Exam
Manual

LearnSmart

Microsoft Windows Vista Configuration (70-620)

This LearnSmart exam manual covers the most important concepts you need to know in order to successfully complete the Windows Vista Configuration exam (70-620). By studying this manual, you will become familiar with an array of exam-related content, including:

- Installing and Upgrading Windows Vista
- Configuring and Troubleshooting Post-Installation System Settings
- Configuring Applications Included with Windows Vista
- And more!

Give yourself the competitive edge necessary to further our career as an IT professional and purchase this exam manual today!

Microsoft Windows Vista Client, Configuring (70-620) LearnSmart Exam Manual

Product ID: 010954
Production Date: July 18, 2011

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

Favorable discounts are offered on all products when ordered in quantity. For more information, please contact us directly:

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

International Contact Information

International: +1 (813) 769-0920

United Kingdom: (0) 20 8816 8036

Table of Contents

Abstract

This Exam Manual is designed to familiarize you with the necessary information you will need to know in order to pass the Microsoft 70-620 exam on Windows Vista Administration and Support. The primary purpose of this tool is to serve as a supplementary training product that you can use in conjunction with other training tools, such as LearnSmart Video Training or Practice Exams. It is not entirely comprehensive, but is instead designed to be quick and efficient, concentrating on the most difficult portions of the exam. After reading this Exam Manual, you should ask yourself how much you knew about the exam before you looked through it. If the answer is a lot, then you are probably prepared for the exam and can test yourself with a practice test. If not, then you need to concentrate more time studying and to reread the Exam Manual once again.

What to Know

The Microsoft 70-620 is the first exam available on the Microsoft Windows Vista platform. Consequently, both the technology involved with the Microsoft exam has changed and the technology involved within the actual test differs as well. This exam is highly concentrated on specific questions involved with the Vista platform, the difference between Vista and Microsoft, and what you need to know to be an effective Vista and Office technology specialist. Thus, it behooves you to spend a *lot* of time studying the *technology* of the test, and not necessarily the procedure. Much of the exam is going to be concentrated on the features of the Vista and Office platforms, not just what you can do with them. Be prepared!

Tips

The best thing you can do to prepare for this exam is get as much experience with Windows Vista as possible. This means that you'll need to purchase a copy of Windows Vista and get a very fast, very reliable computer. Vista is extremely demanding and if you want to know and understand the features very well, you'll need to have something that can turn them on and not stutter or struggle. Additionally, make sure that you take at least one practice test. They're available from LearnSmart and are the single best preparation tool available on the market. Good luck!

Installing and Upgrading Windows Vista

Identify Hardware Requirements

Microsoft's new Windows Vista operating system is the first version of Windows in which the user experience scales to the hardware capabilities of the computer on which Windows Vista is installed. Because of this, it is important to be aware of the operating system hardware requirements and any additional hardware needed to run the Aero desktop.

Vista Requirements

The hardware requirements for Windows Vista are far more demanding than any previous Windows operating system. Windows Vista will scale based on a given system's hardware capabilities. In addition, there are two separate sets of hardware requirements: one for machines that are simply "Vista Capable" (less expensive, but not necessarily Aero capable), and one for machines that are "Vista Premium Ready" (requires a high end video card and more RAM to support the Aero desktop).

The following table lists the recommended hardware requirements for Windows Vista:

	Minimum	Vista Capable	Premium Ready
CPU	800 Mhz	800 Mhz	1 Ghz
RAM	512 MB	512 MB	1 GB
GPU	SVGA	DirectX 9	Aero Capable *
Video RAM	n/a	n/a	128 MB
HDD	20 GB	20 GB	40 GB
HDD Free	15 GB	15 GB	15 GB
Optical Drive	CD	CD	DVD

* For more information, see the **Aero Requirements** section.

For more information on the difference between Vista Capable and Vista Premium Ready computers, see: http://www.microsoft.com/windows/products/windowsvista/buyorupgrade/capable.mspx

Aero Requirements

Windows Vista's user interface, code-named "AERO" (Authentic, Energetic, Reflective and Open) is designed to make users more productive by providing an attractive, glass-themed environment. Despite these changes, Windows Vista makes use of common dialog boxes and improved wizards to support applications created before Windows Vista.

Users with high-resolution monitors can take full advantage of their displays because Windows Vista smoothly scales icons and windows. The Aero interface also displays text clearer and sharper and higher resolutions, allowing users who had previously used lower resolutions to make text more readable.

Aero requires:

- DirectX 9 class graphics adapter with Pixel Shader 2.0
- Color depth of 32 bits per pixel (bpp)
- Windows Vista Display Driver Model (WDDM)
- Graphics memory bandwidth of at least 1,800 MB/s at the following resolution:
    - Desktop computer: 1,310,720 pixels (equivalent to 1280 x 1024)
    - Mobile computer: native resolution of built-in display

The following table lists the monitor resolutions supported by Aero:

Graphics Memory	Supported Monitor Resolution
64 MB	Up to 1,310,720 pixels (1280 x 1024)
128 MB	Greater than 1,310,720 & less than or equal to 2,304,000 (1920 x 1200)
256 MB	Greater than 2,304,000 pixels

Note: To achieve the memory requirements outlined above on systems with a Unified Memory Architecture (UMA) [shared memory or integrated graphics chipsets], 1 GB of dual-channel configured system memory (RAM) is required. The system must have at least 512 MB of RAM available for general system activities after graphics processing.

For additional information on the graphics hardware and drivers needed to support the Microsoft Vista Aero experience, see: http://www.microsoft.com/whdc/device/display/graphics-reqs.mspx

Perform a Clean Installation

As with earlier Microsoft operating systems, there are several ways to install Windows Vista. A clean installation is done when installing Windows Vista on a new, formatted partition. For systems with an existing operating system, the Microsoft Vista Windows Easy Transfer utility will transfer files and settings from the previous operating system installation.

You can use any of the following methods to perform a clean installation:

- Boot directly from the CD or DVD (Vista Premium Ready version) if the computer does not have an existing operating system.
- Run setup.exe from within an existing operating system.
- Overwrite an existing operating system with an image file.

Setup.exe can be run from the following sources:

- CD or DVD (Vista Premium Ready version)
- Network share

Upgrade to Windows Vista from previous versions of Windows

Not all earlier Windows operating systems are supported for an upgrade or migration to Windows Vista. However, if a computer is currently running a supported version of Microsoft Windows or a different edition of Windows Vista, to the user may upgrade or migrate to a newer or more advanced edition of Windows Vista.

Upgrade

Selecting "Upgrade" from the installation program will perform an in-place upgrade. This option preserves all user settings, data, hardware device settings, applications, and other configuration information automatically. It is always advisable to perform a backup of existing data files before beginning the upgrade process. An in-place Windows Vista upgrade can be performed on the following operating systems:

- Windows 2000
- Windows XP
- Windows Vista

Note: Microsoft recommends that you back up all your important data before performing an upgrade.

Migrate

A migration is appropriate when the user wants a clean installation of Windows Vista while retaining all of the previous installation's settings. Migration is typically used when a user has a new computer running Windows Vista and wants to move their files and settings from their old hardware to the new Windows Vista computer. Follow these steps below to perform a migration:

- Back up the user's files and settings.
- Perform a clean installation or upgrade.
- Restore the user's files and settings.
- Reinstall the applications.

Start a Windows Vista migration by selecting Custom (Advanced) from the installation program and perform a clean installation of Windows Vista. However, to ensure that your computer operating system configuration is migrated, you must first backup user-related settings, application settings, your data, and other system configuration settings, before finally restoring these settings onto your computer when it is running Windows Vista.

Microsoft provides two utilities to assist with the migration process:

- Windows Easy Transfer (WET)
- User State Migration Tool V3.0 (USMT)

Note: When an upgrade is not possible, the Windows Vista installation program prohibits the selection of Upgrade during the installation process.

