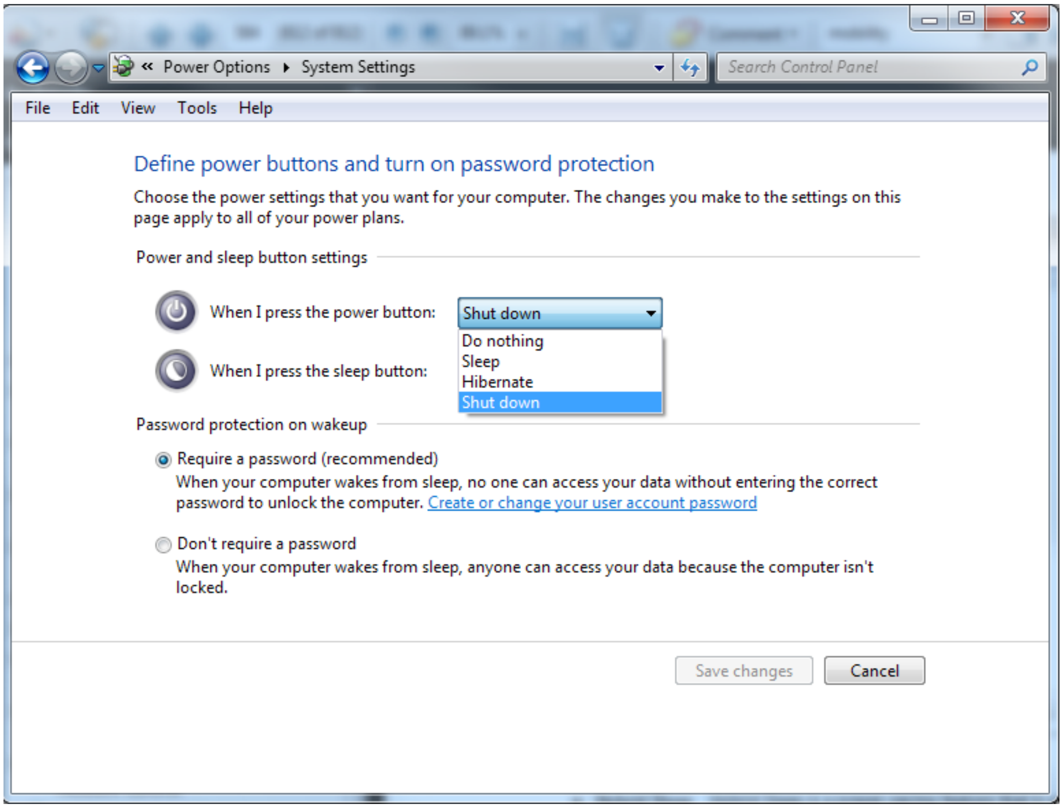
○ High performance Change plan settings
Favors performance, but may use more energy.

Hide additional plans

○ Power saver Change plan settings
Saves energy by reducing your computer's performance where possible.

Figure 63: Selecting a Power Plan

You can make adjustments to these default plans or you can create your own from the Power Options center in Control Panel. There are four states that you can set the system to as options for when a low or critical power level is reached. These states also apply to any changes you make to the behavior of the power buttons.



Define power buttons and turn on password protection

Choose the power settings that you want for your computer. The changes you make to the settings on this page apply to all of your power plans.

Power and sleep button settings

When I press the power button: Shut down

Do nothing
Sleep
Hibernate
Shut down

When I press the sleep button:

Password protection on wakeup

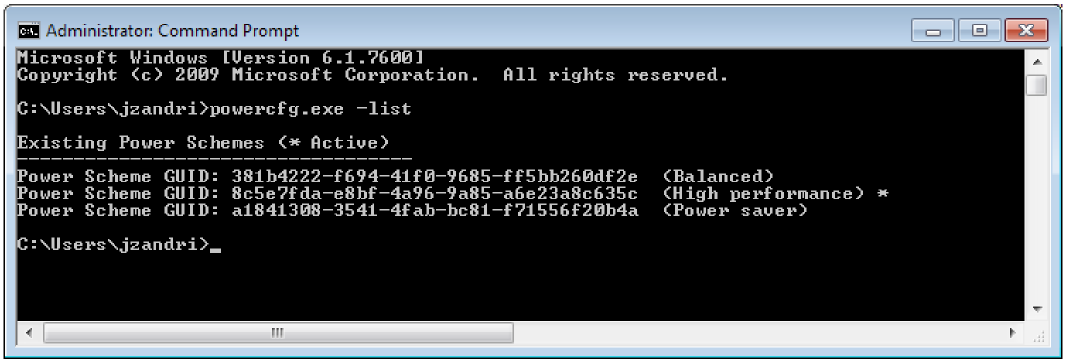
● Require a password (recommended)
When your computer wakes from sleep, no one can access your data without entering the correct password to unlock the computer. Create or change your user account password

○ Don't require a password
When your computer wakes from sleep, anyone can access your data because the computer isn't locked.

Figure 64: Changing the Behavior of the Power Button

- **Sleep** – when this power state activates, the system is nearly shutdown. Only the RAM remains in an active state, being refreshed every few seconds to keep the current data and session in volatile memory, where it may be reached quickly. This is a more power-friendly solution than a fully running state, but there remains a significant draw on the battery to keep the RAM refreshed. If the system is not brought out of the sleep state before a predetermined time set in the power plan, the system usually transitions to the Hibernate state.
- **Hibernate** – when this power state activates, all of the system devices are turned off and the all of the contents held in RAM are written to a special file on the operating system volume. You can bring a system out of hibernation by using the power buttons on the system.
- **Shutdown** – as the name implies, the system is completely shutdown.
- **Hybrid Sleep** – a configurable power-saving feature that allows contents of the session being held in RAM to be stored and refreshed as normal in RAM but also to be stored in a special file on the hard disk. When the Hybrid Sleep option is enabled, computers put to sleep use Hybrid Sleep rather than ordinary Sleep mode. This is an additional feature that allows for sudden power loss. If a desktop system in Sleep mode were to lose power (e.g. blackout) or a laptop system were to suddenly have its battery removed (when it is on battery power only) the current session saved in RAM in Sleep would be lost due to the sudden total loss of power that was refreshing the session held in RAM. Because **Hybrid Sleep** also uses the stored file, the sudden total loss of power will not cause the session to be lost because it is also written to the hard drive.

Powercfg.exe is a command-line utility that you can use to manage any of the Windows 7 power settings as well as some of the advanced settings that cannot be configured through Group Policy or the Advanced Plan Settings. One of these actions is to export or migrate a configured power plan on one system to another. This would need to be done by an administrator from an elevated command prompt. At an elevated command prompt you would type **powercfg.exe** with the – list switch to get the following output:



```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\jzandri>powercfg.exe -list

Existing Power Schemes (* Active)
-----------------------------------
Power Scheme GUID: 381b4222-f694-41f0-9685-ff5bb260df2e  (Balanced)
Power Scheme GUID: 8c5e7fda-e8bf-4a96-9a85-a6e23a8c635c  (High performance) *
Power Scheme GUID: a1841308-3541-4fab-bc81-f71556f20b4a  (Power saver)

C:\Users\jzandri>_
```

Figure 65: Using powercfg.exe

Once you take note of the power scheme that you want to export you will probably want to use the MARK capability of the command window to copy the GUID to the clipboard so that you don't have to enter it manually.

The next step would be to enter the following command and switch **powercfg.exe -EXPORT** indicating the desired location for the output as well as the name for the file. The completed step will look like this:

```
C:\Users\jzandri> powercfg.exe -EXPORT c:\TEMP\mytestscheme.pow
8c5e7fda-e8bf-4a96-9a85-a6e23a8c635c
```

The resulting file will be available in the directory you specified. You can copy the file onto another system and then import it for use by running:

```
C:\Users\jzandri> powercfg.exe –import c:\TEMP\mytestscheme.pow
```

(**Note:** substitute the path and file name for your *.pow file).

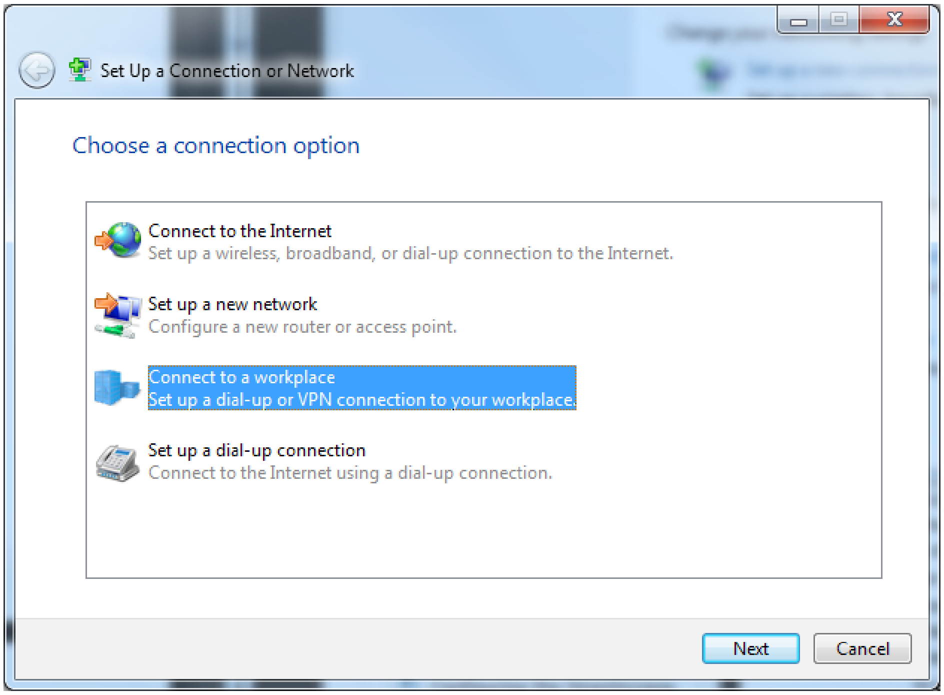
Configure Remote Connections

Configure and Administer VPN Connections

VPNs are used to create secured tunnels over a public network - the Internet, in other words - back to their corporate networks. This is an inexpensive solution to direct dial or frame relay set ups providing remote access to network resources such as printers, databases, internal SharePoint sites and so forth.

On your Windows 7 system, you create a new VPN connection in the **Network And Sharing Center.**

1. Click **Set Up A New Connection Or Network.**
2. Choose **Connect to a Workplace**.



Set Up a Connection or Network

Choose a connection option

Connect to the Internet
Set up a wireless, broadband, or dial-up connection to the Internet.

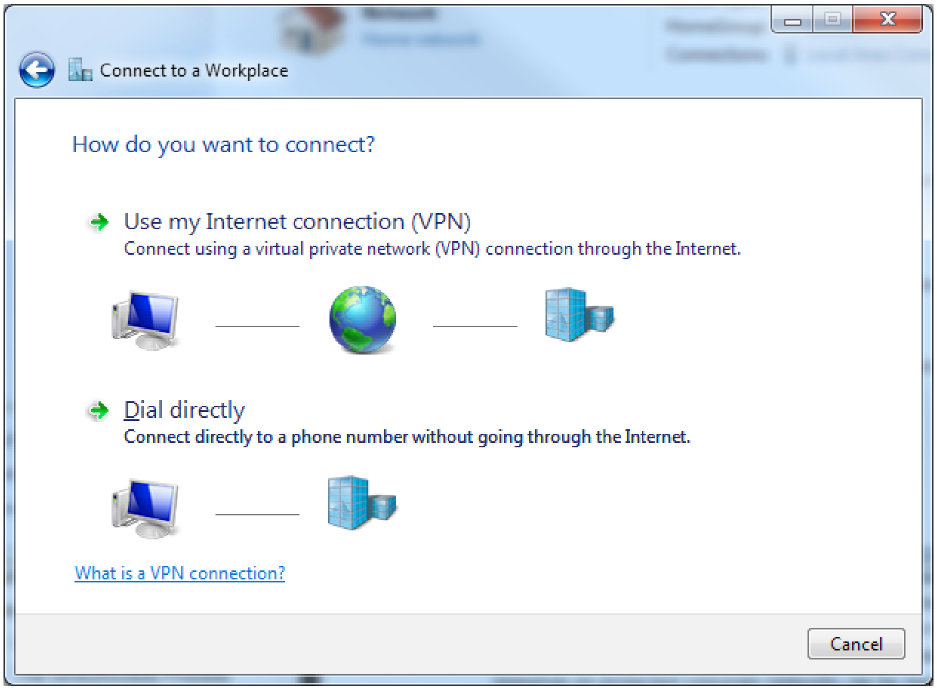
Set up a new network
Configure a new router or access point.

Connect to a workplace
Set up a dial-up or VPN connection to your workplace.

Set up a dial-up connection
Connect to the Internet using a dial-up connection.

Figure 66: Setting Up a VPN Connection

3. You're given two options: to configure a VPN session or to dial directly.



Connect to a Workplace

How do you want to connect?

Use my Internet connection (VPN)
Connect using a virtual private network (VPN) connection through the Internet.

Dial directly
Connect directly to a phone number without going through the Internet.

What is a VPN connection?

Figure 67: Selecting a VPN Connection Method

When you create new connection and allow the operating system to set the VPN type automatically, the connection will always be attempted using the most secure protocol available. The VPN protocols natively supported in Windows 7 include:

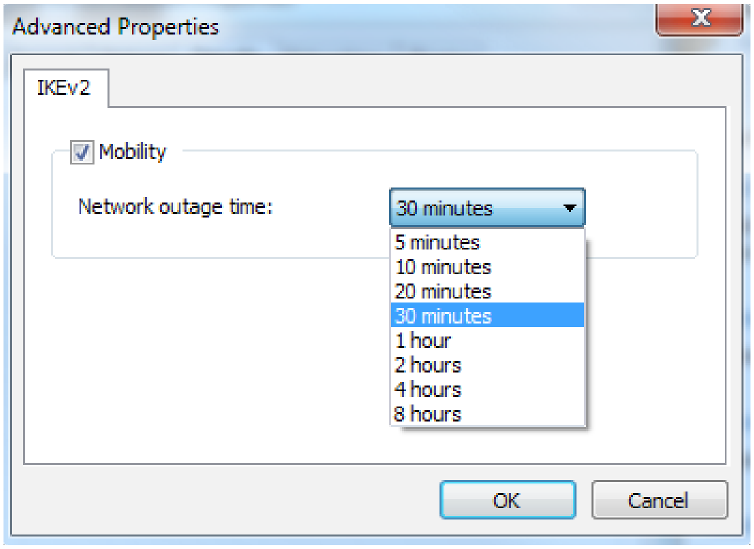
- **PPTP** – the most common VPN protocol is the Point to Point Tunneling Protocol but it is the least secure as PPTP does not require access to a public key infrastructure (PKI). For authentication, PPTP uses: **MS-CHAP, MS-CHAPv2, EAP, and PEAP**. For encryption, PPTP uses **MPPE** (Microsoft Point-to-Point Encryption). PPTP connections provide data confidentiality but not data integrity or data origin authentication.
- **L2TP / IPsec** – Layer Two Tunneling Protocol using Internet Protocol Security is the most secure VPN protocol, providing per-packet data origin authentication, data integrity, replay protection, and data confidentiality using digital certificates. A L2TP / IPsec solution cannot be used behind NAT (Network Address Translation) unless the client and server support IPsec NAT Traversal (NAT-T). Windows 7, Windows Server 2003, and Windows Server 2008 all offer native support for NAT-T.
- **SSTP** – Secure Socket Tunneling Protocol (SSTP) is a form of VPN tunnel that provides a mechanism to transport PPP or L2TP traffic through an SSL 3.0 channel. SSTP tunnels use port 443 and since most firewalls allows this traffic for secure connections to internet locations these types of VPNs are the easiest to set up successfully. Using PPTP, L2TP/IPsec, and IKEv2 VPN protocols require firewall exceptions. SSTP supports data origin authentication, data integrity, replay protection, and data confidentiality.
- **IKEv2** – When you configure a new VPN connection with the default settings, Windows 7 attempts to make an IKEv2 connection first using UDP port 500 by default. IKEv2 supports IPv6, the VPN Reconnect feature, Extensible Application Protocol (EAP) and computer certificates for client side authentication. IKEv2 supports Microsoft Protected EAP (PEAP), Microsoft Secured Password (EAP-MSCHAP v2), and Microsoft Smart Card or Other Certificate for authentication but it does not support POP, CHAP, or MS-CHAPv2 (without EAP). IKEv2 offers data origin authentication, data integrity, replay protection, and data confidentiality.

Windows 7 supports password-based authentication protocols and certificate-based authentication protocols for both dial-up and VPN connections.

- **Password Authentication Protocol (PAP)** – uses unencrypted passwords for authentication and is not enabled by default for Windows 7 VPN connections. It is not supported by remote access servers running Windows Server 2008.
- **Challenge Authentication Protocol (CHAP)** – password-based authentication protocol. CHAP is enabled by default for Windows 7 VPN connections. It is not supported by remote access servers running Windows Server 2008.
- **Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP v2)** – password-based authentication protocol that uses the credentials of the currently logged on user for authentication for VPN connections.
- **Protected Extensible Authentication Protocol with Transport Layer Security (PEAP /PEAP-TLS)** – certificate-based authentication protocol where users authenticate using certificates. Requires the installation of a computer certificate on the VPN server.
- **EAP -MS-CHAP v2/PEAP -MS-CHAP v2** – most secure password-based authentication protocols available to VPN clients running Windows 7. Requires a computer certificate on the VPN server but not one for the client.
- **Smart Card or Other Certificate** – used to authenticate VPN connections using a smart card or a certificate installed the client system.

VPN Reconnect is a new Windows 7 feature that allows clients reconnect automatically to a disrupted VPN session if it is dropped or lost. It is available on all editions of Windows 7. IKEv2 advanced properties allows you to set up VPN Reconnect.

VPN Reconnect uses the IKEv2 tunneling protocol with the MOBIKE extension (IKEv2 Mobility and Multihoming), which allows you to set advanced properties for network outage time to a range between 5 minutes and 8 hours (the default is 30 minutes).



Advanced Properties

IKEv2

☑ Mobility

Network outage time: 30 minutes

Figure 68: Configuring IKEv2 Outage Time

As needed for your Windows 7 systems, you can still set up a dial-up connection by going to the **Network And Sharing Center** under **Network and Internet** and selecting **Set Up A New Connection Or Network**.

On the **Choose A Connection Option** page you would need to select **Set Up A Dial-Up Connection** and then click **Next** to bring up the **Create A Dial-up Connection** dialog box.

Here you can enter the phone number of the Internet Service Provider (ISP) and the applicable user name and password for the account at the ISP. You would also designate a connection name for this configuration and choose whether or not you want other users of the computer to be able to use the connection. As needed, you can configure dialing rules, such as country code, carrier code, a specific number to access an outside line, or switch between pulse and tone dialing by selecting the Dialing Rules option.

If you need to set up a VPN session so that users can connect to the Windows 7 system you can do this by performing the following steps:

1. Go to **All Control Panel Items\Network Connections** and select **File** and then choose **New Incoming Connection.**

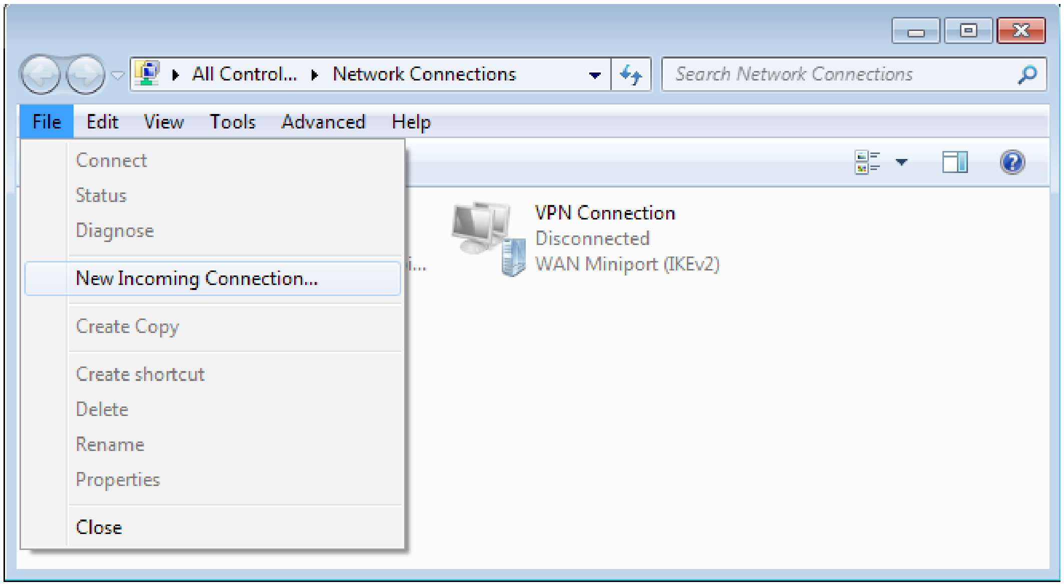
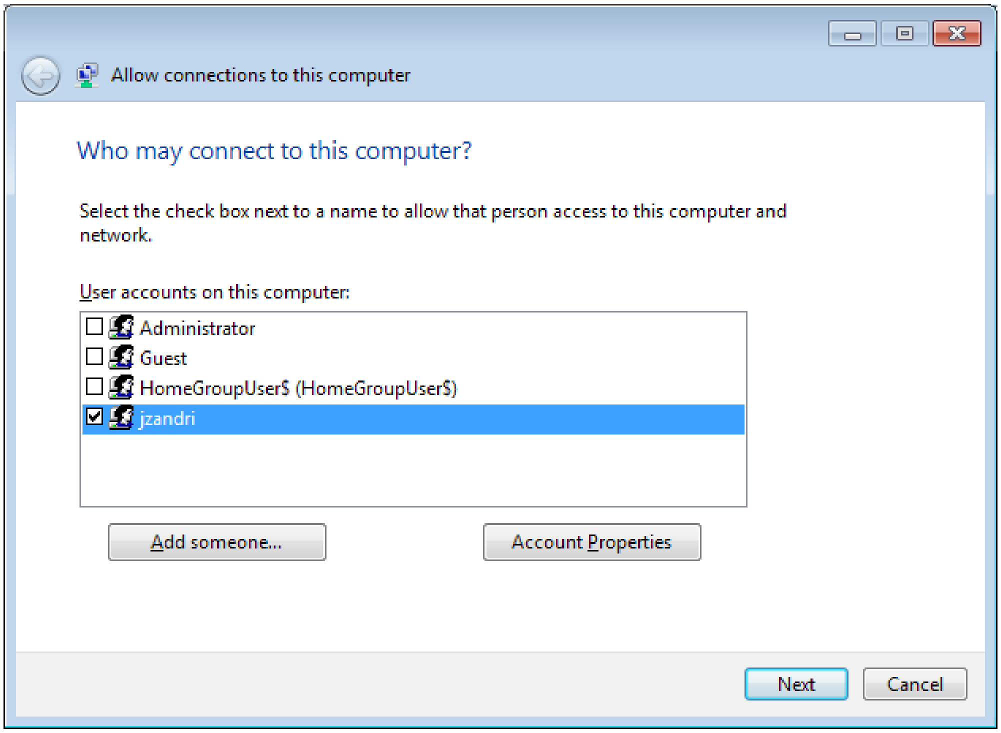


Figure 69: Setting Up a VPN Connection

2. Once you do this you would need to set who is allowed to connect to this system by selecting their names from the "Who may connect to this computer" dialog box.