The following table lists the Windows operating systems that you can upgrade or migrate directly to Windows Vista:

Windows O/S	Scenario	Limitations
2000 Pro	Migration	Windows 2000 Professional does not support an in-place upgrade to editions of Vista
XP *	In-place upgrade	Windows XP Service Pack 2 is required to support in-place upgrades to Vista
Vista	In-place upgrade	Windows Vista supports in-place upgrade to other Windows Vista versions with certain limitations (see Table 1.x)

* You cannot perform an in-place upgrade of all editions of Windows XP to any edition of Windows Vista. For example, you cannot upgrade Windows XP Professional Service Pack 2 to Vista Home Basic edition, but you can upgrade to Vista Business edition. For more information about specific edition-to-edition upgrades, see: http://www.microsoft.com/windowsvista/getready/upgradeinfo.mspx

The table below outlines the upgrade options mapped to the different Windows Vista editions:

Earlier Windows Editions	Windows Vista Editions			
	Home Basic	**Home Premium**	**Business**	**Ultimate**
Windows 2000	Clean install	Clean install	Clean install	Clean install
Windows XP Home	In-place upgrade	In-place upgrade	In-place upgrade	In-place upgrade
Windows XP Professional	Clean install	Clean install	In-place upgrade	In-place upgrade
Windows XP Media Center	Clean install	In-place upgrade	Clean install	In-place upgrade
Windows XP Tablet PC	Clean install	Clean install	In-place upgrade	In-place upgrade
Windows XP Professional x64	Clean install	Clean install	Clean install	Clean install

Upgrade notes:

- If you are currently using Windows 2000 Professional or Windows XP Professional x64, you are eligible for an upgrade copy to a corresponding or better edition of Windows Vista. A clean install is required in this case.
- For versions of Windows earlier than Windows 2000, upgrade copies are not available. Earlier versions of Windows lack the architectural similarity to Windows Vista that both Windows 2000 and Windows XP have. Consequently, there is no direct mechanism for in-place upgrade or migration to Windows Vista from these earlier Windows operating systems. These earlier versions of Windows require you to perform a clean install of a full copy of Windows Vista.
- If the edition of Windows Vista that you choose to install will result in a loss of functionality over your current edition of Windows, a clean install must be done or the installation must be performed on a new partition on your PC.
- The Vista Upgrade Advisor provides assistance in selecting from among the different editions of Vista. The Vista Upgrade Advisor only runs on computers that are running 32-bit versions of either Vista or XP (with Service Pack 2). Additionally, Vista Upgrade Advisor requires both Microsoft Core Extensible Markup Language Services (MSXML) 6.0 and the Microsoft .NET Framework Version 2.0.

Vista Upgrade Advisor performs a scan of the local computer that determines:

- if the computer meets the recommended minimum system requirements
- if the computer has any hardware or device compatibility issues
- if the computer has any application program compatibility issues

The following table details the reports produced by the Vista Upgrade Advisor:

Report Summary	Details
System	This summary indicates whether the computer meets the minimum hardware requirements for the recommended edition of Vista. The report provides information on system memory, DVD drives, hard disk space and the graphics adapter.
Devices	This summary displays the devices installed in the computer and provides information about whether Vista supports these devices; unsupported devices are highlighted.
Programs	This summary highlights problems with applications installed on the computer.

Note: If the Vista Upgrade Advisor highlights a known program compatibility issue, Vista will block the installation of the incompatible program should you attempt to install it after performing a clean install of Vista.

Upgrade from one edition of Windows Vista to another edition

The following table shows the upgrade paths between the different Vista editions:

	Starter	Home Basic	Home Premium	Business	Enterprise	Ultimate
Starter	Repair	Upgrade	Upgrade	Upgrade	Upgrade	Upgrade
Home Basic	Clean install	Repair	Upgrade	Upgrade	Upgrade	Upgrade
Home Premium	Clean install	Clean install	Repair	Clean install	Clean install	Upgrade
Business	Clean install	Clean install	Clean install	Repair	Upgrade	Upgrade
Enterprise	Clean install	Clean install	Clean install	Clean install	Repair	Upgrade
Ultimate	Clean install	Clean install	Clean install	Clean install	Clean install	Repair

Troubleshoot Windows Vista installation issues

Generally, as long as minimum hardware requirements have been met, the Windows Vista installation should be trouble-free. However, if problems do occur, using Microsoft's recommended four-step trouble-shooting approach should help resolve the problem:

1. Determine what has changed.
2. Eliminate possible causes to determine probable cause.
3. Identify a solution.
4. Test the solution.

The following table lists some specific installation problems and their solutions:

Problem	Solution
Error messages appear during setup	Carefully note any messages and search the Microsoft TechNet Knowledge Base for an explanation. The Microsoft TechNet Knowledge Base may be reached here.
Failure to meet mini-mum requirements	Use Windows Catalog to locate products designed for Microsoft Windows and ensure that your hardware meets the minimum requirements for the edition of Windows Vista you want to install.
Improperly installed hardware	Check any messages that appear during the boot phase. Install add-on hardware properly (e.g., video cards and memory modules). If setup encounters a problem during the installation and you suspect a device com-patibility issue, contact the hardware vendor for further assistance.
BIOS upgrade needed	Check your computer supplier's Internet site to see whether a BIOS upgrade is available for Windows Vista. The Windows Vista Upgrade Advisor may highlight any problems with devices or the computer's BIOS, so it is a good idea to run this program on computers that you plan to upgrade or migrate.
Installation media is damaged	Test the CD or DVD on another system.

Log files created during installation are located in the Windows\panther folder. These log files contain clear information about issues and errors encountered during setup. If the computer will not start nor-mally, you can use the Windows Recovery Environment (Windows RE) to start the computer and examine the log files.

Device Driver Troubleshooting

Use the following steps when troubleshooting problems with device drivers in Windows Vista:

1. If you installed a new device, remove the device, and then try to start the computer. If Windows Vista does not start, go to step 2. If Windows Vista starts, go to the Device Manager or check the Event Viewer for additional information.
2. Start the computer, and then press F8 after the POST and before the Vista boot animation. On the *Advanced Boot Options* screen, select *Last Known Good Configuration*, and then press enter. If Windows Vista does not start, go to step 3. If Windows Vista starts, go to the Device Manager or check the Event Viewer for additional information.
3. Start the computer, and then press F8 after the POST and before the Vista boot animation. On the *Advanced Boot Options* screen, select *Safe Mode* and then press enter. If Windows Vista starts in Safe Mode, go to the Device Manager or check the Event Viewer for additional information. If you cannot start Windows Vista in safe mode, you will need to repair Windows Vista using the Windows Recovery Environment.
4. Check this Knowledge Base article for information on instances where Windows Vista may not start after the installation of a device or updating a driver.

Other Installation issues

- Disable existing anti-virus or third party firewall software before beginning an upgrade to Windows Vista. Before beginning the upgrade, it is also advisable to run a check on the existing system for any known virus files.
- If you try to activate the Windows Vista only to get error code 0x8004FE33, you must contact the automated phone system as directed by the Windows Activation Wizard. The cause of this error is a proxy server which is configured to use only basic authentication (alternately, you could try disabling basic authentication on the proxy server).
- Software incompatibility with Windows Vista can cause many application incompatibilities. Use the Microsoft Application Compatibility Toolkit (ACT) 5.0 to verify whether existing software will be compatible with Microsoft Vista.
- If you cannot determine any other cause of the failure, then verify that there is no damage or corruption to the installation media and that the drive you are using to mount the media does not have a hardware fault.
- For additional information on troubleshooting installation problems with Aero, see this article.

Install and configure Windows Vista drivers

Hardware devices will not work without a suitable device driver. Windows Vista automatically downloads drivers and critical fixes during the setup process to ensure that your setup is trouble-free.

Device drivers are specialized, hardware-dependent software that are also specific to an operating system. The device drivers that are included with Windows Vista have a Microsoft digital signature. The digital signature indicates that a particular driver or file has met a certain level of testing and is stable and reliable.

Device drivers are:

- Bundled with Windows Vista.
- Supplied with a device.
- Updated with Windows Update.
- Updated for the manufacturer's Internet site.