Who may connect to this computer?

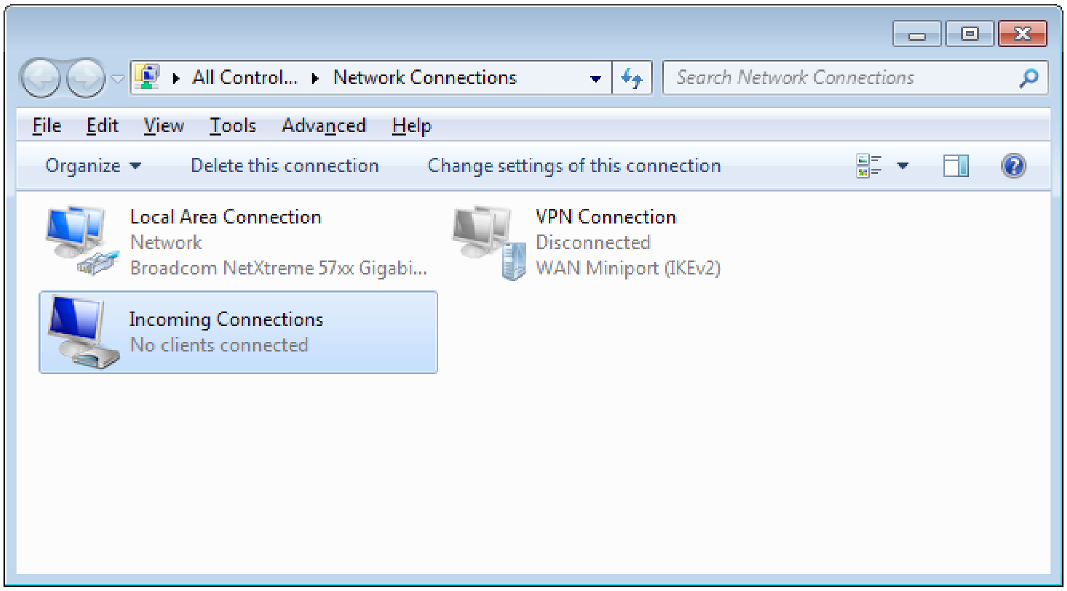
Select the check box next to a name to allow that person access to this computer and network.

User accounts on this computer:

☐ Administrator
☐ Guest
☐ HomeGroupUser$ (HomeGroupUser$)
☑ jzandri

Figure 70: Selecting Users for the VPN

3. On the next page, you can choose from the available types of connections that the system supports and/or the ones that you want to support on the system.
4. You will see **Through The Internet** in you have an active NIC / wireless connection or **Through A Dial-Up Modem** if your system has a modem.
5. The different types of networks and protocols are shown on the next screen; you can choose to leave the selected defaults or make adjustments to them and choose **Allow Access** to continue.
6. Finally, you're brought back to the Network Connections screen and the connection is now available on your system.



Local Area Connection
Network
Broadcom NetXtreme 57xx Gigabi...

VPN Connection
Disconnected
WAN Miniport (IKEv2)

Incoming Connections
No clients connected

Figure 71: A New Incoming Connection

Domain Seven: Monitoring and Maintaining Systems that Run Windows 7

Configure Updates to Windows 7

When properly configured, Windows Update can help keep your system up to date with the latest security releases and other operating system updates automatically as they are released from Microsoft. Windows Update in Windows 7 is part of **Action Center**, which you can launch from the notification area or from the Start Menu.

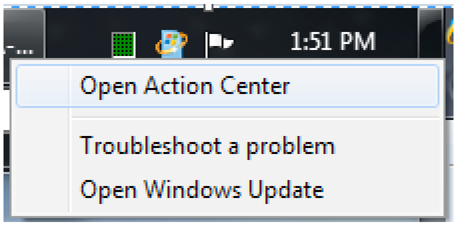
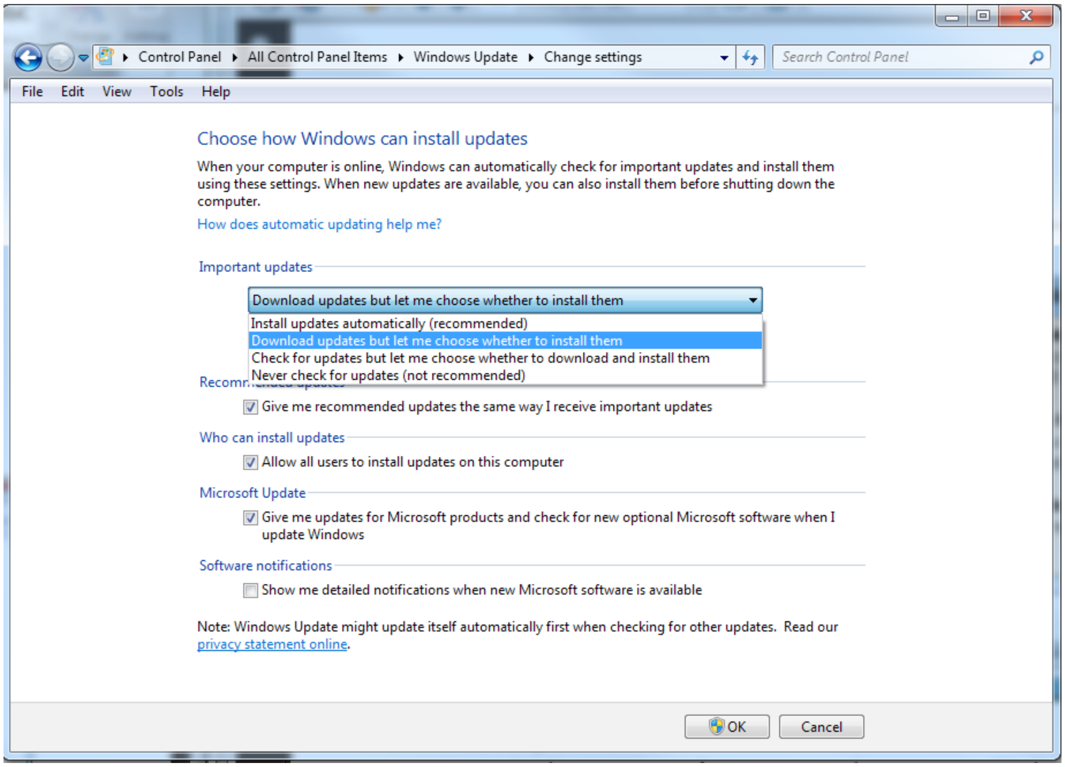


Figure 72: Launching the Action Center

Clicking on Windows Update in the bottom section of the left-hand pane will bring up **Windows Update**. Selecting **Change Settings** from the left-hand pane will enable you to make adjustments to how Windows will check and install important updates as they are released.


Control Panel ▸ All Control Panel Items ▸ Windows Update ▸ Change settings
Search Control Panel
File Edit View Tools Help
OK
Cancel

Choose how Windows can install updates

When your computer is online, Windows can automatically check for important updates and install them using these settings. When new updates are available, you can also install them before shutting down the computer.

How does automatic updating help me?

Important updates

Download updates but let me choose whether to install them

- 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)

Recommended updates

☑ Give me recommended updates the same way I receive important updates

Who can install updates

☑ Allow all users to install updates on this computer

Microsoft Update

☑ Give me updates for Microsoft products and check for new optional Microsoft software when I update Windows

Software notifications

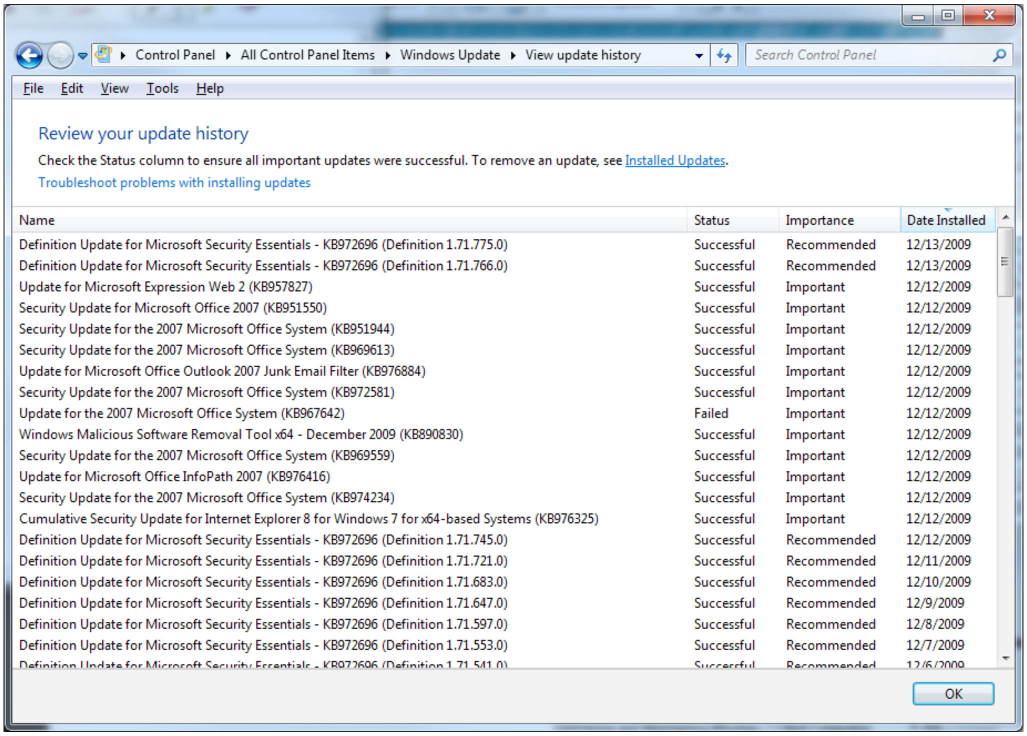
□ Show me detailed notifications when new Microsoft software is available

Note: Windows Update might update itself automatically first when checking for other updates. Read our privacy statement online.

Figure 73: Changing Windows Update Settings

- Installing updates automatically is the default and recommended selection for **Important Updates**. If this default is kept the system will check for updates each day and install them automatically at 3:00AM if they are available. If it is required the system will be rebooted after the updates are installed.
- **Recommended Updates** settings can be changed to reflect how updates marked as recommended, but not important, are downloaded and/or installed. The default setting is a checkbox migrating whatever you choose for Important Updates to Recommended Updates.
- **Who can install updates** allows you to choose whether all users can install updates, or only the system's administrator account can install updates. The default is all users.
- **Microsoft Update** allows you to opt out of updates for all of Microsoft's products. This is not recommended.
- **Software notifications** generate detailed information on new Microsoft software and updates, when available.

You can see the update history for a given system by selecting **View Update History** on the main Windows Update page, in the left action pane. The resulting screen outlines all updates for that particular system.


Control Panel ▸ All Control Panel Items ▸ Windows Update ▸ View update history
Search Control Panel
File Edit View Tools Help
OK

Review your update history

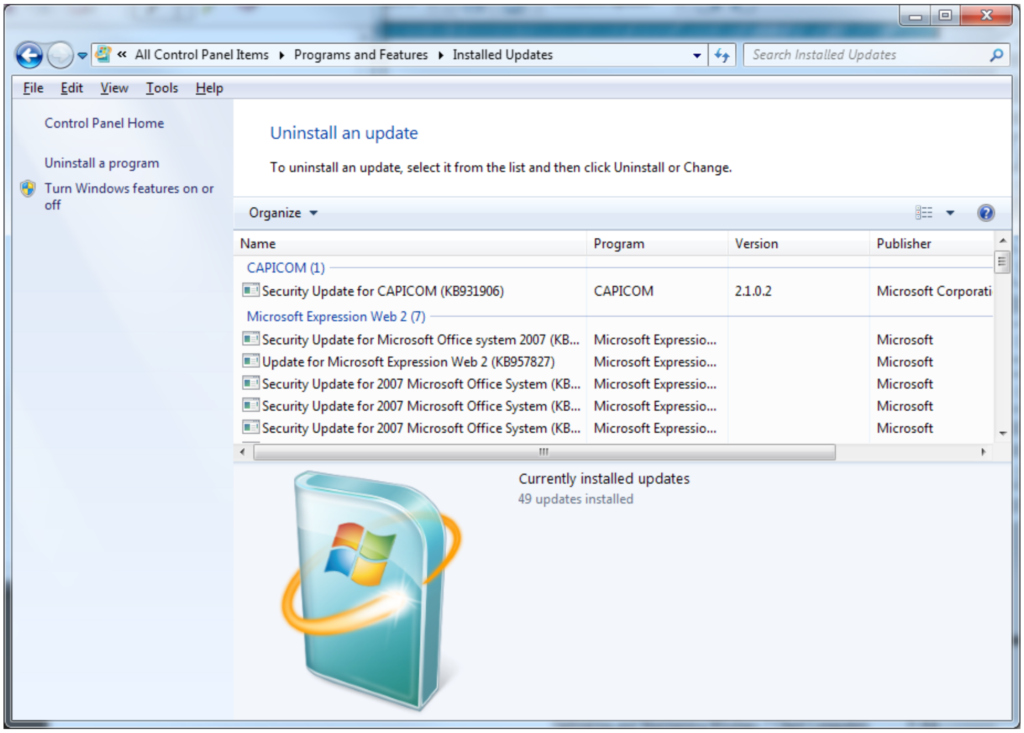
Check the Status column to ensure all important updates were successful. To remove an update, see Installed Updates.

Troubleshoot problems with installing updates

Name	Status	Importance	Date Installed
Definition Update for Microsoft Security Essentials - KB972696 (Definition 1.71.775.0)	Successful	Recommended	12/13/2009
Definition Update for Microsoft Security Essentials - KB972696 (Definition 1.71.766.0)	Successful	Recommended	12/13/2009
Update for Microsoft Expression Web 2 (KB957827)	Successful	Important	12/12/2009
Security Update for Microsoft Office 2007 (KB951550)	Successful	Important	12/12/2009
Security Update for the 2007 Microsoft Office System (KB951944)	Successful	Important	12/12/2009
Security Update for the 2007 Microsoft Office System (KB969613)	Successful	Important	12/12/2009
Update for Microsoft Office Outlook 2007 Junk Email Filter (KB976884)	Successful	Important	12/12/2009
Security Update for the 2007 Microsoft Office System (KB972581)	Successful	Important	12/12/2009
Update for the 2007 Microsoft Office System (KB967642)	Failed	Important	12/12/2009
Windows Malicious Software Removal Tool x64 - December 2009 (KB890830)	Successful	Important	12/12/2009
Security Update for the 2007 Microsoft Office System (KB969559)	Successful	Important	12/12/2009
Update for Microsoft Office InfoPath 2007 (KB976416)	Successful	Important	12/12/2009
Security Update for the 2007 Microsoft Office System (KB974234)	Successful	Important	12/12/2009
Cumulative Security Update for Internet Explorer 8 for Windows 7 for x64-based Systems (KB976325)	Successful	Important	12/12/2009
Definition Update for Microsoft Security Essentials - KB972696 (Definition 1.71.745.0)	Successful	Recommended	12/12/2009
Definition Update for Microsoft Security Essentials - KB972696 (Definition 1.71.721.0)	Successful	Recommended	12/11/2009
Definition Update for Microsoft Security Essentials - KB972696 (Definition 1.71.683.0)	Successful	Recommended	12/10/2009
Definition Update for Microsoft Security Essentials - KB972696 (Definition 1.71.647.0)	Successful	Recommended	12/9/2009
Definition Update for Microsoft Security Essentials - KB972696 (Definition 1.71.597.0)	Successful	Recommended	12/8/2009
Definition Update for Microsoft Security Essentials - KB972696 (Definition 1.71.553.0)	Successful	Recommended	12/7/2009
Definition Update for Microsoft Security Essentials - KB972696 (Definition 1.71.541.0)	Successful	Recommended	12/6/2009

Figure 74: Windows Update History

If you are having an issue with an update, you can select **Installed Updates** and review and / or remove them. From this same view you can elect to turn Windows features on or off as desired.


« All Control Panel Items ▸ Programs and Features ▸ Installed Updates
Search Installed Updates
File Edit View Tools Help
Control Panel Home
Uninstall a program
Turn Windows features on or off
Organize ▾

Uninstall an update

To uninstall an update, select it from the list and then click Uninstall or Change.

Name	Program	Version	Publisher
CAPICOM (1)			
Security Update for CAPICOM (KB931906)	CAPICOM	2.1.0.2	Microsoft Corporati
Microsoft Expression Web 2 (7)			
Security Update for Microsoft Office system 2007 (KB...	Microsoft Expressio...		Microsoft
Update for Microsoft Expression Web 2 (KB957827)	Microsoft Expressio...		Microsoft
Security Update for 2007 Microsoft Office System (KB...	Microsoft Expressio...		Microsoft
Security Update for 2007 Microsoft Office System (KB...	Microsoft Expressio...		Microsoft
Security Update for 2007 Microsoft Office System (KB...	Microsoft Expressio...		Microsoft

Currently installed updates
49 updates installed

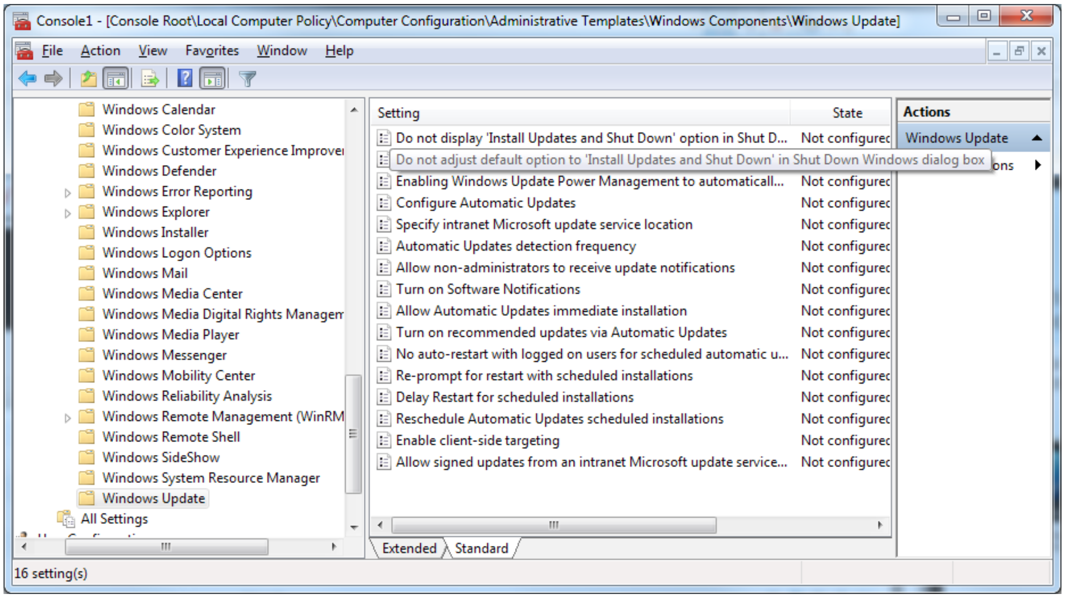
Figure 75: Installed Updates

If you have repeatedly canceled out an update you can elect to hide it from showing up in the regular list of updates available. If you need to restore any of them you can choose that option from the action pane which will bring you to the Restore hidden updates screen. You can also reach this location by navigating to:

Control Panel → **All Control Panel Items** → **Windows Update** → **Restore hidden updates**.

If there are any in the list you can highlight them and choose to restore them. When you review the available updates to install on your system, you will see additional information on the update in the results pane on the far right which offers you direct links to additional information and support details as shown below. If you are connected to the internet you can select the links and you will arrive at the details page. When you choose the More information link you are brought directly to the Knowledge Base article for that update.

You also have the ability to manage Windows Update through group policy, in the group policy editor MMC snap-in. In the Add or Remove Snap-ins page you would navigate to the Group Policy Object Editor and either double click it or highlight it by selecting it once and choosing the Add option. In order to configure the Windows Update settings for the system you will need to look under the Computer Configuration container. Windows Update settings are found under **Administrative Templates** in the **Windows Components** sub container.



Console1 - [Console Root\Local Computer Policy\Computer Configuration\Administrative Templates\Windows Components\Windows Update]

Setting	State
Do not display 'Install Updates and Shut Down' option in Shut D...	Not configured
Do not adjust default option to 'Install Updates and Shut Down' in Shut Down Windows dialog box	
Enabling Windows Update Power Management to automaticall...	Not configured
Configure Automatic Updates	Not configured
Specify intranet Microsoft update service location	Not configured
Automatic Updates detection frequency	Not configured
Allow non-administrators to receive update notifications	Not configured
Turn on Software Notifications	Not configured
Allow Automatic Updates immediate installation	Not configured
Turn on recommended updates via Automatic Updates	Not configured
No auto-restart with logged on users for scheduled automatic u...	Not configured
Re-prompt for restart with scheduled installations	Not configured
Delay Restart for scheduled installations	Not configured
Reschedule Automatic Updates scheduled installations	Not configured
Enable client-side targeting	Not configured
Allow signed updates from an intranet Microsoft update service...	Not configured

16 setting(s)

Figure 76: Editing Windows Update Group Policy Settings

Windows Update can be set on client systems so that updates come from the Microsoft Update servers on the Internet. That is the default out of the box setting most recognized for home deployments of Windows 7 and for small businesses where there are less than 10 computers or so.

In a scenario where there are more systems than that in a single location there is a significant bandwidth savings to be gained by deploying a centralized software update solution like Windows Server Update Services (WSUS), System Center Essentials, or System Center Configuration Manager (SCCM) 2007.

This allows an administrator to set each client system to download their updates in the same location locally on the LAN.

Rather than having each system go on the internet to download updates the system configured as the centralized software update solution will and all the other systems on the LAN will go to it for their updates.

Windows 7 require that the WSUS server be running WSUS 3.0 with Service Pack 1 or later.

Microsoft Update provides security and other important updates according to Microsoft's release schedule. While security updates are delivered on the second Tuesday of each month as a rule and most other releases (non-security) are somewhat scheduled they are not always predicable. Due to this, an enterprise environment does not always have the proper opportunity to test that an update is fully compatible with all of their software and standards before it is made available to clients.

Windows Server Update Service can help to resolve this issue for an enterprise environment.

Windows Server Update Services gives administrators the flexibility to deploy updates according to their own needs and schedule. While the WSUS server might download all of the available updates that are release for a given set of products, the administrator controls when they will be made available to clients for deployment. Additionally, administrators can test an update on a small group of computers before deploying it to all computers in the organization.

Administrators can also centrally roll back the installation of an update across all computers in the organization when WSUS is deployed if the need arises such as in the situation where an issue that was missed in test is discovered and causes issues with Windows 7 clients.

The administrator can remove that update from the list of approved updates and roll back the update from the WSUS server which removes that update from all client computers in the organization that have already deployed it.

Manage Disks

Windows 7 is no different from any prior versions of Windows or any other operating system with respect to reading and writing to disk: there needs to be an associated file system on a given volume to read from it or write to it.

Windows 7 can partition disks in one of two ways: by using **Master Boot Record** (MBR) or a **Globally Unique Identifier Partition Table** (GPT).

MBR partitions are supported under all editions of Windows all the way back to the days before Windows.

GPT is an updated partitioning system supported on Windows Vista, Windows 7, Windows Server 2008, and 64-bit versions of Windows XP and Windows Server 2003 operating systems. It offers the following advantages over MBR partitions:

- MBR partitions are limited to four Primary partitions or three Primary and one Extended partition. GPT can support up to 128 partitions.
- GPT is able to more accurately identify the physical disk geometry, allowing Windows to create partitions and logical drives on cylinder boundaries. Because today's hard drives' physical geometry has been altered to enable larger capacities Windows attempts to do this as accurately as possible when MBR is used but it is not as accurate as GPT.
- The theoretical maximum size for a GPT partition is 18 exabytes; that equals about 18 million terabytes. 2 TB maximum partition size is the limit on an MBR partition.
- MBR does not have redundant partition tables whereas GPT uses primary and backup partition tables for redundancy and CRC32 fields for improved partition data structure integrity.

You can convert disks from MBR to GPT by using the Disk Management MMC snap-in or the DiskPart command-line tool.

Within the Disk Management snap-in, you simply selecting right click the appropriate volume and choose the appropriate Convert option. In this case, we're converting to a GPT Disk. The same actions may be used to convert a disk to MBR, when appropriate.

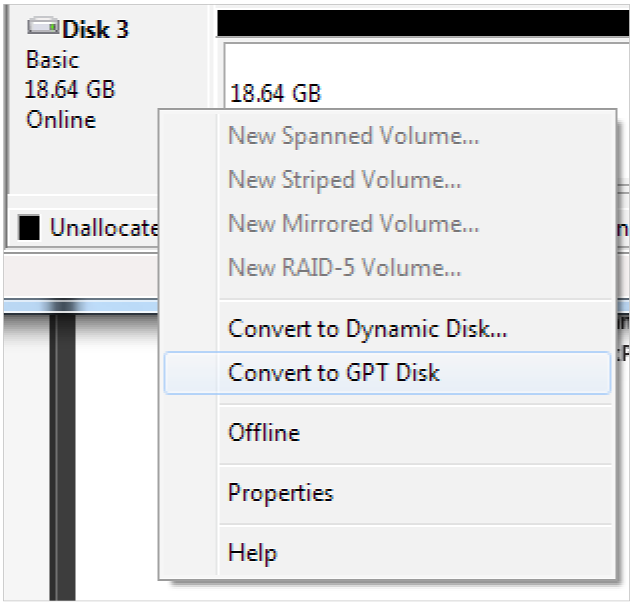


Figure 77: Converting a Disk to a GPT Volume

The DiskPart tool uses the commands **convert gpt** or **convert mbr** to change a disk to the appropriate volume type.

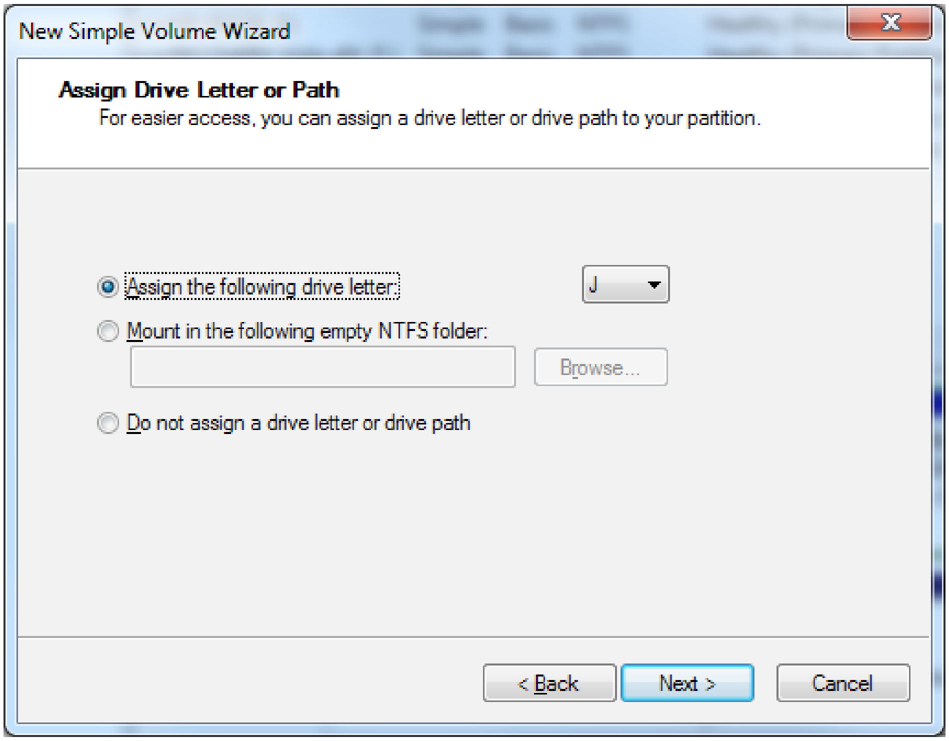
There are two different disk types available in Windows 7:

- **Basic Disks** – use normal partition tables and contain primary partitions, extended partitions, and logical drives.
- **Dynamic Disks** – contain dynamic volumes, such as simple volumes, spanned volumes, striped volumes, mirrored volumes, and RAID-5 volumes.

A basic or dynamic disk can contain any combination of FAT16, FAT32, or NTFS partitions or volumes.
A disk system can contain any combination of storage types but all of the volumes on the same disk must use the same storage type.

You can make a volume from free disk space by performing the following actions:

1. Right-click free space on the disk in **Disk Management** and select the **New Simple Volume Wizard** from the context menu.
2. Select Next on the welcome screen.
3. Specify the volume size from the available disk space.
4. Assign a drive letter or mount the volume to an empty NTFS folder.



New Simple Volume Wizard

Assign Drive Letter or Path

For easier access, you can assign a drive letter or drive path to your partition.

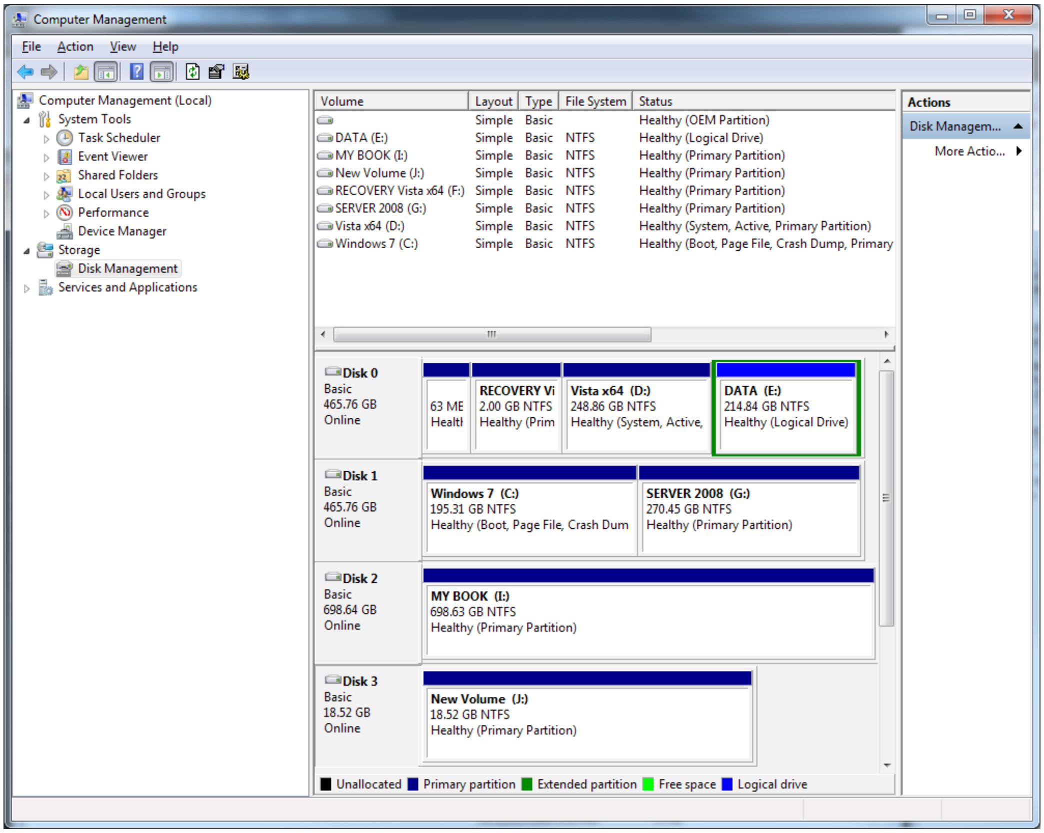
● Assign the following drive letter: J

○ Mount in the following empty NTFS folder:

○ Do not assign a drive letter or drive path

Figure 78: Assigning a Drive Letter or Path

5. Format the partition to complete the process. Once the format is complete, the new volume will appear as a basic disk in the result pane.



Volume	Layout	Type	File System	Status
	Simple	Basic		Healthy (OEM Partition)
DATA (E:)	Simple	Basic	NTFS	Healthy (Logical Drive)
MY BOOK (I:)	Simple	Basic	NTFS	Healthy (Primary Partition)
New Volume (J:)	Simple	Basic	NTFS	Healthy (Primary Partition)
RECOVERY Vista x64 (F:)	Simple	Basic	NTFS	Healthy (Primary Partition)
SERVER 2008 (G:)	Simple	Basic	NTFS	Healthy (Primary Partition)
Vista x64 (D:)	Simple	Basic	NTFS	Healthy (System, Active, Primary Partition)
Windows 7 (C:)	Simple	Basic	NTFS	Healthy (Boot, Page File, Crash Dump, Primary

Disk	Partitions			
Disk 0 Basic 465.76 GB Online	63 ME Healtl	**RECOVERY Vi** 2.00 GB NTFS Healthy (Prim	**Vista x64 (D:)** 248.86 GB NTFS Healthy (System, Active,	**DATA (E:)** 214.84 GB NTFS Healthy (Logical Drive)
Disk 1 Basic 465.76 GB Online	**Windows 7 (C:)** 195.31 GB NTFS Healthy (Boot, Page File, Crash Dum	**SERVER 2008 (G:)** 270.45 GB NTFS Healthy (Primary Partition)		
Disk 2 Basic 698.64 GB Online	**MY BOOK (I:)** 698.63 GB NTFS Healthy (Primary Partition)			
Disk 3 Basic 18.52 GB Online	**New Volume (J:)** 18.52 GB NTFS Healthy (Primary Partition)			

■ Unallocated ■ Primary partition ■ Extended partition ■ Free space ■ Logical drive

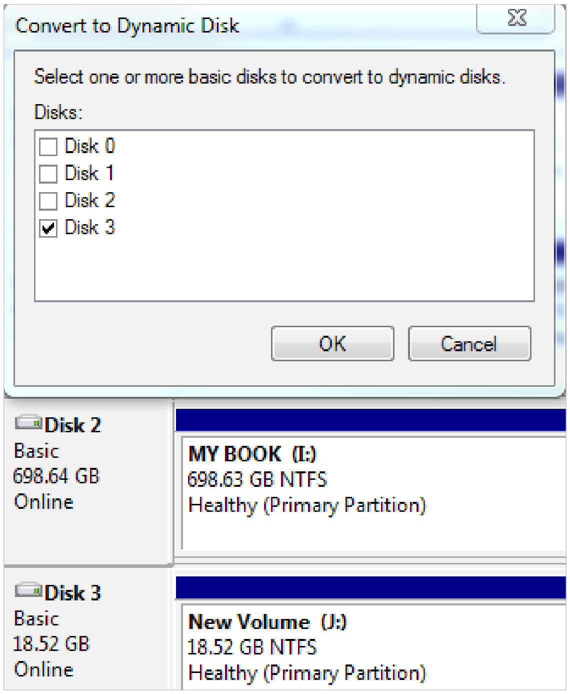
Figure 79: A Newly Created Volume

The summary below outlines the available volume types:

- **Simple Volume** – made up of the free space from a single disk and can be extended within the same disk or onto additional disks. Once a simple volume is extended to at least one additional disk it becomes a spanned volume.
- **Spanned Volume** – created from free disk space linked together from at least one additional disk. Windows allows you to extend a spanned volume across a maximum of 32 physical disks. A spanned volume is not a fault-tolerant design.
- **Stripped Volumes** (also called RAID 0 Volumes) – written and read across at least two or more physical disks. Striped volumes cannot be mirrored or extended and because no parity information is kept, these configurations are not fault-tolerant.
- **Mirrored Volumes** (or RAID 1 Volumes) – these are fault-tolerant. If one of the disks fails, the data can still be accessed from the remaining disk and when the drive is replaced, parity can be rebuilt from the remaining disk. A mirrored volume cannot be extended.
- **RAID-5 –** a fault-tolerant volume configuration made up of at least three physical disks. The data and the parity information is written across this configuration in such a way that if a physical disk fails, the portion of the RAID-5 volume that was on that failed disk can be pulled from the remaining disk, with parity restored by the parity volume. This allows for a single disk in the array to fail without the loss of data. When the failed drive is replaced the full data can be re-written to the new disk. RAID-5 volumes cannot be mirrored or extended.

- **Boot Volume** – contains the Windows operating system files that are located in the %systemroot% and %Systemroot%System32 folders. The boot volume can be the same volume as the system volume. It is often the case when there is a single volume in the system (C:\ only).
- **System Volume** – contains the hardware-specific start up files that are needed to load Windows such as the Windows Boot Manager and the Windows Boot Loader.

Once you make the decision to convert a disk to Dynamic disk, you only need to open the wizard by right clicking the drive and choosing the basic disk that you want to convert. Then, follow the prompts.



Convert to Dynamic Disk

Select one or more basic disks to convert to dynamic disks.

Disks:

□ Disk 0
□ Disk 1
□ Disk 2
☑ Disk 3

Disk 2
Basic
698.64 GB
Online

MY BOOK (I:)
698.63 GB NTFS
Healthy (Primary Partition)

Disk 3
Basic
18.52 GB
Online

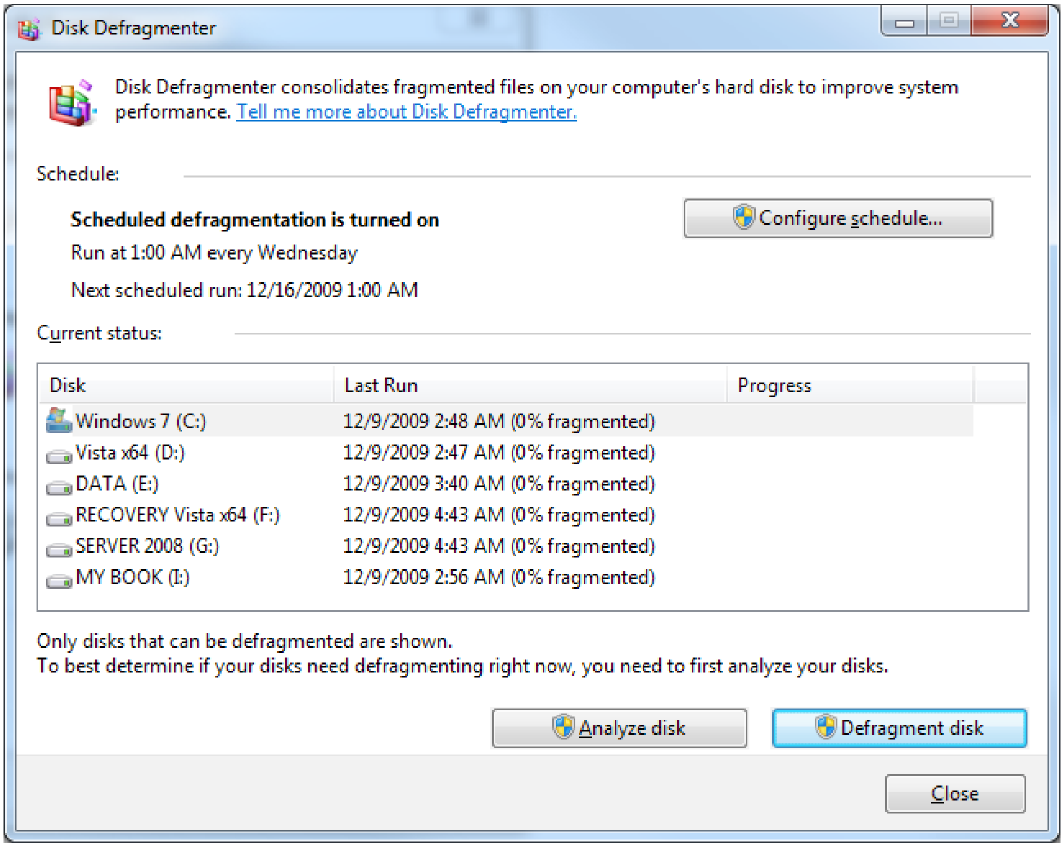
New Volume (J:)
18.52 GB NTFS
Healthy (Primary Partition)

Figure 80: Converting a Basic Disk to a Dynamic Disk

Another part of managing disks includes dealing with file system fragmentation. Fragmentation occurs over time as files are saved, changed, and deleted from disk.

The Windows I/O Manager is configured to attempt to saves files in contiguous areas on a volume for the sake of efficiency. As the free space on a volume fills up, contiguous areas of free-space large enough to fit data being written becomes harder to do. When there is not enough contiguous free-space available, that condition forces the I/O manager to save the data remnants to a non-contiguous area of the disk. This is the resulting condition known as file fragmentation.

Disk defragmentation simply moves data around on the disk so that it is more optimally stored.
The Disk Defragmenter on Windows 7 runs automatically on a scheduled basis; you can also perform manual defragmentation if you want or need to. This action can be taken from the Tools tab of the property page for the given drive.



Disk Defragmenter

Disk Defragmenter consolidates fragmented files on your computer's hard disk to improve system performance. Tell me more about Disk Defragmenter.

Schedule:

Scheduled defragmentation is turned on

Run at 1:00 AM every Wednesday

Next scheduled run: 12/16/2009 1:00 AM

Current status:

Disk	Last Run	Progress
Windows 7 (C:)	12/9/2009 2:48 AM (0% fragmented)	
Vista x64 (D:)	12/9/2009 2:47 AM (0% fragmented)	
DATA (E:)	12/9/2009 3:40 AM (0% fragmented)	
RECOVERY Vista x64 (F:)	12/9/2009 4:43 AM (0% fragmented)	
SERVER 2008 (G:)	12/9/2009 4:43 AM (0% fragmented)	
MY BOOK (I:)	12/9/2009 2:56 AM (0% fragmented)	

Only disks that can be defragmented are shown.
To best determine if your disks need defragmenting right now, you need to first analyze your disks.

Figure 81: Windows 7 Disk Defragmentation Tool

If you need to disable automatic defragmentation, hit the **Configure schedule** button and clear the **Run on a schedule** checkbox. This is the same location where you would modify the defragmentation schedule and / or choose the volumes you want to defragment. When you have a need for a striped volume (RAID 0), you can create it from the Disk Management MMC from any of the dynamic disks that you have on your system.