Using Device Manager

The Device Manager tool in Windows Vista helps you manage and configure devices. It is the first tool you should use when troubleshooting devices.

By using the Device Manager tool, you can perform the following tasks:

- **View a list of installed devices**. The Device Manager tool shows all devices that are currently installed. This device list is re-created after every system restart or dynamic change.
- **Uninstall a device**. The Device Manager tool can be used to uninstall the device driver and remove the driver software from the computer.
- **Enable or disable devices**. If you want a device to remain attached to a computer without being enabled, you can disable the device instead of uninstalling it. Disabling a device differs from uninstalling one because only the drivers are disabled -- the hardware configuration is not changed.
- **Troubleshoot devices**. If a device is not operating correctly, you can use the Device Manager tool as part of your troubleshooting process. For example, you may see a device listed as Unknown Device next to a yellow question mark if the operating system cannot locate a suitable driver for the device.
- **Update device drivers**. If you have an updated driver for a device, you can use the Device Manager tool to apply the updated driver.
- **Roll back drivers**. If you experience system problems after you update a driver, you can roll back to the previous driver by using driver rollback. This handy feature enables you to reinstall the last device driver that was functioning before the installation of the current (and possibly faulty) device driver.

Plug-and-Play

Windows has supported Plug-and-Play (PnP) since Windows 9x. Windows Vista provides improved support for evolving technologies, including Peripheral Component Interconnect Express (PCIe) and hot-add memory. It is important to understand how PnP works when troubleshooting any issues encountered with hardware devices.

When you install a new device, Windows Vista will recognize and configure it. In order to support PnP, devices must contain configuration and driver information. Windows Vista reads this information when the device is attached and completes the configuration so that the device works properly with other installed devices.

The detection of the device depends on the type of device you install:

- For Universal Serial Bus, IEEE 1394 (FireWire) and Small Computer System Interface (SCSI) devices, you plug in the devices and Windows Vista will detect these devices automatically.
- For Peripheral Component Interconnect (PCI) and Accelerated Graphics Port (AGP) PnP cards, you must turn the computer off to install the device. Windows Vista will detect these devices on restart.

If a driver is not available on the system, Windows Vista will prompt you for it and you must provide the media or a path to the driver.

Dynamic Update

Dynamic Update is a feature of Vista Setup that works with Windows Update to download any critical fixes and device drivers that are required during the setup process. Dynamic Update downloads new drivers for devices required by setup that are connected to the computer.

Dynamic Update downloads the following types of files:

- **Critical Updates**: Dynamic Update replaces files from the Vista operating system DVD that require critical fixes or updates. Dynamic Update also replaces DLLs that Setup requires. The only files that are downloaded are those that replace existing files; no new files are downloaded.
- **Device drivers**: Dynamic Update only downloads drivers that are not included on the operating system CD or DVD. Dynamic Update does not update existing driver; however, you can obtain these by connecting to Windows Update after setup is complete.

The main purpose of Dynamic Update is to ensure that the setup process has the latest fixes. This ensures a smooth installation. Dynamic Update was not designed to be a replacement for Windows Update. After the installation is complete you should still use Windows Update to download all your other drivers and to keep your system safe with the latest security updates from Microsoft.

Configuring and Troubleshooting Post-Installation System Settings

Troubleshoot post-installation configuration issues

Most post-installation issues can be resolved by using the System Configuration tool. You can use this tool to help identify problems that might prevent Windows from starting correctly.

Note: System Configuration is intended to find and isolate problems, but it is not meant as a startup management program.

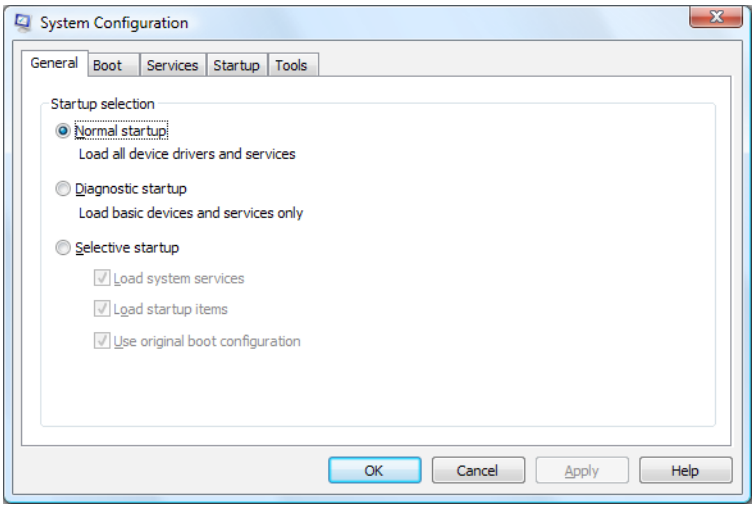

Figure 1 – System Configuration

The General tab of the System Configuration allows you to select startup modes for Windows Vista. Both the Diagnostic startup and Selective startup modes can be used to help isolate post-installation configuration issues.

- Use the Diagnostic startup mode to determine if there is a problem with Windows files or device drivers. If a problem occurs in the Diagnostic startup mode then you should search Windows Help and Support for the topic "Startup Repair." If a problem does not occur, then use the Selective startup mode.
- Use the Selective startup mode to try and find a problem by turning individual services and startup programs on or off. Follow the steps below to complete the diagnostic process:
    - From the **General Tab**, click **Selective Startup** and then clear the **Load Startup Items** check box.
    - Ensure that the **Load System Services** check box is selected, click OK, and then click Restart.

- If the problem occurs after restarting, perform the following steps to identify the service that is causing the problem:
  - Select the **Services Tab** within System Configuration and click **Disable All**. Then, select the check box for the first service listed and restart the computer. If the problem does not occur, then you can eliminate the first service as the cause of the problem.
  - With the first service selected, select the second service check box, and then restart the computer.
  - Repeat this process until you reproduce the problem. If you cannot reproduce the problem, then you can eliminate the system services as the cause of the problem.
- If a system service is not the source of the problem, then perform the following steps to identify the startup item that is causing the problem:
  - Select the **Startup** Tab within System Configuration and click Disable all. Then, repeat the same process of elimination performed for system services for the startup items (i.e., enable each startup item per restart until the problem is reproduced).

Configure and troubleshoot Windows Aero

Windows Aero overview

The Aero Desktop is a new feature included in Microsoft Windows Vista Home Premium, Business, Enterprise or Ultimate, and is designed to make it easier for users to work within multiple applications and to locate documents and information on their computer. These features range from simple graphical improvements, such as window transparency, to the fully redesigned multitasking system, Windows Flip 3D.

A basic user interface is included for computers running Microsoft Windows Vista Home Basic and for computers without the hardware required to run Windows Aero.

The following table details the different Microsoft Windows Vista user experiences:

Experience	Features
Windows Aero	• Transparent glass • Taskbar thumbnails • Windows Flip • Windows Flip 3D • Smooth window animations
Standard	• Desktop Composition (smooth window re-draw) • Increased stability • User interface scaling (higher DPI support)

Basic	• Redesigned Start Menu • Streamlined Explorers • Live icons • Preview/reading pane • New wizard/dialogs
Windows Classic	• Windows 2000 look and feel

Aero is designed to be very reliable. Open windows glide across the screen when they are moved or resized, and redraw artifacts, latency, or the tearing effects that sometimes occurred with earlier operating systems have been completely eliminated. The Aero experience also reduces graphics driver-related system crashes and unexpected stops.

Configuring Windows Aero

Aero's most noticeable feature is the translucent glass effect, which displays dynamic reflections and provides smooth animations. The glass effect was designed to allow users to focus on the content of a window, while providing better context for the surrounding elements on the desktop. The environment may be personalized by configuring the following settings:

- The color of the windows.
- The amount of saturation of the screen colors.
- The level of the window transparency.

Windows Flip 3D lets you dynamically flip through all your open windows to quickly and visually work with many programs at a time.