1. Open **Disk Management** and **right-click** a free-space segment that you want to include in the striped volume; click **New Striped Volume,** starting the wizard.
2. On the Select Disks page you would need to select from the available disks and then click Add to add the disks to the striped volume.
3. Additionally you would need to specify the amount of space to use on the disks for the striped volume.
4. On the **Assign Drive Letter or Path** page you can keep the default setting to assign the next available drive letter to the new volume. (You have the option to mount the volume on an empty NTFS folder on an existing volume as well).
5. On the Format Volume page of the New Striped Volume Wizard you can choose the formatting options for the new volume. Windows 7 supports only NTFS formatting from the Disk Management snap-in.

If you need to format with FAT or FAT32, you'll have to use diskpart from the command line:

```
FORMAT FS=FAT32 LABEL="New Volume" QUICK COMPRESS
```

To create the RAID 0 disk, enter the following at the DISKPART> prompt:

```
DISKPART> prompt: create volume stripe [size=<n>]
disk=<n>[,n[,..]]
```

The total size of the stripe volume is the size multiplied by the number of disks.

For RAID 1 configurations, the steps are pretty much the same. The difference is that you right-click the first disk of your mirror and click New Mirrored Volume to kick off the wizard and then select the second disk. In this scenario you need to have an equal or greater amount of unallocated disk space on that second disk to create the mirror.

The Diskpart tool can also be used to create a mirrored volume. While RAID 1 configurations allow you the benefit of fault tolerance their disadvantage is that you lose 50% of your possible total free space in achieving that redundancy.

RAID 5 requires at least three disks where RAID 0 and RAID 1 only required two. (RAID 0 needs **at least two**; RAID 1 configurations **require** two). When you create a RAID 5 volume, it is set up similarly to RAID 0, with one exception. On each physical disk, some of the capacity is reserved to store parity information about the contents of the other disks in the set. This information is stored in a compressed state. If and when a disk fails, the parity information is decompressed and leveraged so that all of the data can be accessed the same way as if the disk failure never occurred.

You create your RAID 5 volume on your system the same way you would RAID 0 in the Disk Management MMC except that you right-click the first disk with unallocated space and click New RAID-5 Volume to start that wizard. You then select the remaining disks in the set and specify the size of the volume. Equal portions of unallocated space on each disk will be used by default. From there you then specify the drive letter or mount point and the formatting option. You can also use the Diskpart tool to create a RAID-5 volume by entering the following syntax at the DISKPART> prompt:

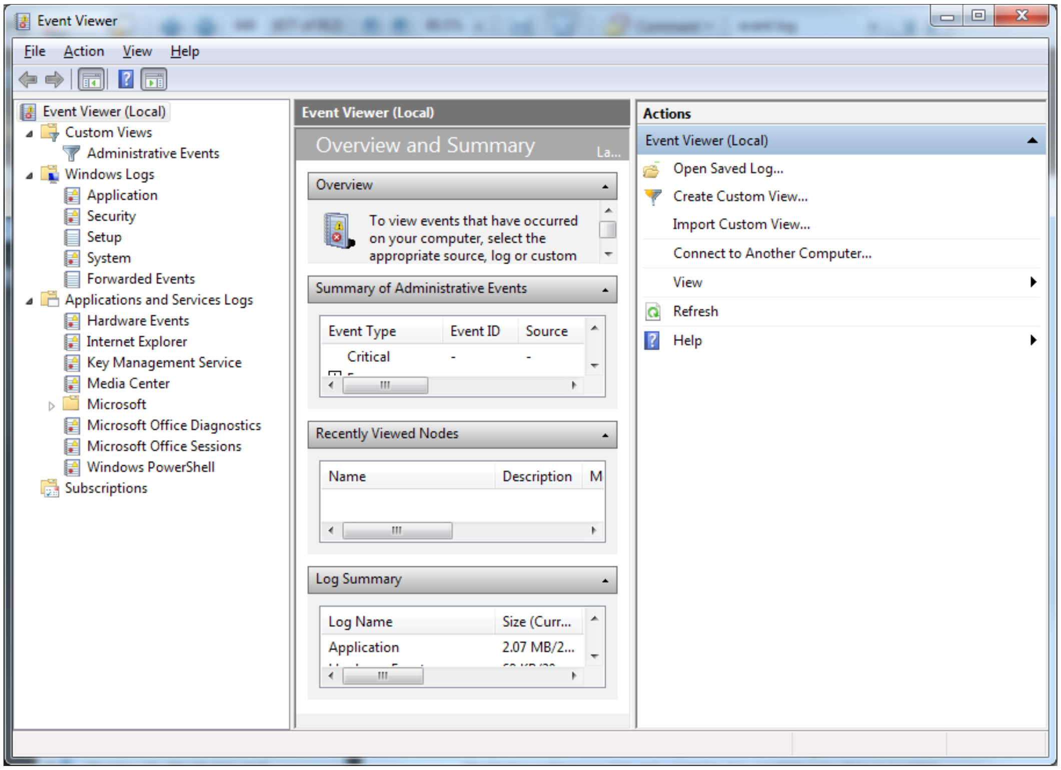
```
create volume raid [size=<n>] disk=<n>[,n[,..]]
```

Monitor Systems and Configure Performance Settings

Configure and Administer Event Logging

As part of the process of managing systems in your Windows 7 systems you may need to troubleshoot problems affecting system performance and one of the best ways to start this task is to review any events that appear in the Event Viewer logs.

You can launch the Event Viewer as part of the Computer Management MMC or in its own stand alone MMC.



To view events that have occurred on your computer, select the appropriate source, log or custom

Event Type	Event ID	Source
Critical	-	-

Name	Description	M

Log Name	Size (Curr...
Application	2.07 MB/2...

Figure 82: Windows 7 Event Viewer

You'll notice that on Windows 7 systems, by default, there are five Windows logs: Application, Security, Setup, System and Forwarded Events.

Application or program events are logged in the **Application Log** which will contain any errors, warning, or informational alerts as processed by the system. A logged error is usually a noteworthy event that would otherwise need to be addressed especially in the situation where it re-occurs regularly. A logged warning event might not necessarily need to be addressed, especially if it is a one off occurrence, but repeated warnings are usually an indication of a building condition that may impact performance down the line. An information event is just a notification of a noteworthy item and generally will not require any response or any administrative action.

Security-related events are logged audit events that are recorded in the **Security Log** which will identify failed or successful actions of a security activity such as authenticating to the system or accessing restricted share or the failure to complete these actions successfully.

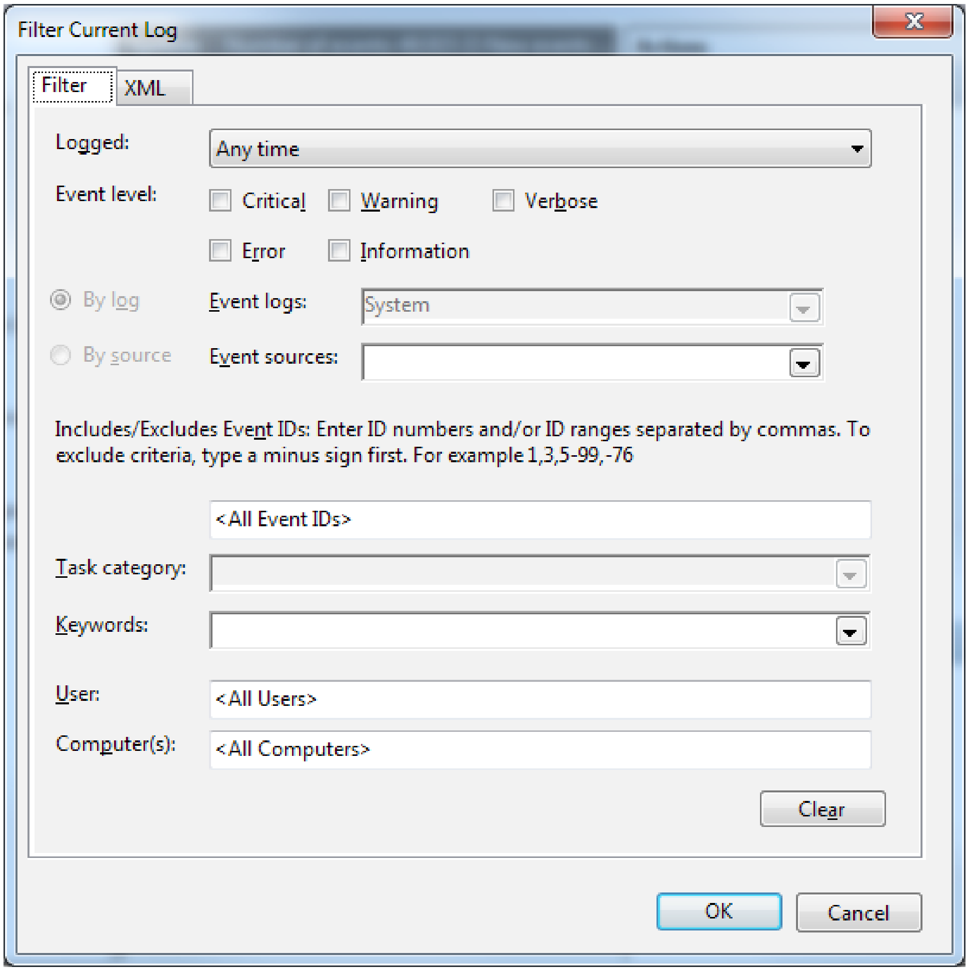
Setup events are recorded in the **Setup Log** and can be a combination of many different activities logged from system actions from initiating changes to be performed with the rollout of an update on the system to program installs that require a system restart and so forth.

System events are logged in the **System Log** by the Windows system services and the operating system itself and are classified as error, warning, or informational messages. These messages are handled much in the same way as their counterparts in the Application Log.

Events that are logged in one system and forwarded to another system for review are called forwarded events and are kept in the **Forwarded Events Log.**

Understanding the Details and Use of Filtering Event Logs

Log filtering is performed when you want to view only certain logged events, such as only Warning event levels. Simply select the appropriate log and then select **Filter Current Log** from the action pane. You can create a custom filtered log, containing events from any of Windows' logs by clicking **Create Custom View** from the action pane.



Filter Current Log

Filter | XML

Logged: Any time

Event level: □ Critical □ Warning □ Verbose □ Error □ Information

● By log Event logs: System

○ By source Event sources:

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

<All Event IDs>

Task category:

Keywords:

User: <All Users>

Computer(s): <All Computers>

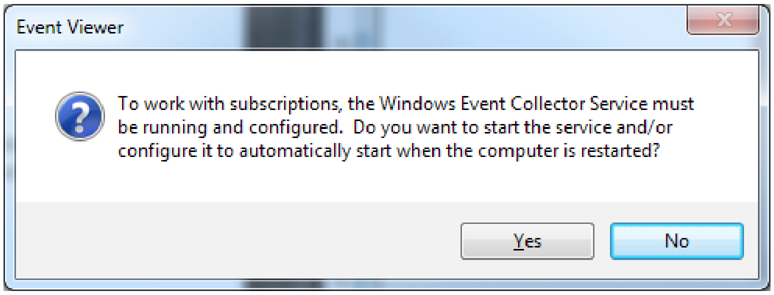
Figure 83: Creating a Filter

You can choose multiple event levels by selecting more than one of the available check boxes - Critical, Warning, Verbose, Error, and / or Information. You can also limit the scope of the logged events by time. The default setting is "Any time".

Configuring and Administering Event Subscriptions

To receive forwarded events on a computer, you can set up subscriptions by configuring the computer that will receive the forwarded events and the computer or computers that will be forwarding events. Once the systems are correctly configured you can create a subscription to specify which events to collect.

1. Open the Event Viewer as an administrator and choose Subscriptions in the console tree.
2. If the Windows Event Collector service is not started, you will be prompted to confirm that you want to start it. You must be a member of the Administrators group to start this service.



Event Viewer

To work with subscriptions, the Windows Event Collector Service must be running and configured. Do you want to start the service and/or configure it to automatically start when the computer is restarted?

Figure 84: Starting the Windows Event Collector Service

3. On the Actions menu, click **Create Subscription** and then go to the **Subscription Name** box to enter a common name for the subscription.
4. You can enter any optional description details at this point, if you like.
5. In the destination Log box, choose the log file where collected events are to be stored. This is the Forwarded Events log by default.
6. Select **Add** to choose the target systems from which events are to be collected.
7. You can then test connectivity to the remote computer by selecting the computer and clicking **Test**.
8. Select **Events** to display the **Query Filter** dialog box, where you can configure controls to specify any criteria that events must meet to be collected.
9. Select **OK** on the Subscription Properties dialog box and the subscription is added to the Subscriptions pane. If the operation was successful, the subscription will be listed with a status of **Active**.
10. All of the Events logged on the target systems that meet listed criteria will be copied to the collector system's Forwarded Events log.

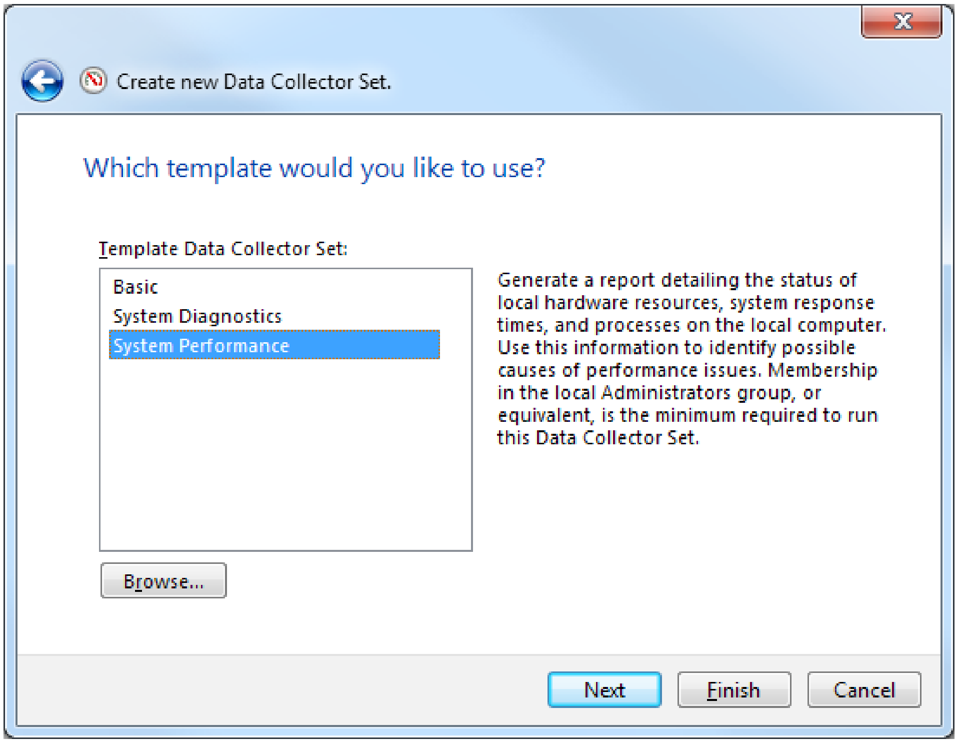
Configuring and Administering Data Collector Sets

As the administrator of the system you will need to use **Data Collector Sets** to organize collected data for review in the Performance Monitor. Collected data can also be used to generate alerts when upper or lower thresholds are reached. Data Collector Sets will generally contain Performance counter information, Event trace data, and system configuration information from registry key values.

You can create your own Data Collector Set. Or, Windows provides several preconfigured templates that focus on performance data and/or general system diagnosis information or based on server roles deployed on the system.

To create a Data Collector Set from Performance Monitor:

1. Open Performance Monitor.
2. Right click the **Data Collector Sets** → **User Defined** node, select **New**, and then choose **Data Collector Set**. This will start the **Create New Data Collector Set Wizard**.
3. Choose a name for your Data Collector Set and click **Next**.
4. You have the option to create the collection from a template or to create what you need manually. Using the template is recommended.



Create new Data Collector Set.

Which template would you like to use?

Template Data Collector Set:

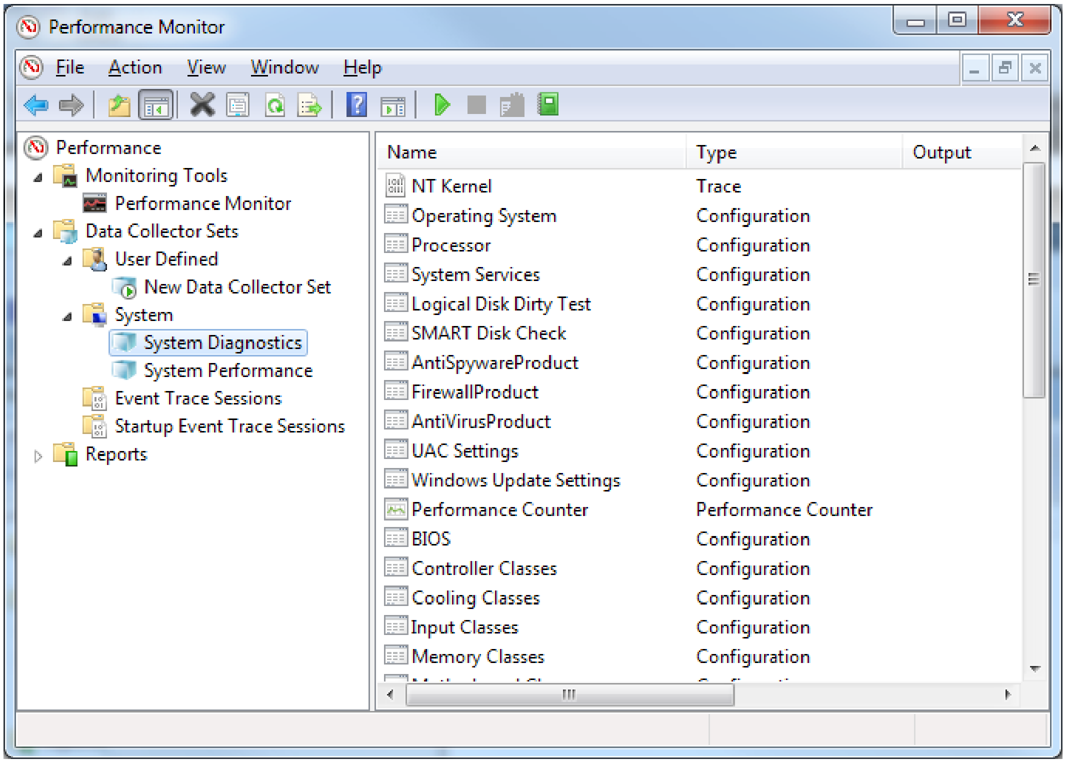
- Basic
- System Diagnostics
- System Performance

Generate a report detailing the status of local hardware resources, system response times, and processes on the local computer. Use this information to identify possible causes of performance issues. Membership in the local Administrators group, or equivalent, is the minimum required to run this Data Collector Set.

Figure 85: Selecting a Data Collector Set Template

5. Once you choose a template, select **Next** to continue.
6. You'll need to choose a location to save the data. The default location is **%systemdrive%\PerfLogs\Admin\New Data Collector Set**. It's recommended to rename the directory. Click **Next**.
7. Next, define a specific user account for the Data Collector Set to run as (or you can leave it as default.)
8. Before you click **Finish** to save your current settings and exit the wizard, you may choose to save the data collector set, start the data collector set running, or open the properties of the data collector set.
9. If you choose to start the data collector set, you'll notice it running when the wizard closes.

If you do not wish to create your own Data Collector Set, you can use one of the predefined sets in the system. In the console tree, expand **Data Collector Sets**, then expand **System** and choose one of the sets provided.



Name	Type	Output
NT Kernel	Trace	
Operating System	Configuration	
Processor	Configuration	
System Services	Configuration	
Logical Disk Dirty Test	Configuration	
SMART Disk Check	Configuration	
AntiSpywareProduct	Configuration	
FirewallProduct	Configuration	
AntiVirusProduct	Configuration	
UAC Settings	Configuration	
Windows Update Settings	Configuration	
Performance Counter	Performance Counter	
BIOS	Configuration	
Controller Classes	Configuration	
Cooling Classes	Configuration	
Input Classes	Configuration	
Memory Classes	Configuration	

Figure 86: Predefined Data Collector Sets

To start the data collector set, right click the appropriate set and choose **Start**. Once the data collection is completed you are able to review it either in report form or you can view the results right in the Performance Monitor as a graphical representation of the data collected.

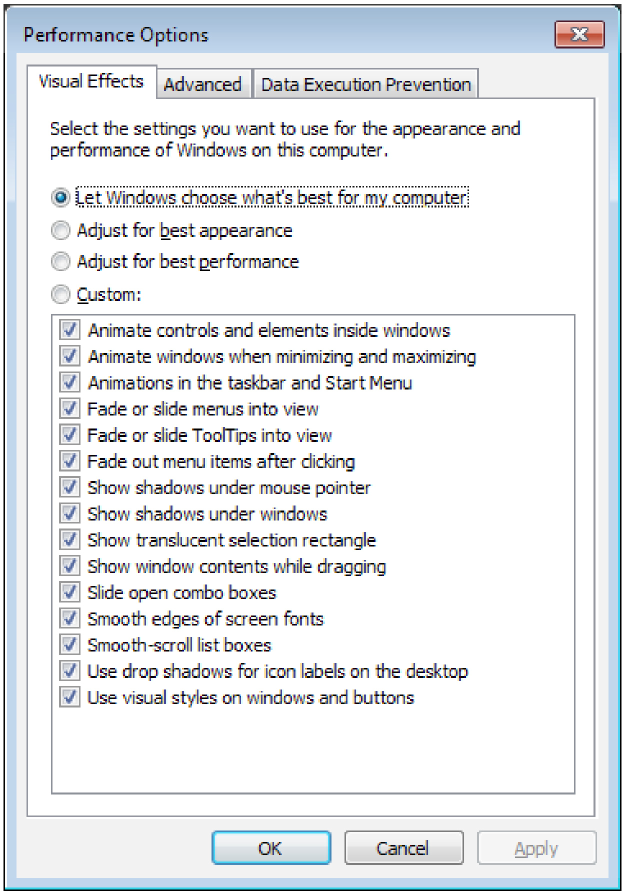
Configure Performance Settings

Windows 7 provides some native tools to display and reconfigure performance settings and resolve performance issues and you can also leverage Windows Management Instrumentation (WMI) scripts to write your own as needed / desired.

There are a number of tools that Windows 7 provides and each performs a different function of helping an administrator review a system's current performance.

Tool	**Use**
Performance Information	Lists information for speed and performance
Performance Monitor	Multiple graph views of performance
Resource Monitor	Monitor use and system Performance
Windows Experience Index	Measure the computer's key components
Monitoring Tools	Performance Monitor
Data Collector Set	Performance Counters / Event traces
Windows Memory Diagnostic	Check system memory problems
Fix a Network Problem	Network Troubleshooter
Reliability Monitor	Reviews reliability and problem history
Problem Reports and Solution Tool	Checks for solutions to problem reports
Startup Repair Tool	Scan the computer for startup problems
Backup and Restore Tool	Back up or restore user / system data
Image Backup	A copy of the drivers for the system
System Repair Disc	Used to start the computer
System Restore	Restore the computer to an earlier point in time
Previous Versions of Files	Copies of files / folders
Restore Point	A stored state of the computers system files
Disc Space Usage	Maximum disk space used for system protection
Windows Update	Service that provides software updates
Change Update Settings	Settings for windows update
View Update History	Review the computers update history

The Performance Options tool can be accessed by clicking Advanced Tools on the Performance Information and Tools dialog box. Finally, click **Adjust the appearance and performance of windows**.



Select the settings you want to use for the appearance and performance of Windows on this computer.

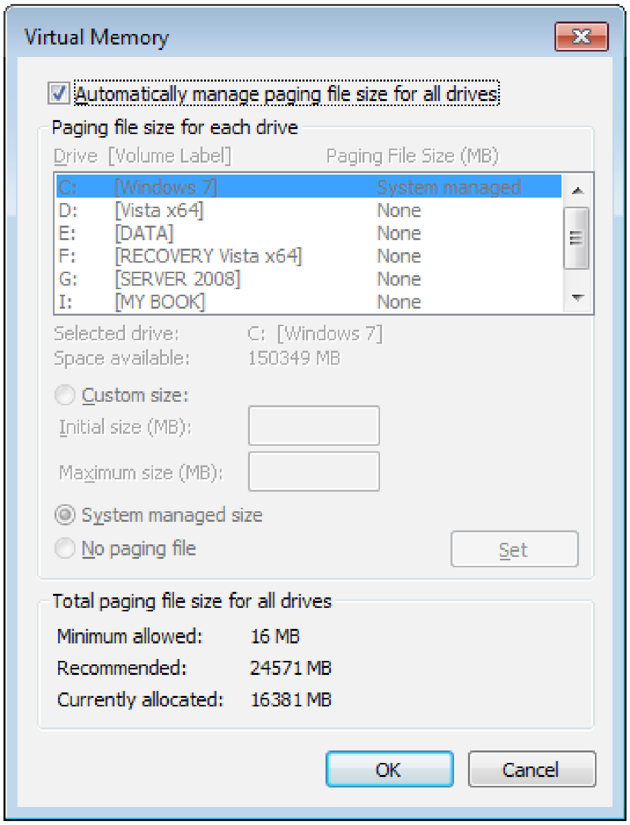
● Let Windows choose what's best for my computer
○ Adjust for best appearance
○ Adjust for best performance
○ Custom:

☑ Animate controls and elements inside windows
☑ Animate windows when minimizing and maximizing
☑ Animations in the taskbar and Start Menu
☑ Fade or slide menus into view
☑ Fade or slide ToolTips into view
☑ Fade out menu items after clicking
☑ Show shadows under mouse pointer
☑ Show shadows under windows
☑ Show translucent selection rectangle
☑ Show window contents while dragging
☑ Slide open combo boxes
☑ Smooth edges of screen fonts
☑ Smooth-scroll list boxes
☑ Use drop shadows for icon labels on the desktop
☑ Use visual styles on windows and buttons

Figure 87: Performance Options

On the Visual Effects tab, you can see that the default setting is **Let Windows Choose what's best for my computer**. You also have the option to adjust settings for best appearance or best performance. You may also set up a custom configuration by clearing desired checkboxes.

On the Advanced tab you can select the options for Processor scheduling. The default selection is shown above as set for Programs although you can elect to change it to background services as applicable. From this tab as well you can view and control the settings for virtual memory by selecting the Change button in the virtual memory section.



Virtual Memory

☑ Automatically manage paging file size for all drives

Paging file size for each drive

Drive	[Volume Label]	Paging File Size (MB)
C:	[Windows 7]	System managed
D:	[Vista x64]	None
E:	[DATA]	None
F:	[RECOVERY Vista x64]	None
G:	[SERVER 2008]	None
I:	[MY BOOK]	None

Selected drive: C: [Windows 7]
Space available: 150349 MB

○ Custom size:
Initial size (MB):
Maximum size (MB):
● System managed size
○ No paging file

Total paging file size for all drives

Minimum allowed:	16 MB
Recommended:	24571 MB
Currently allocated:	16381 MB

Figure 88: Configuring Virtual Memory

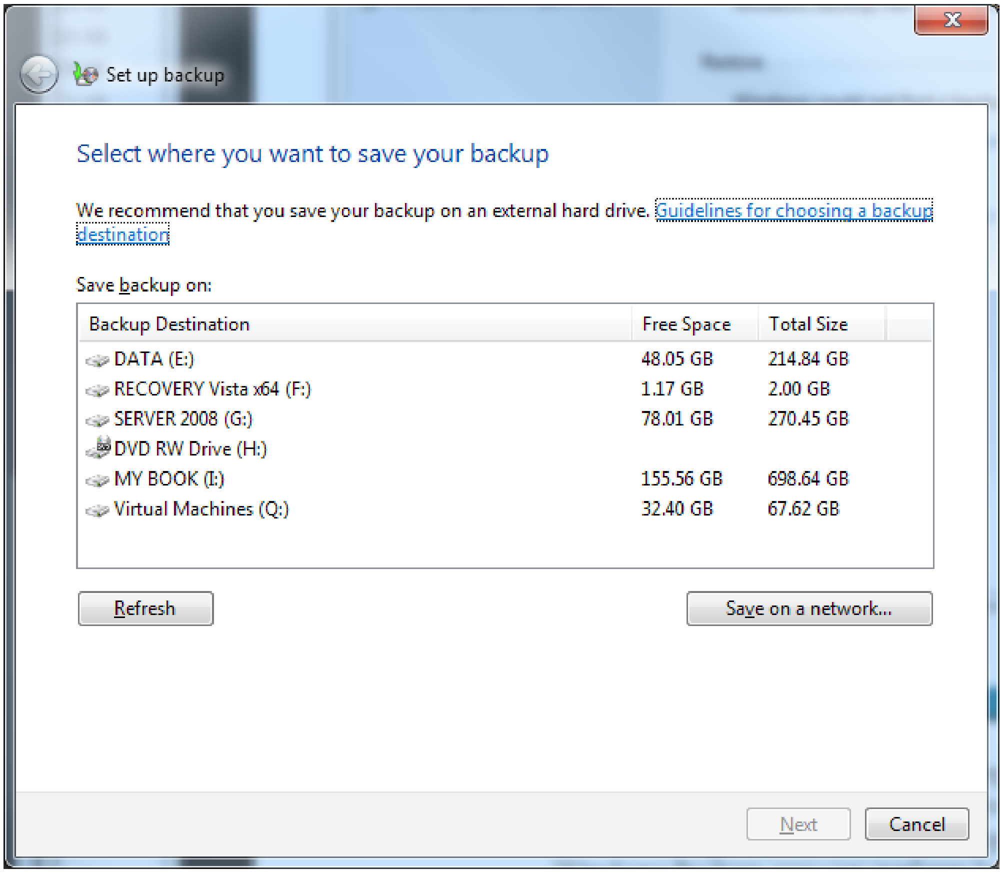
If your installed processor(s) support Data Execution Prevention you can enable that on the Data Execution Prevention (DEP) tab. Data Execution Prevention (DEP) is a security feature that is used to try to prevent damage to the installed operating system from poorly coded programs, viruses, malware and other security threats.

In one form or another, these programs intentionally attack the operating system by attempting to run their code from within RAM that is otherwise reserved for the operating system and other protected programs. DEP monitors programs to make sure that they use computer memory in an expected fashion. If DEP notices a program using memory that should otherwise be off limits, it will force the program to close and notifies you through a pop-up dialog in the system tray.

Domain Eight: Configuring Backup and Recovery Options

Configure Backup

Windows has tools available to allow you to back up your files and folders and to recover your system in the event of a failure. You can find the backup tool by navigating to: **Control Panel** → **System and Security** → **Backup and Restore**. Once launched, you have the option to create a backup, a system image or a system repair disk.



Select where you want to save your backup

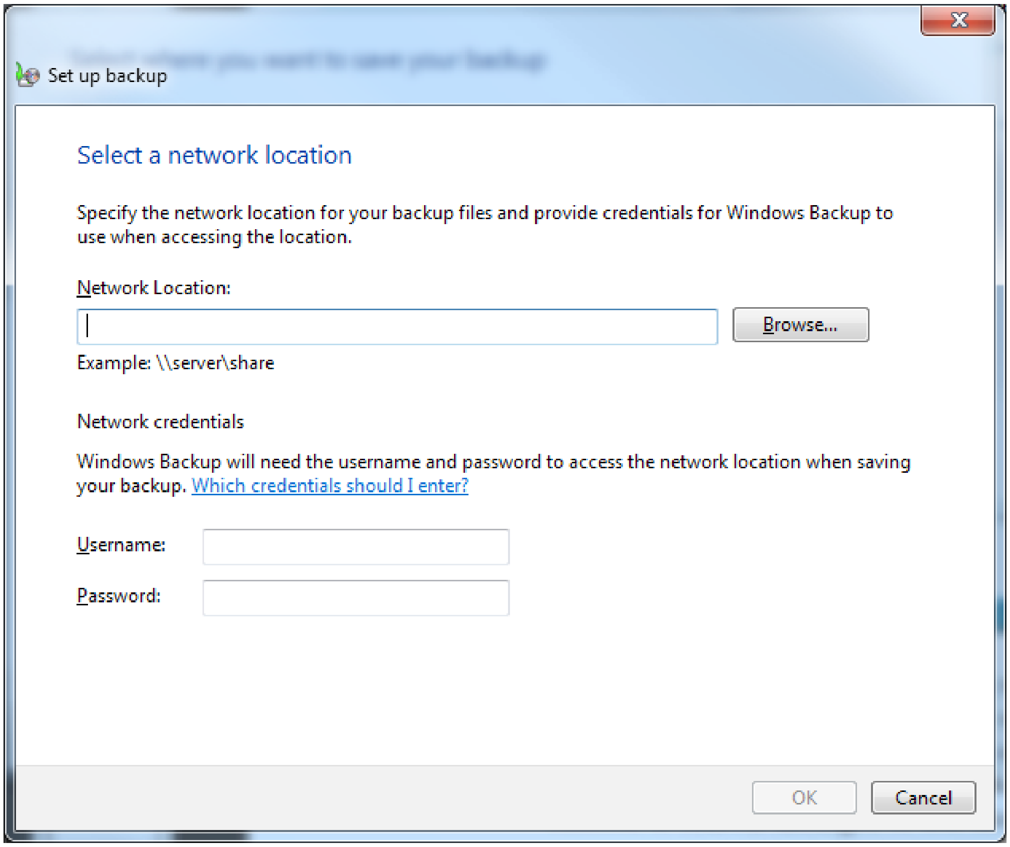
We recommend that you save your backup on an external hard drive. Guidelines for choosing a backup destination

Save backup on:

Backup Destination	Free Space	Total Size
DATA (E:)	48.05 GB	214.84 GB
RECOVERY Vista x64 (F:)	1.17 GB	2.00 GB
SERVER 2008 (G:)	78.01 GB	270.45 GB
DVD RW Drive (H:)		
MY BOOK (I:)	155.56 GB	698.64 GB
Virtual Machines (Q:)	32.40 GB	67.62 GB

Figure 89: Creating a Backup

When you run the backup utility, you'll have the option to save your backup to any attached or network storage locations available. Choose one of the provided destinations and click **Next**, or select **Save on a network**. This will open a further dialogue box requiring you to enter a path and credentials, as needed.



Select a network location

Specify the network location for your backup files and provide credentials for Windows Backup to use when accessing the location.

Network Location:

Example: \\server\share

Network credentials

Windows Backup will need the username and password to access the network location when saving your backup. Which credentials should I enter?

Username:

Password:

Figure 90: Setting Up a Network Backup Location

Windows 7 helpfully evaluates any backup location you choose for its viability. Pay attention to any messages. Adjust your location, as necessary, and continue.

Once you choose a location, the system will ask if you want to choose specific data to back up or to Let Windows choose, the default option. If you let Windows choose, the backup utility will automatically include data files that are saved on the local system in libraries, on the desktop, and in default Windows folders for all people with a user account on the computer. Those default Windows folders include:

- AppData
- Contacts
- Desktop
- Downloads
- Favorites
- Links
- Saved Games
- Searches

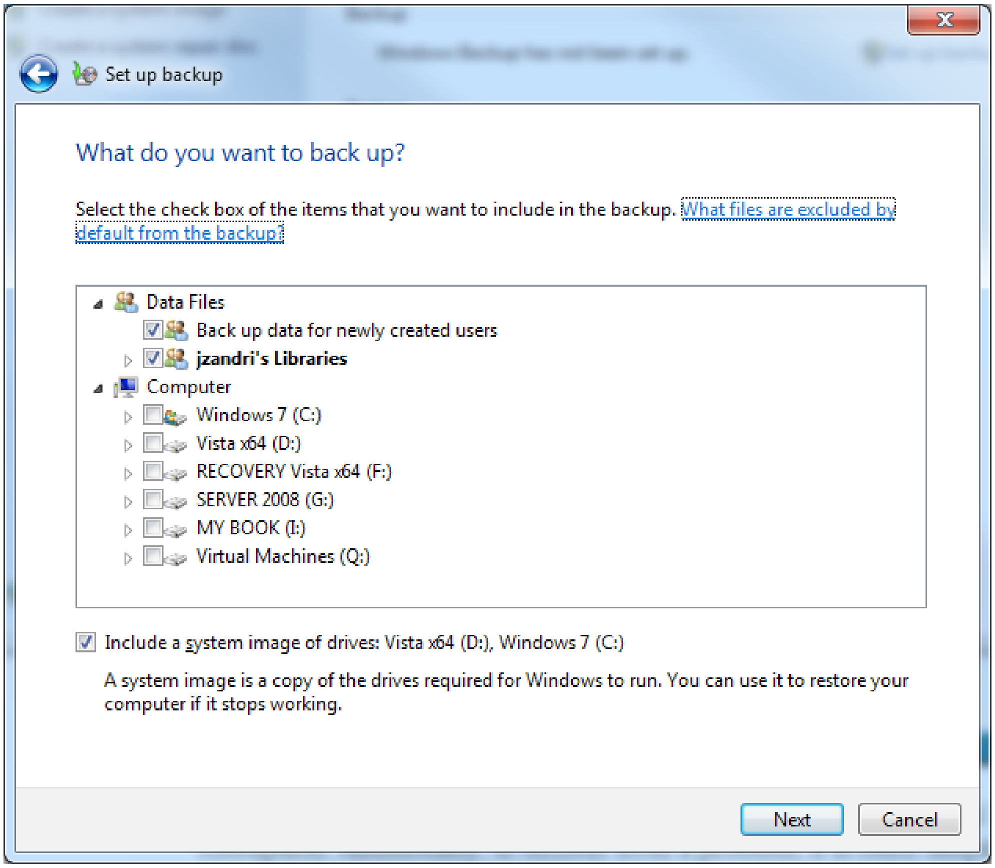
If the location you're saving the backup to is formatted with NTFS and has enough free space, the backup routine will also capture a system image of your programs, the Windows operating system, and all drivers and registry settings. This image can be used to restore the contents of your computer back to the state that the system was in at the time the backup was run.

When you restore your system from a system image, you can't choose individual items to restore: it's an all or nothing operation. All of your installed programs, system settings, and files are replaced with the contents of the system image.

A system image backup will include personal files, but Windows Backup should be configured to back up data and information in a separate back up so that you can restore just those individual files and folders on demand and as needed. Windows Backup won't back up the following items:

- Program files.
- Files stored on hard disks that are formatted using the FAT file system.
- Files that are in the Recycle Bin.
- Temporary files on drives smaller than 1 GB.

If you decided to use the Let me choose option, the backup routine will present you with a list of choices to make as shown in the example below:



Set up backup

What do you want to back up?

Select the check box of the items that you want to include in the backup. What files are excluded by default from the backup?

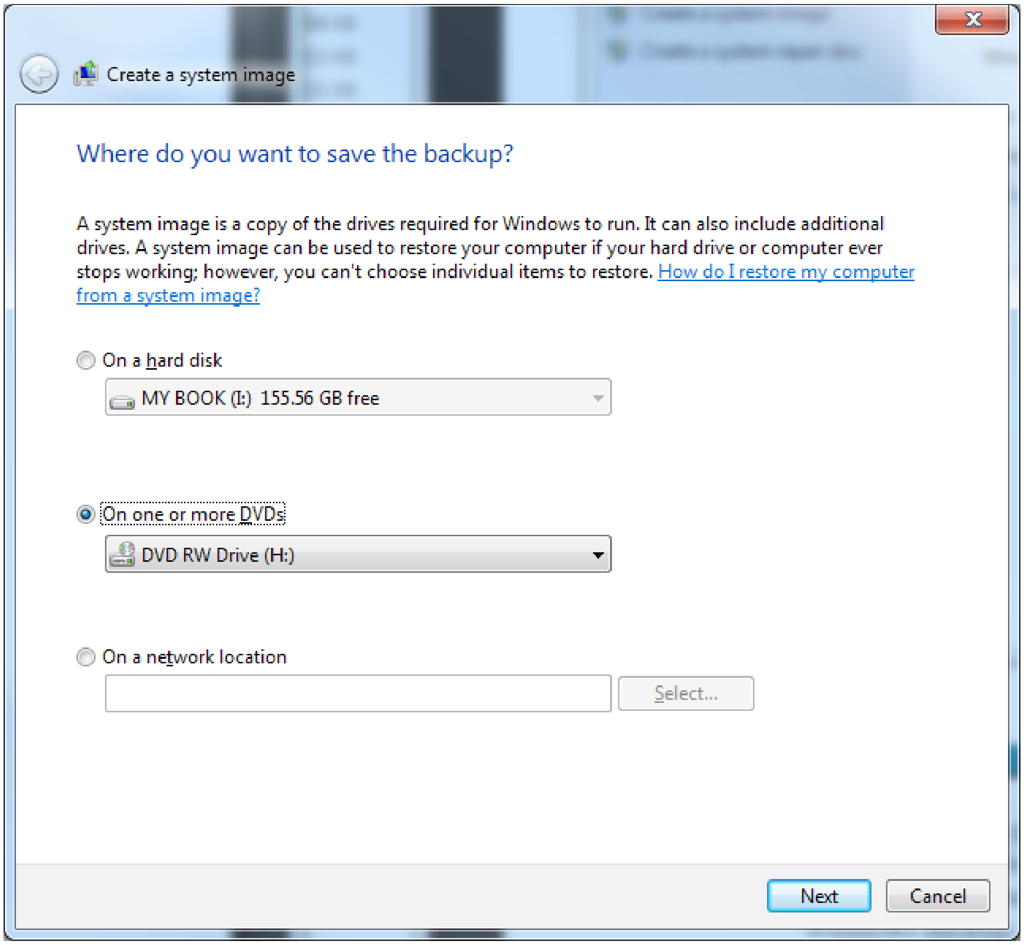
- Data Files
  - ☑ Back up data for newly created users
  - ☑ **jzandri's Libraries**
- Computer
  - □ Windows 7 (C:)
  - □ Vista x64 (D:)
  - □ RECOVERY Vista x64 (F:)
  - □ SERVER 2008 (G:)
  - □ MY BOOK (I:)
  - □ Virtual Machines (Q:)

☑ Include a system image of drives: Vista x64 (D:), Windows 7 (C:)

A system image is a copy of the drives required for Windows to run. You can use it to restore your computer if it stops working.

Figure 91: Selecting Folders and Files for Backup

You'll notice there are some items already selected, by default; you can add to and remove from these as desired. You may also include a system image, if you desire, from this page. Alternately, you may elect to create a system image from the link on the left side of the main Backup and Restore window. If you elect to create a system image, clicking Next will produce the following screen:


Create a system image

Where do you want to save the backup?

A system image is a copy of the drives required for Windows to run. It can also include additional drives. A system image can be used to restore your computer if your hard drive or computer ever stops working; however, you can't choose individual items to restore. How do I restore my computer from a system image?

○ On a hard disk

MY BOOK (I:) 155.56 GB free

● On one or more DVDs

DVD RW Drive (H:)

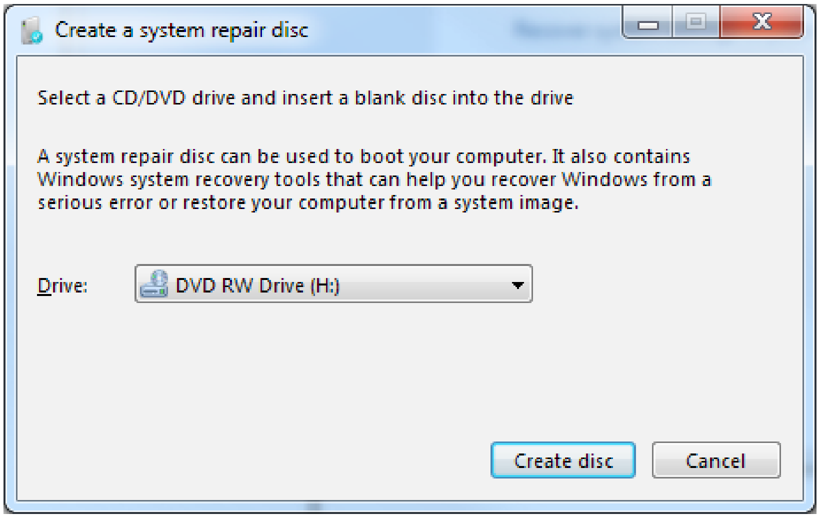
○ On a network location

Figure 92: Creating a System Image

You'll have the option to choose between locally attached storage and a network location. Once you choose a location for the backup and click **Next**, you'll see that the drives that are required to run Windows are already selected. You may choose other drives to add to the image, with the exception of the drive you are backing up to. Finally, you'll be asked to confirm your selections, with a message indicating the amount of space necessary for the backup.