Troubleshooting Windows Aero

If a WDDM (Windows Driver Display Model) graphics card is present, Windows Vista enables the Windows Aero interface. If a compliant graphics card is not present, Windows Vista will run, but the computer will be restricted to the basic interface. The manufacturer of your video card should provide Aero-compatible drivers. Check the video card manufacturer's website for more information.

These are some solutions to other common problem with running Windows Aero:

- How to determine if a computer is able to run Windows Aero.
    - Ensure that the selected edition of Windows Vista can run Aero (see the first paragraph of this section).
    - To determine which edition of Windows Vista is on a computer, do the following:
        - Open the Welcome Center by clicking the **Start** button.
        - Click **Control Panel**.
        - Click **System and Maintenance**.
        - Click **Welcome Center**.
        - The edition of Windows Vista is displayed along with the computer details near the top of the window.

- The correct edition of Windows Vista is installed, but the system is unable to run Aero.
  - Ensure the computer meets the minimum hardware requirements for running Aero:
    - 1 gigahertz (GHz) 32-bit (x86) or 64-bit (x64) processor.
    - 1 gigabyte (GB) of random access memory (RAM).
    - 128 megabyte (MB) graphics card.
    - Aero also requires a DirectX 9 class graphics processor that supports the Windows Display Driver Model Driver, hardware Pixel Shader 2.0, and 32-bit color per pixel.
  - For the best results, follow these graphics processor recommendations:
    - 64 MB of graphics memory to support a single monitor with a resolution that is less than 1,310,720 pixels (for example, a 17–inch flat panel LCD monitor that has a 1280 × 1024 resolution).
    - 128 MB of graphics memory to support a single monitor with a resolution from 1,310,720 to 2,304,000 pixels (for example, a 21.1–inch flat panel LCD monitor that has up to a 1600 × 1200 resolution).
    - 256 MB of graphics memory to support a single monitor with a resolution greater than 2,304,000 pixels (for example, a 30–inch wide-screen flat panel LCD monitor that has up to a 2560 × 1600 resolution).
- The computer meets the minimum recommendations, but still does not show Windows Aero.
  - Ensure that the color is set to 32 bit, the monitor refresh rate is higher than 10 hertz, the theme is set to Windows Vista, the color scheme is set to Windows Aero, and window frame transparency is on. All of the settings below may be reached by navigating to **Start -> Control Panel -> Appearance and Personalization -> Personalization**. For each individual setting, follow the instructions below:
    - To set the color to 32 bit: Select **Display Settings**. Under **Colors**, click **Highest (32 bit)**. Click **OK**. If you can't select 32 bit color, ensure that the screen resolution is at the highest possible setting and try again.
    - To set the monitor refresh rate: Select **Display Settings** followed by **Advanced Settings**. Open the **Monitor** tab and then change the refresh rate to a setting higher than 10 hertz. Click **Apply**. The monitor will then adjust, followed by a message asking if you would like to keep your changes. Click **Yes**. If you do not respond to this message within 15 seconds, the refresh rate will revert to its previous setting. Click **OK** (changes to the refresh rate affect all users on the computer).
    - To change the desktop theme to Windows Vista: Select **Theme**. In the theme list, click **Windows Vista** and then click **OK**.
    - To change the color scheme to Windows Aero: Select **Windows Color and Appearance**. If the Appearance Settings dialog box is not displayed, at the bottom of the page, click **Open classic appearance properties**. In the **Color scheme** list, click **Windows Aero** followed by **OK**.
    - To turn on window frame transparency: Select **Window Color and Appearance** followed by the **Enable transparency** check box. If you see the Appearance Settings dialog box instead of the Window Color and Appearance window, the theme might not be set to Windows Vista, the color scheme might not be set to Windows Aero, or the computer might not meet the minimum hardware requirements for running Windows Aero.

- A new video card meeting the requirements for running Aero has been installed, but Windows Aero still does not display.
    - If the graphics card and driver were installed after Windows Vista was first set up, depending on the manufacturer, you might need to update the computer's performance score, which will automatically enable Aero.
        - To update your computer's performance score: Navigate to **Start -> Control Panel -> System and Maintenance -> Performance Information and Tools**. Click **Update my score**. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.
- Windows Aero will not consistently display Aero glass.
    - If you are running the Power saver plan, Windows sometimes turns off transparency automatically. If you don't want this to happen, you can switch to the Balanced power plan.
        - To change an existing power plan: Navigate to **Start -> Control Panel -> System and Maintenance -> Power Options**. On the **Select a power plan** page, click **Balanced**. Click **OK**.

Configure and troubleshoot parental controls

Configuring and troubleshooting Parental Controls

Before you get started, make sure that each child has a standard user account. Parental Controls can only be applied to standard user accounts. To set up Parental Controls for your child, you'll need an Administrator user account.

Follow the steps below to turn on Parental Controls for a standard user account:

- Open Parental Controls by navigating to **Start -> Control Panel -> User Accounts -> Setup Parental Controls**. Administrator permission is required. If you are prompted for a administrator password or confirmation, type the password or provide confirmation.
- Select your child's standard user account.
- Under **Parental Controls**, click **On**.
- Once you've turned on Parental Controls, you can adjust the individual settings that you want to control:
    - **Web restrictions**. You can restrict the websites that children can visit, make sure children only visit age-appropriate websites, indicate whether you want to allow file downloads, and set up which content you want the content filters to block and allow. You can also block or allow specific websites.
    - **Time limits**. You can set time limits to control when children are allowed to log on to the computer. You can set different logon hours for every day of the week. For more information, see Control when children can use the computer.
    - **Games**. You can control access to games, choose an age rating level, choose the types of games you want to block, and decide whether you want to allow or block unrated or specific games. For more information, see Specify which games children can play.
    - Allow or block specific programs. You can prevent children from running programs that you don't want them to run. For more information, see Prevent children from using specific programs.

It is important to remember that you cannot set Parental Controls on a computer administrator account. In domain-attached versions of Vista, this tool is called simply User Accounts and you cannot set Parental Controls on a domain-based user account. To apply Parental Controls to a user, the user must have a local, standard user account.

Configure Windows Internet Explorer

Configuring Internet Explorer

Internet Explorer can be customized to suit a user's working environment and preferences by using settings in the Internet Options dialog box.

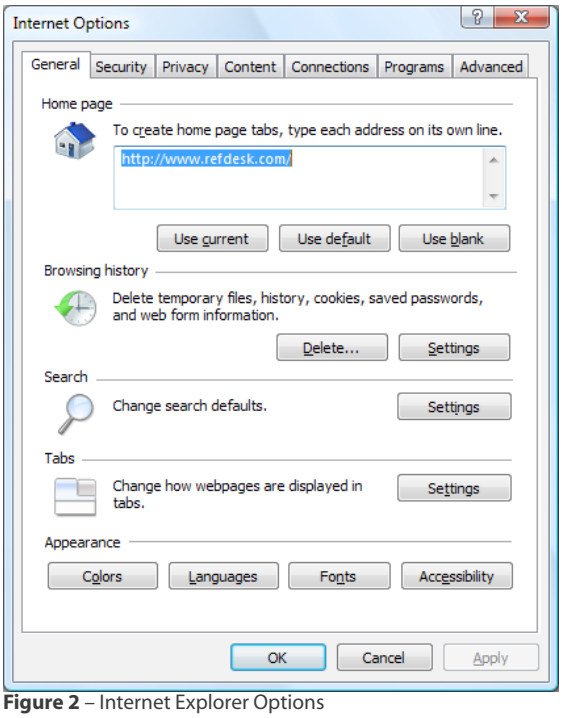

Figure 2 – Internet Explorer Options

The following table describes the most common configuration options available for Internet Explorer 7.0:

Tab	Settings
General	• **Home page**: specify a single page or a set of pages to open on multiple tabs when Internet Explorer opens. • **Browsing history**: delete sensitive information such as temporary files, history, cookies, saved passwords, and Web form information. • **Search**: set the default search provider used by the Instant Search box. • **Tabs**: configure tab behavior, or disable tabbed browsing. • **Appearance**: configure the colors, languages, fonts and accessibility settings.
Security	• **Security Zone configuration**: customize security levels for each security zone. • **Default level**: Reset a single zone to default security level. • **Reset all zones to default level**: reset all zones to default security levels.
Privacy	• Settings: set an overall level for cookies on your computer, and customize the level for individual Web sites. • Pop-up Blocker: enable or disable the Pop-up Blocker, and customize settings for individual Web sites.
Content	• **Content Advisor**: set ratings for acceptable content on this computer and set a supervisor password to allow settings to be changed or overridden. • **Certificates**: manage certificates used for encrypted connections and identification. • **AutoComplete**: store previous entries on Web sites and have matches suggested. • **Feeds**: configure frequency of updates and Internet Explorer behavior when a feed is detected.
Connections	• Dial-up and Virtual Private Network Settings: configure settings for connecting to the Internet by using a VPN or Dial-up connection. • Local Area Network (LAN) Settings: configure settings for connecting to the Internet by using a LAN, and set automatic configuration options.
Programs	• **Internet Programs**: specify default HTML Editor, E-mail, Newsgroups, **Internet** call, Calendar, and Contact List programs. • **Default Web Browser**: Set Internet Explorer as the default Web browser. • **Manage Add-ons**: enable or disable add-ons, view add-ons currently loaded, add-ons that run without requiring permission, and downloaded ActiveX controls.

Advanced	• **Advanced Settings**: configure detailed settings for Internet Explorer. • **Reset Internet Explorer settings**: reset all Internet Explorer settings to defaults - disables toolbars and add-ons, deletes temporary Internet files, history, cookies and passwords, and resets Web browser settings, search providers, and homepages. For more information, see the section on **Reset Internet Explorer Settings**, below.

Troubleshooting Internet Explorer

Perhaps one of the most common problems associated with Internet Explorer can be summed up in one question: "Why is my Internet connection so slow?"

The type of Internet connection you use is the most important factor in determining your connection speed. The three most common ways to connect to the Internet from home are dial-up, DSL and cable. If you have a choice, cable is usually the fastest; however, both DSL and cable are faster than dial-up.

If you use a dial-up connection, there are a couple of ways to optimize your Internet speed. First, use the fastest modem you can. The fastest modem on the market sends and receives information at a rate of 56 kilobits per second (Kbps). You won't get a full 56 Kbps speed most of the time, but a good dial-up service will provide several access numbers and a way to optimize which number your modem dials. In this way, you should be able to get speeds at around 45-50 Kbps.

Second, make sure that your phone line is in good condition. If the telephone wiring in your home or business is old or deteriorating, you might be picking up stray signals or cross talk from other phone lines. These problems will slow your Internet connection because the modem will have to send the same information over and over until it is transmitted without interruption. Check your telephone wires to ensure they are not damaged, frayed or twisted around power or other telephone cables. If you notice crackling in your phones, you might want to contact your phone provider to have them check the lines inside and outside your home to make sure they are in good condition.

The health of your computer can affect your Internet connection. Spyware and viruses can cause speed-related problems. Additionally, your Internet connection speed can be affected by add-on programs, the amount of memory the computer has, hard disk space and condition, and active programs.

Two of the most frequent causes of poor Internet performance are spyware and viruses. Spyware can slow your system by interfering with your browser and monopolizing your Internet connection. Spyware monitors your Internet use and keystrokes, which adds delays. The problem is compounded when there are multiple spyware programs running at the same time. If the problem is severe enough, you can lose connectivity altogether. To get your Internet performance back, you should regularly run an anti-spyware program.

Computer viruses can also cause poor Internet performance. When a virus infects a computer, it installs computer code which will attempt to propagate itself, usually by sending copies of itself through e-mail. Some viruses can multiply at the rate of hundreds of e-mail messages per minute, which leaves little computing power and Internet connection bandwidth for anything else. Viruses often do not give any obvious indication that they are running, so it is best to run your anti-virus software at all times.

Browser add-ons also cause performance problems. Browser add-ons are programs (such as multimedia add-ons or search bars) that usually appear on your browser's toolbar. Many browser add-ons can add to a rich browsing experience, offering multimedia or specialized document viewing. However, some add-ons can slow your Internet connection. If you suspect that add-ons are causing slow performance, try starting Internet Explorer in Add-ons disabled mode. Add-ons are disabled only for the session, but if you find your performance improves, you can use the Add-on Manager to turn them off permanently. To access the Add-on Manager from Internet Explorer, click Tools, and then click Add-on Manager.

Like all computer programs, Internet Explorer requires a certain amount of computing power, memory, and disk space to run efficiently. Every webpage you view is first downloaded to memory and then saved to temporary disk files. Running another program that is using lots of memory and computing power can compete with Internet Explorer and cause delays. If you find your Internet connection running slowly and you have other programs running, try closing them. If you want to run several programs, consider increasing the memory you have on your computer. Low disk space can also cause performance problems. You can increase your disk space by deleting Internet Explorer's temporary files.

Reset Internet Explorer settings

Occasionally, settings get changed in Internet Explorer that could possibly affect how Internet Explorer works. You can reset Internet Explorer to its default settings. By resetting Internet Explorer settings, you return it to the state it was in when it was first installed on your computer. This is useful for troubleshooting problems that might be caused by settings that were changed after installation. When you restore Internet Explorer's default settings, some Web pages that rely on previously stored cookies, form data, passwords, or previously installed browser add-ons might not work correctly. Resetting Internet Explorer to its default settings does not delete your favorites, feeds and a few other personalized settings.

Resetting Internet Explorer's settings is not reversible. After a reset, all previous settings are lost and cannot be recovered. Rather than resetting everything, you might want to reset specific settings or delete your webpage history.

If you purchased your computer with Windows already installed, any settings the manufacturer specified will be reapplied. These settings might include a specific home page or search provider.

The following table describes what will happen to various settings when you reset Internet Explorer:

Settings categories	Items affected
Settings that are deleted	• Browser history, temporary Internet files, cookies, form data, and stored passwords. • Typed URL information, offline Web pages, menu extensions. • Web sites added to intranet, trusted, or restricted zones. • Web sites added for special cookie handling under the Privacy tab. • Web sites allowed to use pop-ups under Pop-up Blocker settings. • Explorer most recently used list.

Settings that are reset to Windows or manufacturer defaults	• Home page. • Search providers, tabbed browsing settings. • Colors, languages, fonts and accessibility settings (General tab). • Security settings for all zones (Security tab). • Advanced tab settings. • Privacy tab settings. • Pop-up blocker, AutoComplete, Phishing Filter, and Zoom settings. • Page setup, toolbar, and text size settings. • Feeds settings (sync and notification, not feeds themselves). • ActiveX controls that are not on the pre-approved list (reset to opt-in state). • Toolbars, browser helper objects, and browser extensions are disabled.
Settings and items that are maintained	• Favorites. • Feeds. • Content Advisor settings. • Pre-approved ActiveX controls. • Temporary Internet file (cache) path settings. • Certificate information. • Internet Programs (e-mail, instant messenger, and other programs associated with Internet use). • Internet connection, proxy, and VPN settings. • Default web browser setting. • Toolbars are not restored.

Follow the steps below to reset Internet Explorer settings:

1. Close any Internet Explorer or Windows Explorer windows that are currently open.
2. Navigate to **Start -> Internet Explorer -> Tools -> Internet Options**.
3. Click the **Advanced** tab, and then click **Reset**.
4. In the **Reset Internet Explorer Settings** dialog box, click **Reset**.
5. When Internet Explorer finishes restoring the settings, click **Close**, and then click **OK**.
6. Close Internet Explorer.

Your changes will take effect the next time you open Internet Explorer.

Notes

- If you close all visible windows, but still get an error message when trying to reset, you might have programs running that are not visible. Restart Windows, open Internet Explorer, and try resetting again.
- If any of the categories fail to reset, it is because Internet Explorer could not access a file or registry setting. This can be caused by insufficient security privileges, files or settings being used by another program, or low memory or high CPU usage. Restart your computer and try again.
- If you are using Internet Explorer on a server and have turned off hardening (stronger security settings for use on servers), reset will go to client level security. You must reinstall hardening if you want the increased security level.

Configuring Windows Security Features

Windows Vista grants a new, larger set of permissions to the User group than previous editions of Windows so that users with accounts in that group can perform the most commonly used tasks. These permissions can be modified by editing the local security policy or by deploying a new group policy. Microsoft has evaluated these additional permissions and rights for their security impact on a computer. Surveys were performed that indicated that as many as 80% of all users have full administrative access to their desktops. Many necessary tasks require this level of access.. The increased permission control methods introduced with Windows Vista have been designed to reduce this figure significantly, with the added benefit of reducing the risk of malicious system damage as well.

The following table lists the additional privileges that have been granted to standard user accounts:

New Privilege	Function
View System Clock and Calendar	In earlier versions of Windows, users could not view the System Clock and Calendar. They still cannot change the date and time, because it may be needed for login time restrictions and to timestamp audit logs.
Change Time Zone	Users can change the time zone when traveling.
Install Wired Equivalent Privacy (WEP) to connect to secure wireless networks	Users can connect to public WiFi networks and use encryption to protect their data.
Change Display settings	Users can configure the computer display according to their needs.
Change Power Management settings	Users can adjust power schemes to optimize battery life based on vari9ous usage scenarios.
Install Fonts	Users can update fonts, which are held in a protected location.

Add printers and other devices that have the required drivers installed on the computer or are provided by an IT administrator	Users can install pre-approved devices that use Plug-and-Play (PnP) technology.
Create and configure a Virtual Private Network (VPN) connection	Users can create an encrypted connection to their workplaces.
Download and install updates using User Account Control compatible installer	Users can install critical updates to ensure the integrity of laptops if they are disconnected from the corporate network for an extended amount of time.

Configure and troubleshoot User Account Control.

User Account Control overview

Earlier versions of Windows came with three, built-in classes of users, each with a different set of privileges. These user classes were:

- **Administrators** – this account had all privileges.
- **Power Users** – this account had more privileges than Users, but fewer than Administrators.
- **Users** – this account had the most basic set of privileges.

Windows Vista, unlike previous versions of Windows, has both standard users and administrators access resources and run applications in the security context of standard users by default. You can then raise the privilege level of a standard user account by entering valid administrator credentials. You cannot use the privileges of an administrator account unless you confirm it through the UAC confirmation dialog box. This feature reduces the exposure and attack surface of the operating system by requiring that all users run as standard users (the set of users with the least privilege).

Configuring User Account Control

Enable or disable UAC

An administrator has the ability to turn User Account Control (UAC) on or off. The UAC is turned on by default in Windows Vista. Follow the steps below to enable or disable UAC:

1. Navigate to **Start -> Control Panel -> User Accounts**. Click **User Accounts**.
2. In the User Accounts tasks window, change **Turn User Account Control** to on or off, depending on your preference.
3. If UAC is currently configured in Admin Approval Mode, the User Account Control message appears. Click **Continue**.
4. The User Account Control dialog box appears. Do one of the following:
    - **To disable UAC**, clear the Use User Account Control (UAC) to help protect your computer check box.
    - **To enable UAC**, select the Use User Account Control (UAC) to help protect your computer check box.
5. Click **OK**.

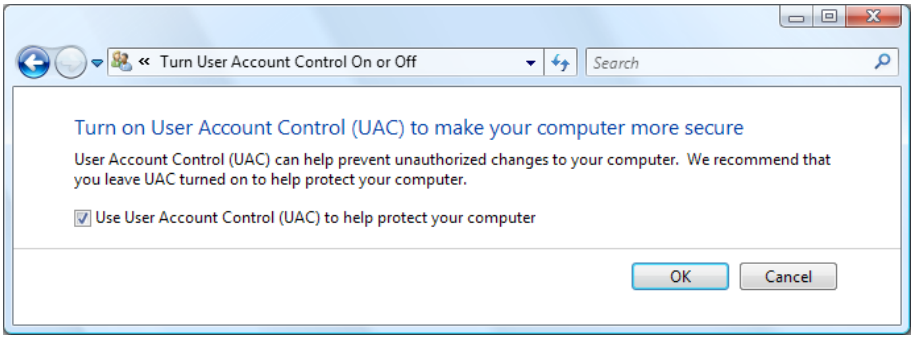

Figure 3 – User Account Control configuration

Administering UAC with the local Security Policy Editor and Group Policy
Prior to Windows Vista, standard users working on a personal computer or in a network setting often had the option of installing applications. The key difference then was that, although administrators could create Group Policy settings to limit application installations, they did not have access to limit application installations for standard users as a default setting. In a UAC environment, administrators do have this ability. Administrators can still use Group Policy to define an approved list of devices and deployment.

There are nine Group Policy object (GPO) settings that can be configured for UAC along with their default values:

- **Switch to the secure desktop when prompting for elevation**
  - There are two possible settings for this GPO:
    - **Enabled** – The built-in Administrator will be run as an administrator in Admin Approval Mode.
    - **Disabled** – The Administrator runs with a full administrator access token.
- **Behavior of the elevation prompt for administrators in Admin Approval Mode**
  - There are three possible values for this GPO:
    - **No prompt** – The elevation occurs automatically and silently. This option allows an administrator in Admin Approval Mode to perform an operation that requires elevation without consent or credentials. Note: this scenario should only be used in the most constrained environments and is NOT recommended.
    - **Prompt for consent** – An operation that requires a full administrator access token will prompt the administrator in Admin Approval Mode to select either Continue or Cancel. If the administrator clicks Continue, the operation will continue with their highest available privilege.
    - **Prompt for credentials** – An operation that requires a full administrator access token will prompt an administrator in Admin Approval Mode to enter an administrator user name and password. If the user enters valid credentials, the operation will continue with the applicable privilege.

- **Behavior of the elevation prompt for standard users**
  - There are two possible values for this GPO:
    - **No prompt** – No elevation prompt is presented and the user can only perform administrative tasks by using "Run as administrator" or by logging on with an administrator account. Most enterprises running standard-user desktops as standard user will configure the "No prompt" policy to reduce help desk calls.
    - **Prompt for credentials** – An operation that requires a full administrator access token will prompt the user to enter an administrative user name and password. If the user enters valid credentials the operation will continue with the applicable privilege.
- **Detect application installations and prompt for elevation**
  - There are two possible values for this GPO:
    - **Enabled** – The user is prompted for consent or credentials when Windows Vista detects an installer.
    - **Disabled** – Application installations will silently fail or fail in a non-deterministic manner. Enterprises running standard-user desktops that leverage delegated installation technologies like GPSI or SMS will disable this feature. In this case, installer detection is unnecessary and therefore not required.
- **Only elevate executables that are signed and validated**
  - There are two possible values for this GPO:
    - **Enabled** – Only signed executable files will run. This policy will enforce PKI signature checks on any interactive application that requests elevation. Enterprise administrators can control the administrative application allowed list through the population of certificates in the local computers Trusted Publisher Store.
    - **Disabled** – Both signed and unsigned code will be run.
- **Only elevate UIAccess applications that are installed in secure locations**
  - There are two possible values for this GPO:
    - **Enabled** – The system will only give UIAccess privileges and user rights to executables that are launched from under %ProgramFiles% or %windir%. The ACLs on these directories ensure that the executable is not user-modifiable (which would otherwise allow elevation of privilege). UIAccess executables launched from other locations will launch without additional privileges (i.e. they will run "asInvoker").
    - **Disabled** – The location checks are not done, so all UIAccess applications will be launched with the user's full access token upon user approval.
- **User Account Control: Run all administrators in Admin Approval Mode (Note: Changing this setting will require a system reboot).**
  - There are two possible values for this GPO:
    - **Enabled** – Both administrators and standard users will be prompted when attempting to perform administrative operations. The prompt style is dependent on policy.