In order to restore your computer from a system image, you need a system repair disk. This is another backup option available on the main Backup and Restore screen.

When you choose to create a system repair disk, you'll be required to insert blank, writable media, such as a DVD or CD, in order to copy the necessary files. Simply insert the disk, press "Create Disc" and let Windows complete the installation.



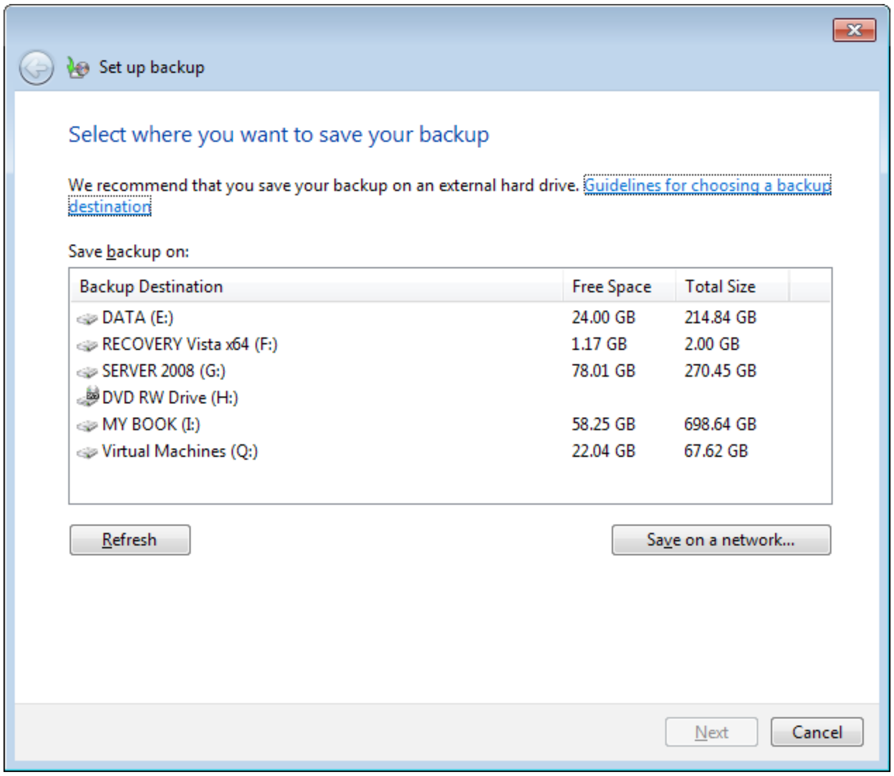
Select a CD/DVD drive and insert a blank disc into the drive

A system repair disc can be used to boot your computer. It also contains Windows system recovery tools that can help you recover Windows from a serious error or restore your computer from a system image.

Drive: DVD RW Drive (H:)

Figure 93: Creating a System Repair Disk

When you need to set up a schedule to regularly backup specific files and folders you can do so by going into the Control Panel and then to the System And Security center and clicking Back up your computer. The next screen is where you would select where you want to save your backup.



Select where you want to save your backup

We recommend that you save your backup on an external hard drive. Guidelines for choosing a backup destination

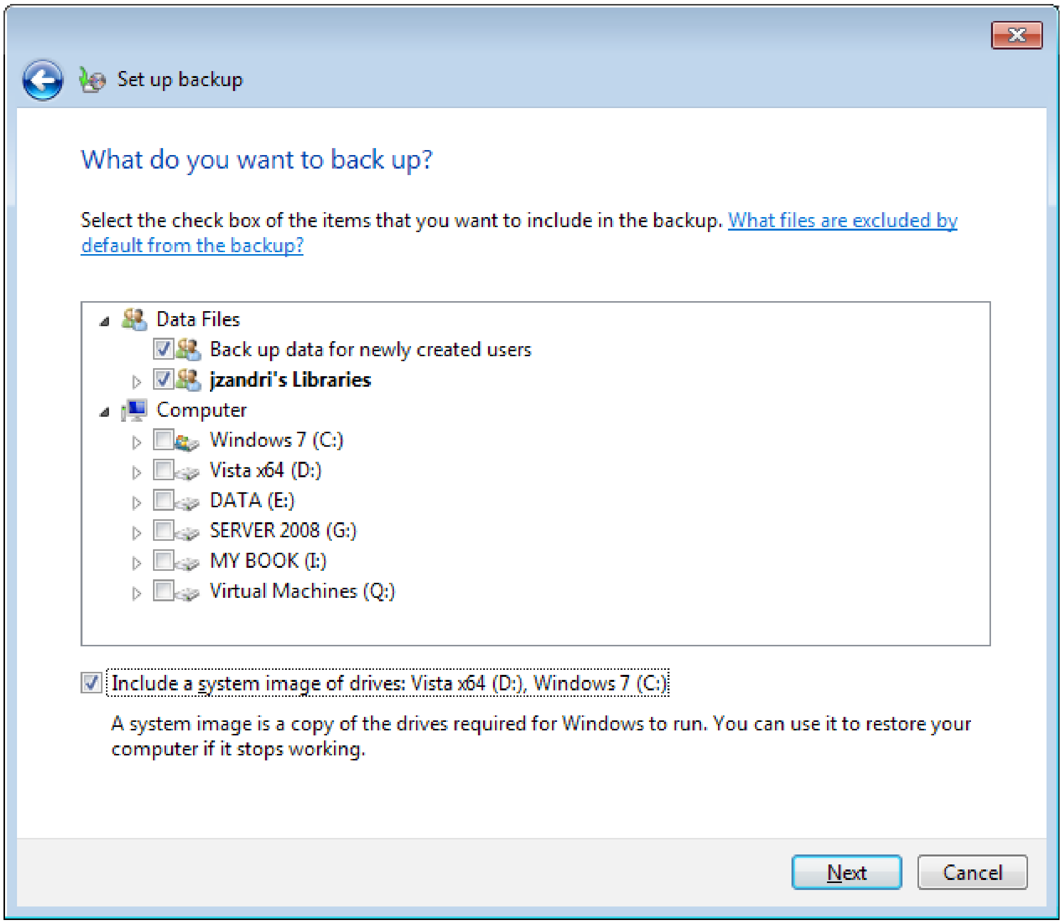
Save backup on:

Backup Destination	Free Space	Total Size
DATA (E:)	24.00 GB	214.84 GB
RECOVERY Vista x64 (F:)	1.17 GB	2.00 GB
SERVER 2008 (G:)	78.01 GB	270.45 GB
DVD RW Drive (H:)		
MY BOOK (I:)	58.25 GB	698.64 GB
Virtual Machines (Q:)	22.04 GB	67.62 GB

Figure 94: Saving a Backup

Once you choose a default location, click **Next** and you'll be provided with the default option to **Let Windows choose**. You can change to the Let me choose option to continue.

On the next page you can choose just those files and folders that you want to back up. As you can see from the defaults, the Libraries are selected for you as is the Include a system image of drives check box:



What do you want to back up?

Select the check box of the items that you want to include in the backup. What files are excluded by default from the backup?

- Data Files
  - ☑ Back up data for newly created users
  - ☑ **jzandri's Libraries**
- Computer
  - □ Windows 7 (C:)
  - □ Vista x64 (D:)
  - □ DATA (E:)
  - □ SERVER 2008 (G:)
  - □ MY BOOK (I:)
  - □ Virtual Machines (Q:)

☑ Include a system image of drives: Vista x64 (D:), Windows 7 (C:)

A system image is a copy of the drives required for Windows to run. You can use it to restore your computer if it stops working.

Figure 95: Selecting Files to Back Up

Once you make a choice of what it is that you want to back up you can complete the final step and execute the first scheduled backup of that process you just defined. When the backup is completed you'll see the status and the schedule on that page. If you need to change it you can select the Change Settings option which will allow you to walk through the entire process and the steps again to make the necessary changes.

Configure System Recovery Options

The System Restore Tool

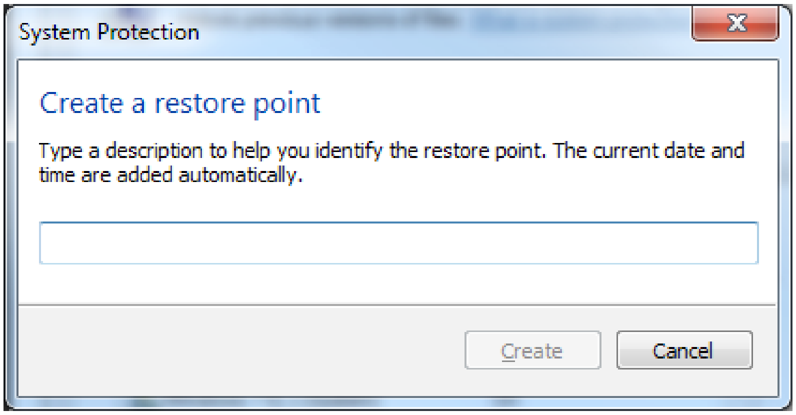
The System Restore tool and system restore points allow users to restore a system state to an earlier point in time. There is any number of reasons this might be done: a system crash, recovering from a poisoned update, a faulty device driver that might otherwise force you to do a reinstall of the operating system.

All system files and folders will be brought back to the saved point in time state they were in when the system restore point was created and will include the following settings by default:

- Registry
- Dllcache folder
- User profile
- COM+ and WMI information
- IIS metabase
- Certain monitored system files

There are a couple of ways to kick off the system restore process.

1. Go to the **Computer Properties** page and choose the **System Protection** option.
2. You'll land on the System Protection tab of the properties page.
3. If you want to manually create a restore point, click the **Create** button.
4. You'll need to assign a name to the restore point. Then, once more, click **Create**.



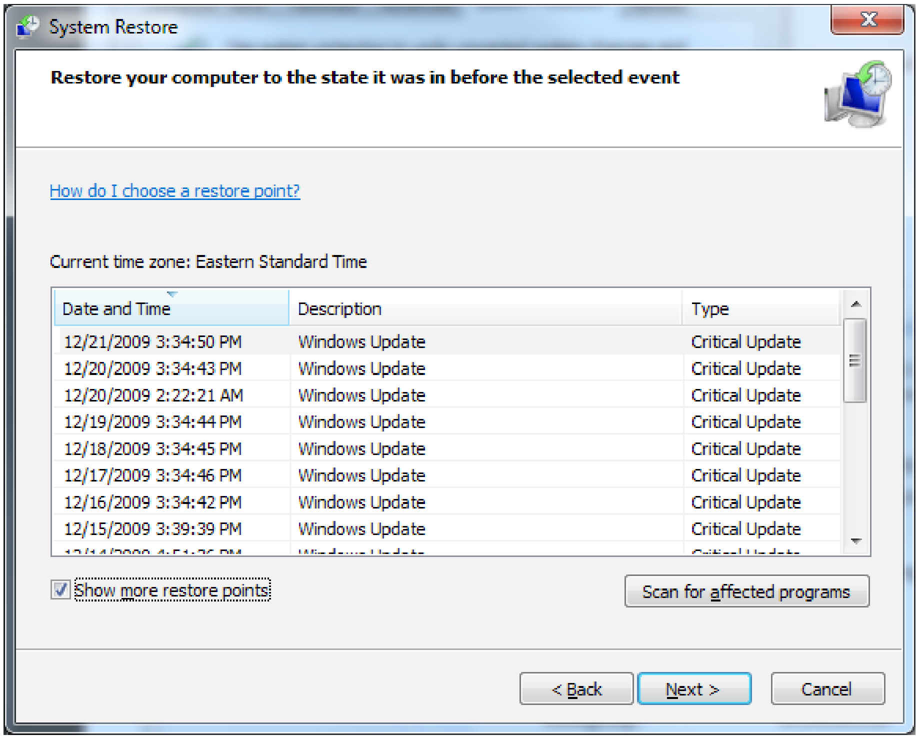
System Protection

Create a restore point

Type a description to help you identify the restore point. The current date and time are added automatically.

Figure 96: Creating a Restore Point

The system will also automatically create restore points through some software installations and all Windows updates.



System Restore

Restore your computer to the state it was in before the selected event

How do I choose a restore point?

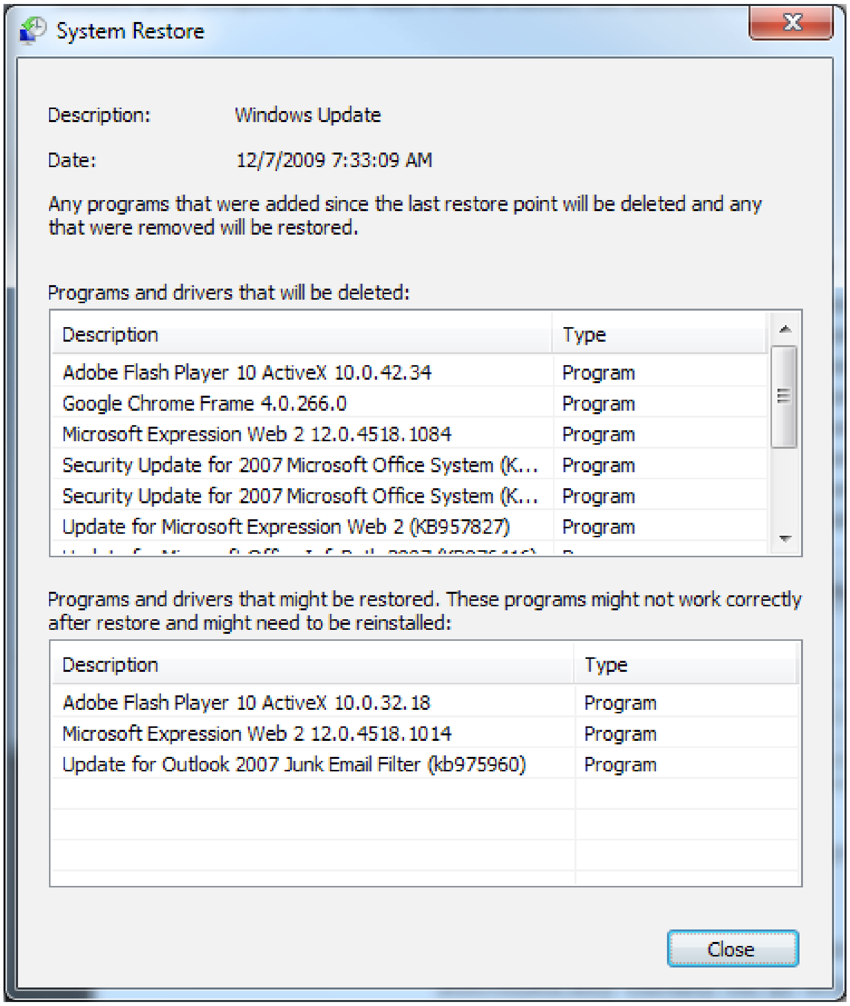
Current time zone: Eastern Standard Time

Date and Time	Description	Type
12/21/2009 3:34:50 PM	Windows Update	Critical Update
12/20/2009 3:34:43 PM	Windows Update	Critical Update
12/20/2009 2:22:21 AM	Windows Update	Critical Update
12/19/2009 3:34:44 PM	Windows Update	Critical Update
12/18/2009 3:34:45 PM	Windows Update	Critical Update
12/17/2009 3:34:46 PM	Windows Update	Critical Update
12/16/2009 3:34:42 PM	Windows Update	Critical Update
12/15/2009 3:39:39 PM	Windows Update	Critical Update
12/14/2009 4:51:36 PM	Windows Update	Critical Update

☑ Show more restore points

Figure 97: Automatically Created Restore Points

When you are choosing a restore point, you'll want to make sure to scan the affected programs that a restoration might impact by choosing that option from this page.



Description: Windows Update

Date: 12/7/2009 7:33:09 AM

Any programs that were added since the last restore point will be deleted and any that were removed will be restored.

Programs and drivers that will be deleted:

Description	Type
Adobe Flash Player 10 ActiveX 10.0.42.34	Program
Google Chrome Frame 4.0.266.0	Program
Microsoft Expression Web 2 12.0.4518.1084	Program
Security Update for 2007 Microsoft Office System (K...	Program
Security Update for 2007 Microsoft Office System (K...	Program
Update for Microsoft Expression Web 2 (KB957827)	Program

Programs and drivers that might be restored. These programs might not work correctly after restore and might need to be reinstalled:

Description	Type
Adobe Flash Player 10 ActiveX 10.0.32.18	Program
Microsoft Expression Web 2 12.0.4518.1014	Program
Update for Outlook 2007 Junk Email Filter (kb975960)	Program

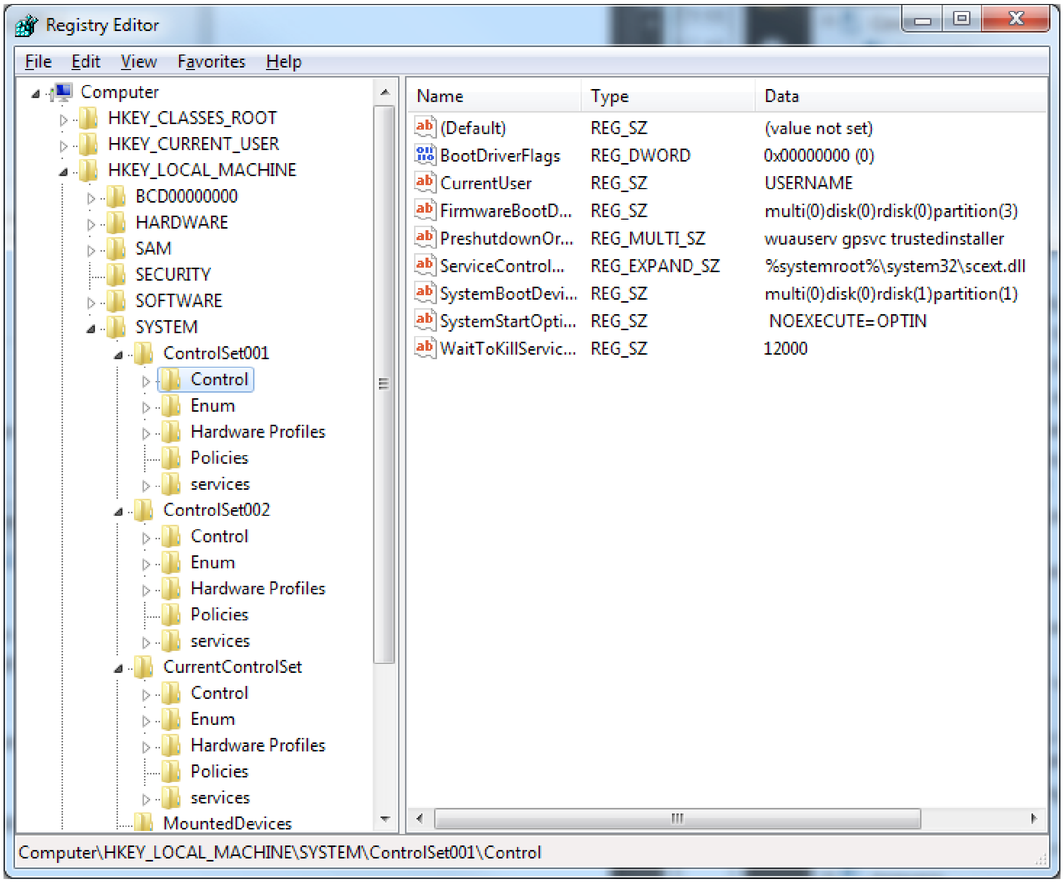
Figure 98: Programs and Features Affected by the System Restore

You can manage the settings for system restore from the System Properties tag by selecting the operating system drive and choosing **Configure**.

Understanding Last Known Good Configuration

Last Known Good Configuration is one of the Windows startup options that automatically will be available on crashed or improperly shut down Windows 7 systems. The option may also be brought up by hitting the F8 key during start up before the Windows logo appears. The Last Known Good Configuration startup option will attempt to use the last saved set of system settings that worked correctly.

When you are successfully log on to your Windows installation, your current configuration in ControlSet001 in the registry is copied to CurrentControlSet and becomes the Last Known Good Configuration.



```
Computer
  HKEY_CLASSES_ROOT
  HKEY_CURRENT_USER
  HKEY_LOCAL_MACHINE
    BCD00000000
    HARDWARE
    SAM
    SECURITY
    SOFTWARE
    SYSTEM
      ControlSet001
        Control
        Enum
        Hardware Profiles
        Policies
        services
      ControlSet002
        Control
        Enum
        Hardware Profiles
        Policies
        services
      CurrentControlSet
        Control
        Enum
        Hardware Profiles
        Policies
        services
      MountedDevices
```

Name	Type	Data
(Default)	REG_SZ	(value not set)
BootDriverFlags	REG_DWORD	0x00000000 (0)
CurrentUser	REG_SZ	USERNAME
FirmwareBootD...	REG_SZ	multi(0)disk(0)rdisk(0)partition(3)
PreshutdownOr...	REG_MULTI_SZ	wuauserv gpsvc trustedinstaller
ServiceControl...	REG_EXPAND_SZ	%systemroot%\system32\scext.dll
SystemBootDevi...	REG_SZ	multi(0)disk(0)rdisk(1)partition(1)
SystemStartOpti...	REG_SZ	NOEXECUTE=OPTIN
WaitToKillServic...	REG_SZ	12000

Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control

Figure 99: Last Known Good Config in the Registry

When you have an issue with a configuration setting, software installation or system update that cannot be resolved in Safe Mode or using Driver Rollback you can attempt to use the data stored in the Last Known Good Configuration.

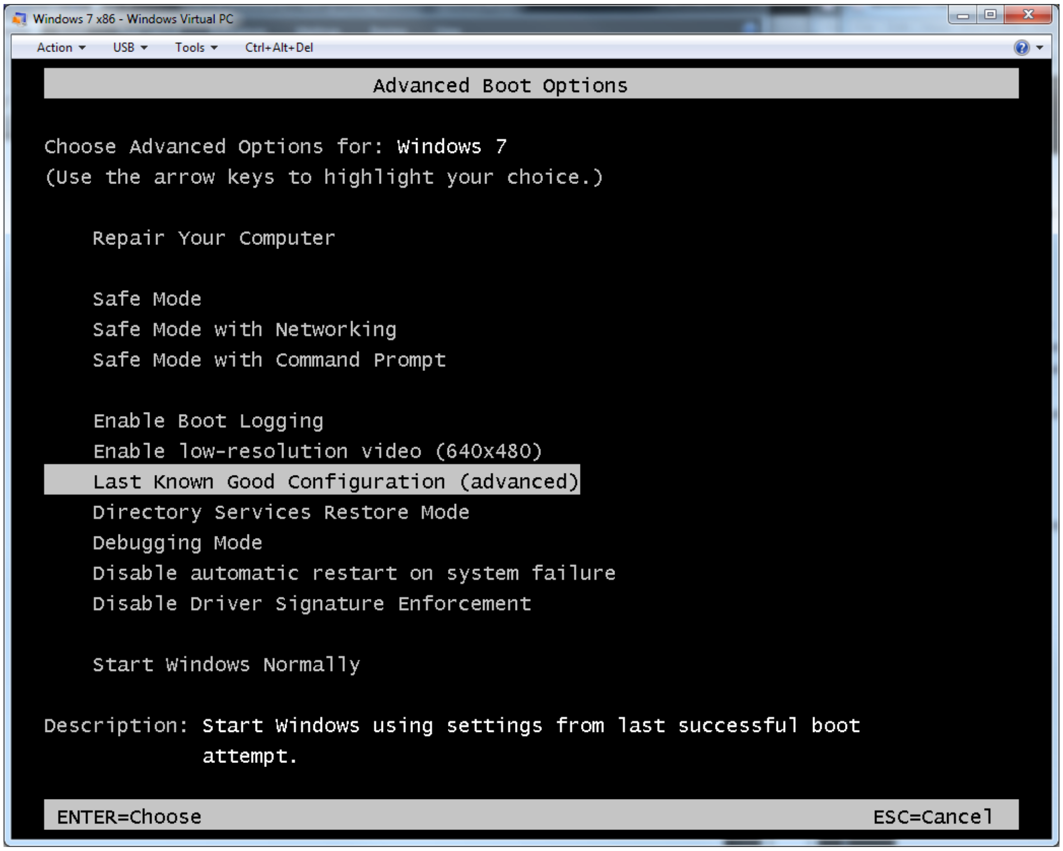
This can be a very useful tool, with one exception: if you're able to log in after the error or issue occurs, then the error condition will be committed to the CurrentControlSet and, thus, becomes the Last Known "Good" Configuration. In other words, you'll simply be restarting the system with the issue.

If you can use the Last Known Good Configuration start up option before you log in and replicate that information, you stand a better chance of rescuing the system from the problem condition.

As an example, let's say you make some system changes with an application install and through the application interface some adjustments are made to the registry and the system begins to show signs of slowing down and eventually crashes the application and some other applications on the system. You might not be able to get the registry editor open to effect repairs - or even know where to start.

This scenario is the perfect example of when you can use the Last Known Good Configuration start up option.

Shut down the system (or power it off if it is not responding correctly) and then restart the system. Before the Windows logo comes up you hit F8 and choose the Last Known Good Configuration start up option.



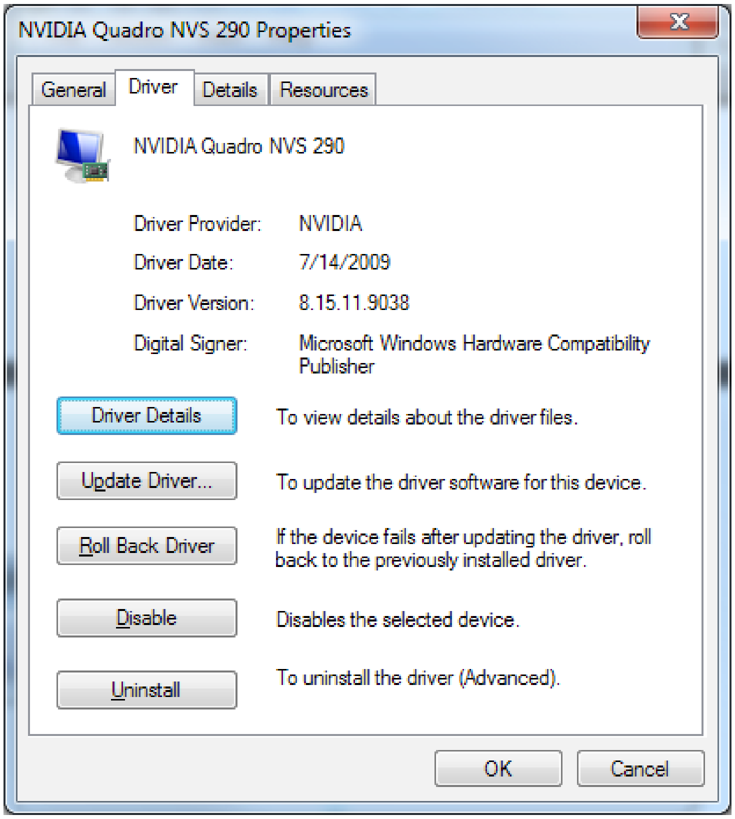
```
                              Advanced Boot Options

Choose Advanced Options for: Windows 7
(Use the arrow keys to highlight your choice.)

    Repair Your Computer

    Safe Mode
    Safe Mode with Networking
    Safe Mode with Command Prompt

    Enable Boot Logging
    Enable low-resolution video (640x480)
    Last Known Good Configuration (advanced)
    Directory Services Restore Mode
    Debugging Mode
    Disable automatic restart on system failure
    Disable Driver Signature Enforcement

    Start Windows Normally

Description: Start Windows using settings from last successful boot
             attempt.

 ENTER=Choose                                                 ESC=Cancel
```

Figure 100: Starting in Last Known Good Config

Understanding Driver Rollback

Driver Rollback is another way you can perform a restore, of sorts, to your system. You start the process using Device Manager and then choosing the device you are having issues with. By default, only administrators can install, uninstall, and roll back drivers.

Once you have the troublesome device selected, **right click** to bring up the properties page.



NVIDIA Quadro NVS 290 Properties

NVIDIA Quadro NVS 290

Driver Provider: NVIDIA

Driver Date: 7/14/2009

Driver Version: 8.15.11.9038

Digital Signer: Microsoft Windows Hardware Compatibility Publisher

To view details about the driver files.

To update the driver software for this device.

If the device fails after updating the driver, roll back to the previously installed driver.

Disables the selected device.

To uninstall the driver (Advanced).

Figure 101: Driver Properties Page

On the **Driver** tab, click the Roll Back Driver button. When you choose to roll back, you'll receive a warning message before you can commit.

Generally, driver roll back is one of the last steps you're going to take when troubleshooting a device. In most cases, there is a good reason for a released revision or update to drivers and, unless you're experiencing a specific issue with the new driver, you're not going to want to roll it back to a previous version.

Having said that, if you have updated a device driver but the new driver does not work as well as the previous one, or causes conflicts with other drivers, this is where it might make sense to roll it back.

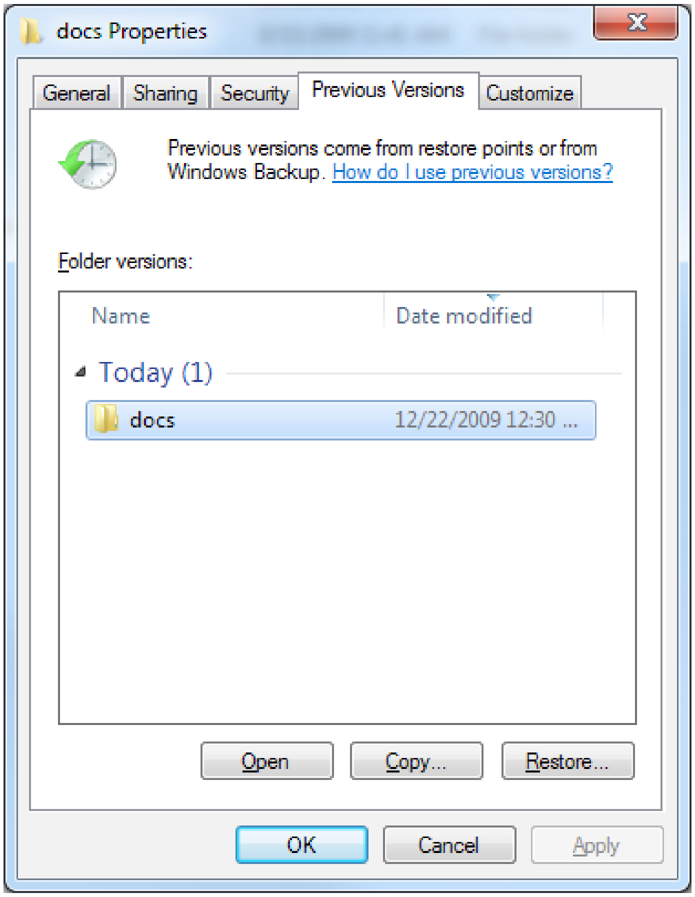
Configure File Recovery Options

Shadow copies are copies of files and folders that the operating system automatically saves when it creates a restore point. Windows 7 uses Volume Shadow Copy Service (VSS) to do this.

When you need to restore a file that you previously deleted or changed, or when you want to revert to an earlier version of a file, you can either restore the file from a shadow copy.

If the system is configured to use the Shadow Copy service, you'll actually have several versions of the file, with different creation dates, to restore from. Previous versions are saved as part of a restore point when system protection is running on your machine and configured to create the previous versions of copies.

When you need to gain access to a previous version, all you need to do is **right click** a folder, go to the properties page and choose the **Previous Version** tab.



Previous versions come from restore points or from Windows Backup. How do I use previous versions?

Folder versions:

Name	Date modified
Today (1)	
docs	12/22/2009 12:30 ...

Figure 102: A Folder's Previous Version Listing

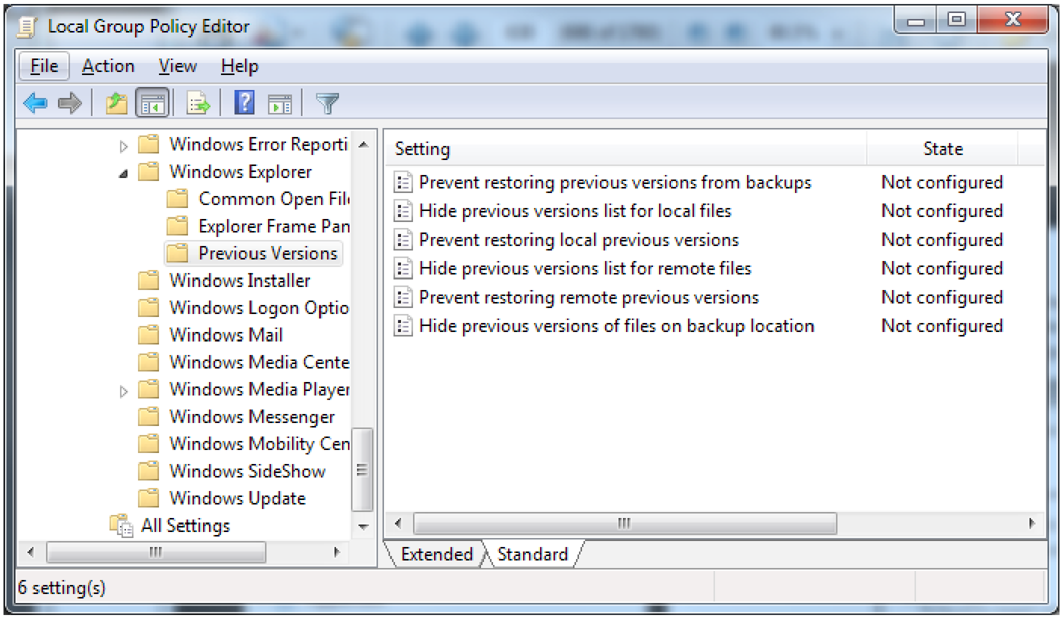
Here, you can open the previous version, copy it to another location or restore it back into its original location. It is always better to do any restoring in an alternate location so that the action of a restore doesn't inadvertently recover other files that were not intended to be restored.

When you choose the OPEN option a new Windows Explorer window will open as shown below, allowing access to all the files in the previous version. You'll notice in the screen shot that the path is \\localhost\I$\Data\saved\docs (December 22, 2009). To restore a single, simply open it and save it elsewhere. Alternately, you can right click the file and choose either the **Send to** or **Copy** options from the context menu.

You may need to make adjustments with respect to the maximum disk space that is used for system protection. By default, 5% of the total disk space is used and, as space fills up, older restore points are deleted to make room for newer restore points.

If you need to make the settings for Previous Version files universal within your enterprise, this can be done by using Group Policy settings that are available in **Policies\Administrative Templates\Windows Components\Windows Explorer\Previous Versions.**

The settings are available under both the Computer Configuration and the User Configuration nodes of the policy.



Setting	State
Prevent restoring previous versions from backups	Not configured
Hide previous versions list for local files	Not configured
Prevent restoring local previous versions	Not configured
Hide previous versions list for remote files	Not configured
Prevent restoring remote previous versions	Not configured
Hide previous versions of files on backup location	Not configured

Figure 103: Previous Versions Group Policy Settings

- **Prevent Restoring Previous Versions From Backups** – allows you to suppress the Restore button in the previous versions property page when the user has selected a previous version of a local file.
    - When this policy is enabled, the Restore button will be disabled.
    - When this policy is disabled, the Restore button will remain active for a previous version corresponding to a backup.
- **Hide Previous Versions List For Local Files** – hides the list of previous versions of files that are on local disks. Previous versions may come from the on-disk restore points or from backup media.
    - When this policy is enabled, users will not be able to list or restore previous versions of files on local disks.
    - When the policy is disabled, users will be able to list and restore previous versions of files on local disks.
- **Prevent Restoring Local Previous Versions** – lets you suppress the Restore button in the previous versions property page when the user has selected a previous version of a local file.
    - When this policy is enabled, the Restore button will be disabled.
    - When this policy is disabled the Restore button will remain active for a previous version corresponding of a local file.

- **Hide Previous Versions List For Remote Files** – lets you hide the list of previous versions of files that are on file shares. The previous versions come from the on-disk restore points on the file share.
    - When this policy is enabled, users will not be able to list or restore previous versions of files on file shares.
    - When this policy is disabled, users will be able to list and restore previous versions of files on file shares.
- **Prevent Restoring Remote Previous Versions** – allows the administrator to disable the Restore button in the previous versions property page when the user has selected a previous version of a file on a file share.
    - When this policy is enabled, the Restore button will be disabled when the user selects a previous version corresponding to a file on a file share.
    - When this policy is disabled, the Restore button will be available for files on a file share.
- **Hide Previous Versions Of Files On Backup Location** – allows an administrator to hide entries in the list of previous versions of a file in which the previous version is located on backup media. Previous versions can come from the on-disk restore points or the backup media.
    - When this policy is enabled, users will not see any previous versions corresponding to backup copies, and will only see previous versions corresponding to on-disk restore points.
    - When this policy is disabled, users will be able to see previous versions corresponding to backup copies as well as previous versions corresponding to on-disk restore points.

Practice Questions

Chapter 1

1. You have a number of company computers that are currently running Windows Vista Home Premium Edition. Each of these computers is equipped with a 2-GHz 64-bit processor, 2-GB of RAM, an 80 GB hard drive and a DirectX 9-compliant video card. You attempt to upgrade the machines to Windows 7 64-bit edition and are having problems with the hardware requirements. What is most likely the problem? Select the best answer.

○ A. The hard drive does not have 16 GBs free to support Windows 7.

○ B. The hard drive does not have 20 GBs free to support Windows 7.

○ C. The computers must have at least 3 GB of RAM to install Windows 7 64-bit.

○ D. The computers must have at least 4 GB of RAM to install Windows 7 64-bit.

2. Your manager has decided that all desktop workstations in the enterprise will run Windows 7 Professional. All current computers run Windows Vista Business; however, when you attempt the upgrade on a test computer you receive an error stating that there exists a compatibility problem. You have verified that all system requirements have been met to support the upgrade. What is the most likely problem? Select the best answer.

○ A. Windows 7 Professional cannot be upgraded from Windows Vista Business.

○ B. You must perform a clean installation to upgrade from Windows Vista Business to Windows 7 Professional.

○ C. The corporate computers do not have Windows Vista SP1 installed.

○ D. The corporate computers do not have Windows Vista SP2 installed.

3. Which of the following Windows 7 editions supports BitLocker?
Choose all that apply.

○ A. Windows 7 Ultimate Edition.

○ B. Windows 7 Enterprise Edition.

○ C. Windows 7 Professional Edition.

○ D. Windows 7 Home Premium Edition.

4. You are migrating user state data from a number of Windows Vista computers to replacement Windows 7 computers. You have already created a migration store. You are beginning to migrate the user settings back to the computers and are having a problem with local accounts not being enabled on the destination computers. What loadstate switch option is needed for local accounts to be enabled? Select the best answer.

○ A. /lac

○ B. /lae

○ C. /ui

○ D. /uel

Chapter 2

1. You have configured all of the required parameters in the answer file that you are going to use for your automated deployment of Windows 7 in your organization. What is the default name of the .xml file that is used to guide Windows 7 installation during an automated setup? Select the best answer.

○ A. Unattend.xml.

○ B. Unattended.xml.

○ C. Autounattend.xml.

○ D. Autoattended.xml.

2. You maintain several WIM images that you use for enterprise deployment of Windows 7 in your organization. You need to add a line-of-business application to one of these images. Which of the following command-line statements would mount the windows7.wim image to C:\Offline and therefore enable you to add the new line-of-business application? Select the best answer.

○ A. ImageX /mntrw C:\windows7.wim 2 C:\Offline

○ B. ImageX /mount C:\windows7.wim 2 C:\Offline

○ C. ImageX /mnt C:\windows7.wim 2 C:\Offline

○ D. ImageX /mountrw C:\windows7.wim 2 C:\Offline

3. You are trying to configure a Virtual Hard Disk (VHD) on Windows 7. Which of the following are supported methods for creating a VHD in Windows 7? Choose all that apply.

○ A. Using the vhdboot utility.

○ B. Using the diskpart utility.

○ C. Using the Disk Management MMC snap-in.

○ D. Using the fdisk utility.

Chapter 3

1. After upgrading your workstation from Windows XP to Windows 7, you discover that a program that worked correctly on Windows XP no longer functions. How would you correctly set the compatibility mode to configure the problematic program to run as a Windows XP application? Select the best answer.

❍ A. Right-click the application and select Compatibility from the shortcut menu. Next, check the 'Run this program in compatibility mode for' box and select Windows XP from the drop-down menu.

❍ B. Right-click the application and select Compatibility from the shortcut menu. Navigate to the Compatibility tab and then check the 'Run this program in compatibility mode for' box. Finally, select Windows XP drop the drop-down menu.

❍ C. Right-click the application and select Compatibility from the shortcut menu. Navigate to the Compatibility tab and then check the 'Run this program as a Windows XP Application.'

❍ D. Right-click the application and select Compatibility from the shortcut menu. Navigate to the General tab and check the 'Run this program as a Windows XP Application.'

2. You support a legacy line-of-business application that does not currently have an update to ensure Windows 7 compatibility. This application is required for everyday business and must be run on your organization's new computers that run Windows 7. Which of the following methods represents an alternative solution to enabling compatibility mode for this application? Select the best answer.

❍ A. Apply a patch.

❍ B. Enable administrative privileges.

❍ C. Develop a shim.

❍ D. Downgrade to Windows Vista.

3. In your mixed Windows 7/Windows Vista client environment, you deploy both Software Restriction Policies and AppLocker to your users via Group Policy. How does Windows 7 process a Group Policy Object (GPO) in which both Software Restriction Policies and AppLockers are configured? Select the best answer.

❍ A. Only the Software Restriction Policies will be enforced.

❍ B. Only the AppLocker policies will be enforced.

❍ C. The Software Restriction Policies will be enforced first and then the AppLocker policies will be enforced second.

❍ D. The AppLocker policies will be enforced first and then the Software Restriction Policies will be enforced second.

Chapter 4

1. You are planning an IPv6 address design for your Windows Server 2008- and Windows 7-based domain network. Of the following IPv6 addresses, which is different?
Select the best answer.

○ A. 2002:18d3:e4e0:0:bd95:90e8:31c8:b4b6

○ B. 2002:18d3:e4e:0:bd95:90e8:31c8:b4b6

○ C. 2002:18d3:e4e0:0000:bd95:90e8:31c8:b4b6

○ D. 2002:18d3:e4e::bd95:90e8:31c8:b4b6

2. You are attempting to connect to your corporate WLAN from your Windows 7 laptop computer. Which of the following Windows 7 navigation paths is the most efficient way to connect to your corporate WLAN? Select the best answer.

○ A. Control Panel -> Network and Sharing Center -> Manage Wireless Networks -> [Network Name] -> Connect.

○ B. System Tray -> Connections -> [Network Name] -> Connect.

○ C. Control Panel -> Wireless -> [Network Name] -> Connect.

○ D. Control Panel -> Network Connections -> Manage Wireless Networks -> [Network Name] -> Connect.

3. You are planning a deployment of DirectAccess to all Windows 7-based laptop computers in your organization. Which of the following represent system requirements for DirectAccess deployment? Choose all that apply.

○ A. Windows 7 client.

○ B. PKI infrastructure.