        - **Disabled** – UAC is essentially "turned off" and the AIS service is disabled from automatically starting. The Windows Security Center will also notify the logged on user that the overall security of the operating system has been reduced and will give the user the ability to self-enable UAC.

- **Switch to the secure desktop when prompting for elevation**
    - There are two possible values for this GPO:
        - **Enabled** – Displays the UAC elevation prompt on the secure desktop. The secure desktop can only receive messages from Windows processes, which eliminates messages from malicious software.
        - **Disabled** – The UAC elevation prompt is displayed on the interactive (user) desktop.
- **Virtualize file and registry write failures to per-user locations**
    - There are two possible values for this GPO:
        - **Enabled** – This policy enables the redirection of pre-Windows Vista application write failures to defined locations in both the registry and file system. This feature mitigates those applications that historically ran as administrator and wrote runtime application data back to %ProgramFiles%; %Windir%; %Windir%\system32; or HKLM\Software\.... This setting should be kept enabled in environments that utilize non-UAC compliant software. Applications that lack an application compatibility database entry or a requested execution level marking in the application manifest are not UAC compliant.
        - **Disabled** – Virtualization facilitates the running of pre-Windows Vista (legacy) applications that historically failed to run as a standard user. An administrator running only Windows Vista compliant applications may choose to disable this feature as it is unnecessary. Non-UAC compliant applications that attempt to write %ProgramFiles%; %Windir%; %Windir%\system32; or HKLM\Software\.... will silently fail if this setting is disabled.

To configure UAC Group Policy settings, navigate to **Start -> Run** and type secpol.msc and click **OK**. Under **Security Settings**, expand **Local Policies** and select **Security Options**. In the **details pane** (the right pane), **right-click** the relevant UAC setting and select **Properties** from the context menu. Use the drop-down list box to choose the appropriate value for the setting.

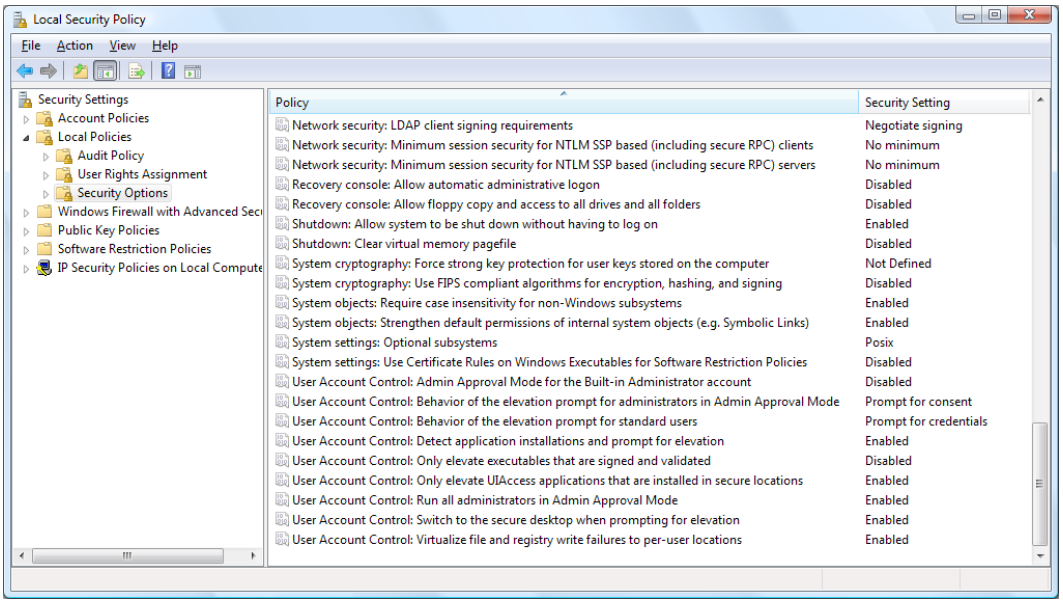

Figure 4 – Local Security Policy, UAC Security Options

Configuring application compatibility for UAC
Applications that are compatible with Windows Vista are designed with the User Account Control (UAC) system in mind. These applications contain functionality that allows them to interact with the UAC and request privilege elevation when necessary; however, you will need to configure legacy applications to request UAC privilege elevation by using the application compatibility tab.

There are several compatibility options available under the application compatibility tab, including "Run this program as an administrator." When you select this option, you are configuring the application to use the UAC system to request privilege escalation. It is important to note that this setting only applies to the account of the currently logged-on user, and no other users are affected by it. Also, you can only configure this option if you have administrator privileges.

If you need to configure a legacy application for multiple users, select the "Show settings for all users" option on the application compatibility tab. This allows an administrator to set compatibility for a legacy application that was used by many users without having to set the option for each account separately.

Troubleshooting User Account Control

When troubleshooting problems with User Account Control (UAC), you many need to perform the following actions:

- Change an account type.
- Configure UAC policy settings.
- Disable the UAC.

Note: To help ensure a safer computing experience, the UAC service and policy must not be disabled or degraded. Window Security Center (WSC) monitors the status of UAC and notifies the user if UAC has been changed to a setting different from what Microsoft recommends. WSC provides a button to restore UAC to the recommended settings in this case.

Configure Windows Defender.

Windows Defender overview

Windows Defender (formerly known as Windows AntiSpyware) is a feature of Windows Vista that helps protect your PC by regularly scanning your computer's hard drive and offering to remove any spyware or other potentially unwanted software that it finds. It also provides always-on protection that monitors key system locations, watching for changes that signal the presence of spyware and checking any files accessed against a constantly updated database of known spyware.

Note: Windows Vista does not include real-time (also known as "on-access") virus protection. Windows Defender complements antivirus software and is not a substitute for third-party antivirus software such as Windows Live OneCare or the applications offered by third party security companies.

Configuring Windows Defender

Update definitions

When you use Windows Defender, it's important to have up-to-date definitions. Definitions are files that act like an ever-growing encyclopedia of potential software threats. Windows Defender uses definitions to determine if software is spyware or other potentially unwanted software, and then alerts you to potential risks. To help keep your definitions up to date, Windows Defender works with Windows Update to automatically install new definitions as they are released. You can also set Windows Defender to check online for updated definitions before scanning.

Scanning options

While Windows Defender includes automatic scanning options to provide regular spyware scanning, you can perform on-demand scanning. The following table lists the scanning options available with Windows Defender:

Scanning Option	Description
Quick Scan	Checks areas on a hard disk that spyware is most likely to infect.
Full Scan	Checks all critical areas, including all files, the registry, and all currently running applications.
Custom Scan	Enables users to scan specific drives and folders.

By default, Windows Defender scans your computer for spyware every day at 2 a.m. unless otherwise specified. During the scan, Windows Defender automatically takes action on high, medium and low alert items, depending on your preferences.

You can also quickly scan the most common locations, such as Program Files and Internet Explorer browser Help objects on your computer at any time by clicking the Scan button. Generally, a quick scan can detect the most common spyware on your computer. You can also elect to perform a full system scan, which takes longer, but examines your entire computer for signs of spyware using a more comprehensive definition set. You can also specify a custom scan using the drop-down menu to scan specific areas of your computer, such as removable storage.

Once a scan is complete, Windows Defender notifies you of any spyware it discovers on your computer. It then prompts you with options for dealing with each threat and recommends appropriate action in most cases.

There are four basic actions you can take if a threat is detected:

- **Ignore**: No action is taken, but the potential threat will continue to be detected in future scans.
- **Quarantine**: Backs up the software in a safe location and then removes it. This prevents the software from running, but it can be restored if needed.
- **Remove**: Deletes the software from the computer entirely.
- **Always Allow**: Adds the software to the "allowed items" list. It will not be detected in future scans.

Windows Defender can scan and remove software even if the user running it is not an administrator—by default, non-administrators can take action on detected items. They can choose to remove, quarantine or ignore items.