○ C. Two or more domain controllers.

○ D. One public IP address on the DirectAccess server.

Chapter 5

1. You manage a Windows-based peer-to-peer network. You are configuring a shared folder on your Windows 7 computer and are trying to ensure that file permissions are applied correctly. You have configured permissions on the share to allow anyone to access the share. You have also configured NTFS permissions so that everyone has read/write access. However, when users attempt to access the share they are prompted for a username and password. How can you prevent this from happening? Select the best answer.

○ A. The Sharing Wizard must be disabled in Windows 7.

○ B. Password-protected sharing is enabled in Windows 7.

○ C. Share permissions are set up incorrectly.

○ D. NTFS permissions are set up incorrectly.

2. You are trying to transfer a number of files from one partition to another on your Windows 7 workstation by using drag-and-drop. The Windows 7 computer has one physical hard drive installed. Which of the following statements describe default drag-and-drop behavior of Windows 7 when transferring files between two drives? Choose all that apply.

○ A. Partition-to-Partition file transfer moves by default.

○ B. Partition-to-Partition file transfer copies by default.

○ C. Internal partition drive file transfer moves by default.

○ D. Internal partition drive file transfer copies by default.

3. You are configuring BranchCache using Distributed Cache mode on a Windows 7 computer. Which ports are required to be open for this mode to function? Select the best answer.

○ A. Inbound : Local : 80 : Remote : 1025 to 5000
Outbound : Local : 1025 to 5000 : Remote : 80
Multicast : 239.255.255.250 (IPv4) and FF02::C (IPv6)

○ B. Inbound : Local : 3702 : Remote : 1025 to 5000
Outbound : Local : 1025 to 5000 : Remote : 3702
Inbound : Local : 80 : Remote : 1025 to 5000
Outbound : Local : 1025 to 5000 : Remote : 80
Multicast : 239.255.255.250 (IPv4) and FF02::C (IPv6)

○ C. Inbound : Local : 3702 : Remote : 1025 to 5000
Outbound : Local : 1025 to 5000 : Remote : 3702
Multicast : 239.255.255.250 (IPv4) and FF02::C (IPv6)

○ D. Inbound : Local : 3702 : Remote : 1025 to 5000
Outbound : Local : 1025 to 5000 : Remote : 80
Multicast : 239.255.255.250 (IPv4) and FF02::C (IPv6)

Chapter 6

1. You plan to protect a FAT32-partitioned USB flash drive with BitLocker-to-Go on your Windows 7 computer. Which operating systems will be able to read the data from this drive once BitLocker-to-go is installed? Choose all that apply.

○ A. Windows Vista.

○ B. Windows XP.

○ C. Windows 7.

○ D. Windows Server 2003 R2.

○ E. Windows 98.

○ F. Windows 95.

2. You are researching mobile computer support in Windows 7. Which of the following features were introduced with Windows 7? Choose all that apply.

○ A. Server-side Offline Files.

○ B. Client-side Offline Files.

○ C. Transparent Caching.

○ D. Background Synchronization.

○ E. Previous Versions.

3. Which of the following best describes the remote access protocol support in the Windows 7 VPN Reconnect feature? Select the best answer.

○ A. IPSec Transparent Mode with IKEv3.

○ B. IPSec Transparent Mode with IKEv2.

○ C. IPSec Tunnel Mode with IKEv2.

○ D. IPSec Tunnel Mode with IKEv3.

Chapter 7

1. You are configuring Windows update settings on a Windows 7 computer by using Group Policy. Where are Windows Update settings stored in Windows 7 Group Policy? Select the best answer.

○ A. User Configuration -> Administrative Templates -> Windows Components -> Windows Update.

○ B. Computer Configuration -> Windows Settings -> Windows Components -> Windows Update.

○ C. Computer Configuration -> Software Settings -> Windows Update.

○ D. Computer Configuration -> Administrative Templates -> Windows Components -> Windows Update.

2. You are attempting to create a second partition on the hard drive of your Windows 7 workstation by shrinking the volume. However, in Windows Explorer the volume displays with zero bytes of available storage space. Which of the following represents the best explanation for this problem? Select the best answer.

○ A. Unmovable files prevent the volume from shrinking.

○ B. The hard drive does not support shrinkage.

○ C. The partition type does not support shrinkage.

○ D. The system BIOS type does not support shrinkage.

3. You are administering security on a Windows 7 computer in your organization. How can you view all security-related events for a specific user of this computer? Select the best answer.

○ A. Run a built-in Windows PowerShell script.

○ B. Use the Computer Management console.

○ C. Define a Custom View in Event Viewer.

○ D. Create a Subscription in Event Viewer.

Chapter 8

1. You need to back up critical document files on your Windows 7 administrative workstation. You plan to accomplish this goal by using native Windows 7 tools. How can you invoke the Windows 7 backup tools? Choose all that apply.

○ A. Access Backup and Restore from the Accessories folder in the Windows 7 Start menu.

○ B. Access the Backup and Restore Control Panel program.

○ C. Access the Properties sheet of the drive that contains the document files.

○ D. Acccess Windows Backup from the Accessories folder in the Start menu.

2. You are planning to use native backup tools on your Windows 7 development computer to create an image of the system drive for disaster recovery purposes. What technology replaced the Complete PC Backup utility in Windows Vista? Select the best answer.

○ A. Complete PC Backup and Restore.

○ B. System Restore.

○ C. Full System Backup.

○ D. Backup and Restore.

3. You are configuring disaster recovery options on a Windows 7 computer in your organization. How can you create system repair disk for use in Windows 7 system troubleshooting? Select the best answer.

○ A. Backup and Restore Control Panel.

○ B. System Restore.

○ C. Disk Management.

○ D. System Control Panel.

Answers & Explanations

Chapter 1

1. Answer: B

Explanation A. Incorrect. Windows 7 64-bit editions require a minimum of 20 GB of free hard drive space to install.

Explanation B. Correct. Windows 7 64-bit editions require a minimum of 20 GB of hard drive space to install.

Explanation C. Incorrect. Windows 7 64-bit editions require a minimum of 20 GB of hard drive space to install. The minimum amount of memory required for Windows 7 64-bit is 2 GB.

Explanation D. Incorrect. Windows 7 64-bit editions require a minimum of 20 GB of hard drive space to install. The minimum amount of memory required for Windows 7 64-bit is 2 GB.

2. Answer: C

Explanation A. Incorrect. To upgrade to Windows 7, only Windows Vista Service Pack 1 (SP1) is required.

Explanation B. Incorrect. To upgrade to Windows 7, only Windows Vista SP1 is required.

Explanation C. Correct. To upgrade to Windows 7, only Windows Vista SP1 is required.

Explanation D. Incorrect. To upgrade to Windows, only 7 Windows Vista SP1 is required.

3. Answers: A, B

Explanation A. Correct. Both Windows 7 Ultimate Edition and Windows 7 Enterprise Edition support the BitLocker drive encryption feature.

Explanation B. Correct. Both Windows 7 Ultimate Edition and Windows 7 Enterprise Edition support the BitLocker drive encryption feature.

Explanation C. Incorrect. Both Windows 7 Ultimate Edition and Windows 7 Enterprise Edition support the BitLocker drive encryption feature.

Explanation D. Incorrect. Both Windows 7 Ultimate Edition and Windows 7 Enterprise Edition support the BitLocker drive encryption feature.

4. Answer: B

Explanation A. Incorrect. The /lae loadstate option is used when to enable local users on the destination computer which have been created by the /lac option.

Explanation B. Correct. The /lae loadstate option is used when to enable local users on the destination computer which have been created by the /lac option.

Explanation C. Incorrect. The /lae loadstate option is used when to enable local users on the destination computer which have been created by the /lac option.

Explanation D. Incorrect. The /lae loadstate option is used when to enable local users on the destination computer which have been created by the /lac option.

Chapter 2

1. Answer: C

Explanation A. Incorrect. The default .xml answer file is named Autounattend.xml. The answer file is typically placed on a removeable media device, such as a USB flash drive, during automated installation.

Explanation B. Incorrect. The default .xml answer file is named Autounattend.xml. The answer file is typically placed on a removeable media device, such as a USB flash drive, during automated installation.

Explanation C. Correct. The default .xml answer file is named Autounattend.xml. The answer file is typically placed on a removeable media device, such as a USB flash drive, during automated installation.

Explanation D. Incorrect. The default .xml answer file is named Autounattend.xml. The answer file is typically placed on a removeable media device, such as a USB flash drive, during automated installation.

2. Answer: D

Explanation A. Incorrect. The /mountrw parameter of the ImageX utility is required in order for the WIM image to be mounted in read/write mode.

Explanation B. Incorrect. The /mountrw parameter of the ImageX utility is required in order for the WIM image to be mounted in read/write mode.

Explanation C. Incorrect. The /mountrw parameter of the ImageX utility is required in order for the WIM image to be mounted in read/write mode.

Explanation D. Correct. The /mountrw parameter of the ImageX utility is required in order for the WIM image to be mounted in read/write mode.

3. Answers: B, C

Explanation A. Incorrect. A VHD can be created on Windows 7 either by using the diskpart command-line utility or by using the Disk Management Microsoft Management Console (MMC) snap-in.

Explanation B. Correct. A VHD can be created on Windows 7 either by using the diskpart command-line utility or by using the Disk Management Microsoft Management Console (MMC) snap-in.

Explanation C. Correct. A VHD can be created on Windows 7 either by using the diskpart command-line utility or by using the Disk Management Microsoft Management Console (MMC) snap-in.

Explanation D. Incorrect. A VHD can be created on Windows 7 either by using the diskpart command-line utility or by using the Disk Management Microsoft Management Console (MMC) snap-in.

Chapter 3

1. Answer: B

Explanation A. Incorrect. In Windows 7, compatibility mode is set on the Compatibility tab of the Properties sheet for an application.

Explanation B. Correct. In Windows 7, compatibility mode is set on the Compatibility tab of the Properties sheet for an application.

Explanation C. Incorrect. In Windows 7, compatibility mode is set on the Compatibility tab of the Properties sheet for an application. There is no checkbox for 'Run this program as a Windows XP Application' in this interface.

Explanation D. Incorrect. In Windows 7, compatibility mode is set on the Compatibility tab of the Properties sheet for an application. There is no checkbox for 'Run this program as a Windows XP Application' in this interface.

2. Answer: C

Explanation A. Incorrect. A patch is, in the vast majority of cases, developed and released by the original equipment manufacturer (OEM) or application developer.

Explanation B. Incorrect. Enabling administrative privileges to standard users opens up unwanted security vulnerabilities.

Explanation C. Correct. A shim is a small piece of code that is inserted between an application and the operating system in order to bridge compatibility issues.

Explanation D. Incorrect. While this approach may resolve the application incompatibility, it is not a practical resolution to this problem.

3. Answer: B

Explanation A. Incorrect. For Windows 7- and Windows Server 2008 R2-based systems, if AppLocker policies are applied for a computer, then they will be processed exclusively.

Explanation B. Correct. For Windows 7- and Windows Server 2008 R2-based systems, if AppLocker policies are applied for a computer, then they will be processed exclusively.

Explanation C. Incorrect. For Windows 7- and Windows Server 2008 R2-based systems, if AppLocker policies are applied for a computer, then they will be processed exclusively.

Explanation D. Incorrect. For Windows 7- and Windows Server 2008 R2-based systems, if AppLocker policies are applied for a computer, then they will be processed exclusively.

Chapter 4

1. Answer: B

Explanation A. Incorrect. This IPv6 address, when fully written out, is 2002:18d3:e4e0:0000:bd95:90e8:31c8:b4b6. With IPv6 shorthand notation, :0000: can also be written as :0:.

Explanation B. Correct. This address is not the same IPv6 address as the others because you can not remove trailing zeros from the address.

Explanation C. Incorrect. This is the same IPv6 address as the other choices.

Explanation D. Incorrect. This IPv6 address is the same address as the other choices. This address, when it is fully written out, is 2002:18d3:e4e0:0000:bd95:90e8:31c8:b4b6. The address fragment :: can be used once in an IPv6 address to replace any number of consecutive zeros.

2. Answer: B

Explanation A. Incorrect. In Windows 7, the most efficient way to connect to a wireless network is to use the Connections icon from the notification area; this item displays all reachable wireless networks.

Explanation B. Correct. In Windows 7, the most efficient way to connect to a wireless network is to use the Connections icon from the notification area; this item displays all reachable wireless networks.

Explanation C. Incorrect. In Windows 7, the most efficient way to connect to a wireless network is to use the Connections icon from the notification area; this item displays all reachable wireless networks.

Explanation D. Incorrect. In Windows 7, the most efficient way to connect to a wireless network is to use the Connections icon from the notification area; this item displays all reachable wireless networks.

3. Answers: A, B

Explanation A. Correct. A Windows 7 client is required for DirectAccess.

Explanation B. Correct. A public key infrastructure (PKI) is required to implement DirectAccess.

Explanation C. Incorrect. Only one Windows Server 2008 R2-based Active Directory domain controller is required for DirectAccess.

Explanation D. Incorrect. DirectAccess requires two consecutive IP addresses on the DirectAccess server.

Chapter 5

1. Answer: B

Explanation A. Incorrect. When password-protected sharing is enabled in Windows 7, connecting users are always prompted for logon credentials for the share to be accessed.

Explanation B. Correct. When password-protected sharing is enabled in Windows 7, connecting users are always prompted for logon credentials for the share to be accessed.

Explanation C. Incorrect. When password-protected sharing is enabled in Windows 7, connecting users are always prompted for logon credentials for the share to be accessed.

Explanation D. Incorrect. When password-protected sharing is enabled in Windows 7, connecting users are always prompted for logon credentials for the share to be accessed.

2. Answers: B, C

Explanation A. Incorrect. By default, all physical partition-to-partition file transfers are copies, and all internal partition file transfers (that is, transfers from one partition to another on a single physical hard drive) are moves.

Explanation B. Correct. By default, all physical partition-to-partition file transfers are copies, and all internal partition file transfers (that is, transfers from one partition to another on a single physical hard drive) are moves.

Explanation C. Correct. By default, all physical partition-to-partition file transfers are copies, and all internal partition file transfers (that is, transfers from one partition to another on a single physical hard drive) are moves.

Explanation D. Incorrect. By default, all physical partition-to-partition file transfers are copies, and all internal partition file transfers (that is, transfers from one partition to another on a single physical hard drive) are moves.

3. Answer: B

Explanation A. Incorrect. In order for a BranchCache client to operate in Distributed Cache mode, you must allow TCP port 80 inbound and outbound from ports 1025 to 5000 (ephemeral), port 3702 inbound and outbound from ports 1025 to 5000 (ephemeral) and multicast traffic from 239.255.255.250 (IPv4) and FF02::C (IPv6).

Explanation B. Correct. In order for a BranchCache client to operate in Distributed Cache mode, you must allow TCP port 80 inbound and outbound from ports 1025 to 5000 (ephemeral), port 3702 inbound and outbound from ports 1025 to 5000 (ephemeral) and multicast traffic from 239.255.255.250 (IPv4) and FF02::C (IPv6).

Explanation C. Incorrect. In order for a BranchCache client to operate in Distributed Cache mode, you must allow TCP port 80 inbound and outbound from ports 1025 to 5000 (ephemeral), port 3702 inbound and outbound from ports 1025 to 5000 (ephemeral) and multicast traffic from 239.255.255.250 (IPv4) and FF02::C (IPv6).

Explanation D. Incorrect. In order for a BranchCache client to operate in Distributed Cache mode, you must allow TCP port 80 inbound and outbound from ports 1025 to 5000 (ephemeral), port 3702 inbound and outbound from ports 1025 to 5000 (ephemeral) and multicast traffic from 239.255.255.250 (IPv4) and FF02::C (IPv6).

Chapter 6

1. Answers: A, B, C

Explanation A. Correct. When BitLocker-to-Go is configured on an FAT32-partitioned flash drive, Windows XP, Windows Vista, Windows 7 and Windows Server 2008 R2 clients can read data from the encrypted volume.

Explanation B. Correct. When BitLocker-to-Go is configured on an FAT32-partitioned flash drive, Windows XP, Windows Vista, Windows 7 and Windows Server 2008 R2 clients can read data from the encrypted volume.

Explanation C. Correct. When BitLocker-to-Go is configured on an FAT32-partitioned flash drive, Windows XP, Windows Vista, Windows 7 and Windows Server 2008 R2 clients can read data from the encrypted volume.

Explanation D. Incorrect. When BitLocker-to-Go is configured on an FAT32-partitioned flash drive, Windows XP, Windows Vista, Windows 7 and Windows Server 2008 R2 clients can read data from the encrypted volume.

Explanation E. Incorrect. When BitLocker-to-Go is configured on an FAT32-partitioned flash drive, Windows XP, Windows Vista, Windows 7 and Windows Server 2008 R2 clients can read data from the encrypted volume.

Explanation F. Incorrect. When BitLocker-to-Go is configured on an FAT32-partitioned flash drive, Windows XP, Windows Vista, Windows 7 and Windows Server 2008 R2 clients can read data from the encrypted volume.

2. Answers: C, D

Explanation A. Incorrect. Both transparent caching and background synchronization were introduced in the Windows 7 version of Offline Files.

Explanation B. Incorrect. Both transparent caching and background synchronization were introduced in the Windows 7 version of Offline Files.

Explanation C. Correct. Both transparent caching and background synchronization were introduced in the Windows 7 version of Offline Files.

Explanation D. Correct. Both transparent caching and background synchronization were introduced in the Windows 7 version of Offline Files.

Explanation E. Incorrect. Both transparent caching and background synchronization were introduced in the Windows 7 version of Offline Files.

3. Answer: C

Explanation A. Incorrect. The VPN Reconnect feature in Windows Server 2008 R2 and Windows 7 supports Internet Protocol Security (IPSec) Tunnel Mode with Internet Key Exchange (IKE)v2.

Explanation B. Incorrect. The VPN Reconnect feature in Windows Server 2008 R2 and Windows 7 supports Internet Protocol Security (IPSec) Tunnel Mode with Internet Key Exchange (IKE)v2.

Explanation C. Correct. The VPN Reconnect feature in Windows Server 2008 R2 and Windows 7 supports Internet Protocol Security (IPSec) Tunnel Mode with Internet Key Exchange (IKE)v2.

Explanation D. Incorrect. The VPN Reconnect feature in Windows Server 2008 R2 and Windows 7 supports Internet Protocol Security (IPSec) Tunnel Mode with Internet Key Exchange (IKE)v2.

Chapter 7

1. Answer: D

Explanation A. Incorrect. The location of Windows Update settings in Windows 7 Group Policy is Computer Configuration -> Administrative Templates -> Windows Components -> Windows Update.

Explanation B. Incorrect. The location of Windows Update settings in Windows 7 Group Policy is Computer Configuration -> Administrative Templates -> Windows Components -> Windows Update.

Explanation C. Incorrect. The location of Windows Update settings in Windows 7 Group Policy is Computer Configuration -> Administrative Templates -> Windows Components -> Windows Update.

Explanation D. Correct. The location of Windows Update settings in Windows 7 Group Policy is Computer Configuration -> Administrative Templates -> Windows Components -> Windows Update.

2. Answer: A

Explanation A. Correct. Shrinking can be prevented via unmovable files or lack of shrinkable space.

Explanation B. Incorrect. Shrinking can be prevented via unmovable files or lack of shrinkable space.

Explanation C. Incorrect. In Windows 7, volume shrinkage can be prevented by the presence of unmovable files or a true lack of shrinkable space on a hard drive.

Explanation D. Incorrect. In Windows 7, volume shrinkage can be prevented by the presence of unmovable files or a true lack of shrinkable space on a hard drive.

3. Answer: C

Explanation A. Incorrect. The Create Custom View function in the Windows 7 Event Viewer allows you to define a view that matches administrator-defined criteria.

Explanation B. Incorrect. The Create Custom View function in the Windows 7 Event Viewer allows you to define a view that matches administrator-defined criteria.

Explanation C. Correct. The Create Custom View function in the Windows 7 Event Viewer allows you to define a view that matches administrator-defined criteria.

Explanation D. Incorrect. The Create Custom View function in the Windows 7 Event Viewer allows you to define a view that matches administrator-defined criteria.

Chapter 8

1. Answers: B, C

Explanation A. Incorrect. The two primary ways to run the native backup utility in Windows 7 are to access the Backup and Restore Control Panel item or to access the Properties sheet of the appropriate hard drive.

Explanation B. Correct. The two primary ways to run the native backup utility in Windows 7 are to access the Backup and Restore Control Panel item or to access the Properties sheet of the appropriate hard drive.

Explanation C. Correct. The two primary ways to run the native backup utility in Windows 7 are to access the Backup and Restore Control Panel item or to access the Properties sheet of the appropriate hard drive.

Explanation D. Incorrect. The two primary ways to run is the native backup utility in Windows 7 are to access the Backup and Restore Control Panel item or to access the Properties sheet of the appropriate hard drive.

2. Answer: D

Explanation A. Incorrect. The Backup and Restore Control Panel in Windows 7 includes a System image option that effectively replaces the Complete PC Backup feature in Windows Vista.

Explanation B. Incorrect. The Backup and Restore Control Panel in Windows 7 includes a System image option that effectively replaces the Complete PC Backup feature in Windows Vista.

Explanation C. Incorrect. The Backup and Restore Control Panel in Windows 7 includes a System image option that effectively replaces the Complete PC Backup feature in Windows Vista.

Explanation D. Correct. The Backup and Restore Control Panel in Windows 7 includes a System image option that effectively replaces the Complete PC Backup feature in Windows Vista.

3. Answer: A

Explanation A. Correct. In Windows 7, you can create a system repair disc by accessing the Backup and Restore Control Panel.

Explanation B. Incorrect. In Windows 7, you can create a system repair disc by accessing the Backup and Restore Control Panel.

Explanation C. Incorrect. In Windows 7, you can create a system repair disc by accessing the Backup and Restore Control Panel.

Explanation D. Incorrect. In Windows 7, you can create a system repair disc by accessing the Backup and Restore Control Panel.