Application options

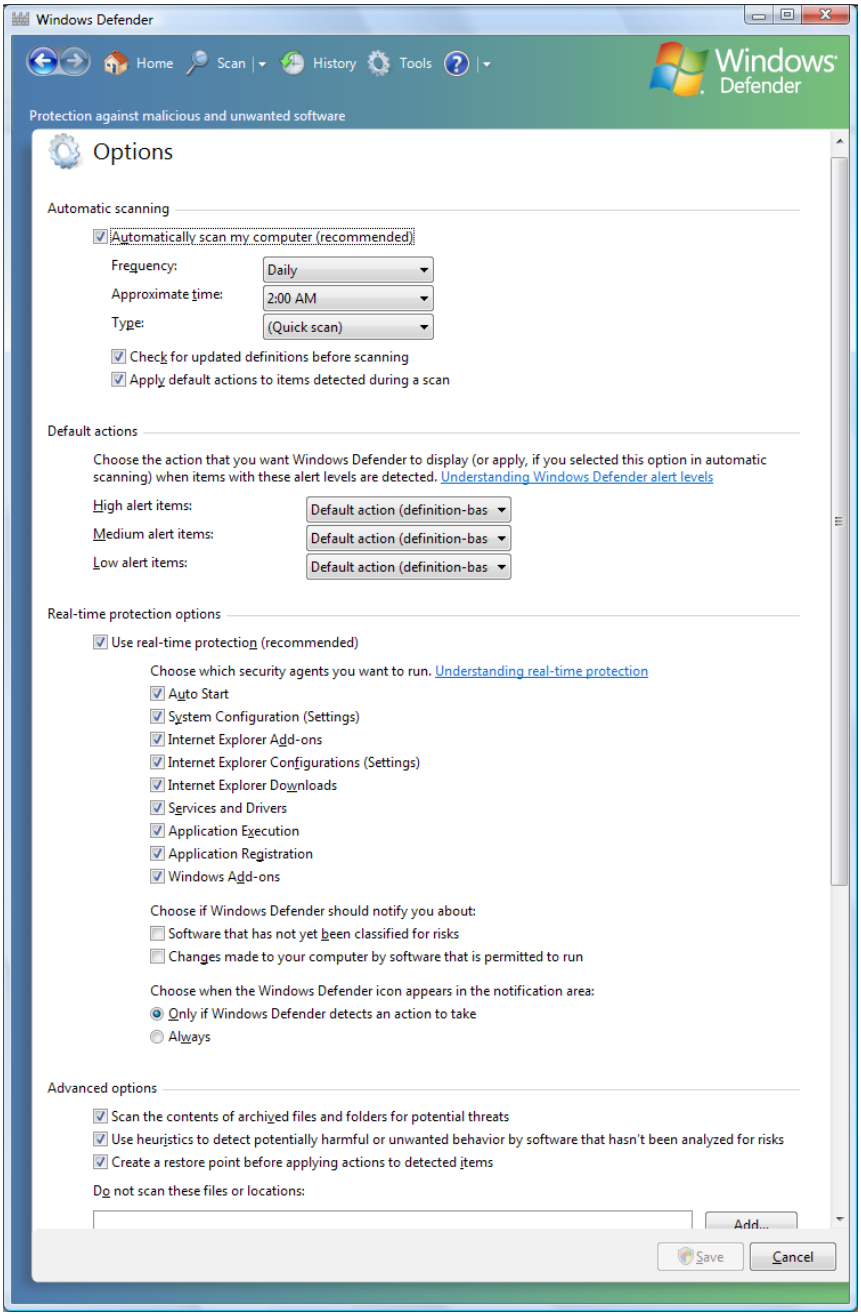

Figure 5 – Windows Defender application options

Follow the steps below to configure the options for Windows Defender, navigate to **Start -> Control Panel -> Windows Defender -> Tools -> Options**. Under **Real-time protection** options, select the **Use real-time protection (recommended)** check box. Select the options you want. To help protect your privacy and your computer, we recommend that you select all real-time protection options. Under "Choose if Windows Defender should notify you about," select the options you want, and then click **Save**. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.

Command line
Windows Defender can be managed from the command line. The MpCmdRun.exe utility enables the configuration and execution of Windows Defender scans. Some of the MpCmdRun.exe utility options are detailed below:

MpCmdRun.exe [command] [-options]

- **Scan** [-ScanType]
  - Runs Scan, either quick scan or full system scan.
- SignatureUpdate
  - Checks for new signature definition updates.
- GetFiles
  - Collects all relevant logs for support.
- **RemoveDefinitions** [-All]
  - Removes definition updates. This command sets the user back to either the previous signature set or the initial signature set the product shipped with.
- Restoredefaults
  - Resets the Windows Defender registry settings to known good defaults.
- GetSWE
  - Exports contents of Software Explorer into a text file.

Configure Dynamic Security for Internet Explorer 7.

Dynamic Security options for Internet Explorer 7.0 allow you to secure your computer while providing a functional browsing environment. Internet Explorer 7.0 has new functionality that helps protect against malicious software and data theft from fraudulent Web sites. Additionally, Internet Explorer 7.0 has safe and easy add-on functionality that gives users full control over adding extra options to their browsing experience while avoiding inadvertent downloads of unwanted software.

The following table describes some of the Dynamic Security options that can be configured in Internet Explorer 7.0:

Dynamic Security Option	Use
ActiveX Opt-in	Disables nearly all pre-installed ActiveX controls to prevent potentially vulnerable controls from being exposed to attack. You can easily enable or disable ActiveX controls as needed through the Information Bar and the Add-on Manager.
Security Status Bar	Enhances awareness of Web site security and privacy settings by displaying color-coded notifications next to the address bar. Internet Explorer 7.0 changes the Address Bar to green for Web sites bearing new High Assurance certificates, indicating the site owner has completed extensive identity verification checks. Phishing Filter notifications, certificate names, and the gold padlock icon are now also adjacent to the address bar for better visibility. Certificate and privacy detail information can easily be displayed with a single click on the Security Status Bar.
Phishing Filter	Helps protect you against phishing sites. Warns you when visiting potential or known fraudulent sites and blocks the site, if appropriate. The opt-in filter is updated several times per hour with the latest security information from Microsoft and several industry partners.
Cross-Domain Barriers	Limits script on Web pages from interacting with content from other domains or windows. This enhanced safeguard will help to protect against malicious software by limiting the potential for malicious Web sites to manipulate flaws in other Web sites or cause you to download undesired content or software.
Delete Browsing History	Enables you to clean up cached pages, passwords, form data, cookies and history from a single dialog box.
Address Bar Protection	Displays an address bar to the user for every window, whether it's a pop-up or standard window, which helps to block malicious sites from emulating trusted sites.
International Domain Name Anti-Spoofing	In addition to adding support for International Domain Names in URLs, notifies you when visually similar characters in the URL are not expressed in the same language, thus protecting you against sites that could otherwise appear as known, trustworthy sites.
URL Handling Security	Redesigned URL parsing ensures consistent processing and minimizes possible exploration. The new URL handler helps centralize critical data parsing and increases data consistency throughout the application.

Fix Settings for Me	Warns you with an Information Bar when current security settings may put you at risk, to help protect you from browsing with unsafe settings. Within the Internet Options dialog box, you will see certain items highlighted in red when they are unsafely configured. In addition to warning you about unsafe settings, reminds you as long as the settings remain unsafe. You can instantly reset Internet security settings to the "Medium-High" default level by clicking the "Fix Settings for Me" option on the Information Bar.
Add-ons Disable Mode	Helps to troubleshoot difficulties launching Internet Explorer or reaching specific Web sites by providing the ability to start in "No Add-ons" mode, where only critical system add-ons are enabled.

The most important Dynamic Security options are:

- Phishing Filter
- Add-ons Disable Mode
- Delete Browsing History
- Fix Settings for Me

Configure security settings in Windows Firewall.

The Windows Vista firewall is much more advanced than previous versions and helps protect you by restricting other operating system resources if they behave in unexpected ways—a common indicator of the presence of malware. For example, if a component of Windows that is designed to send network messages over a given port on your PC tries to send messages via a different port due to an attack, Windows Firewall can prevent that message from leaving your computer, thereby preventing the malware from spreading to other users.

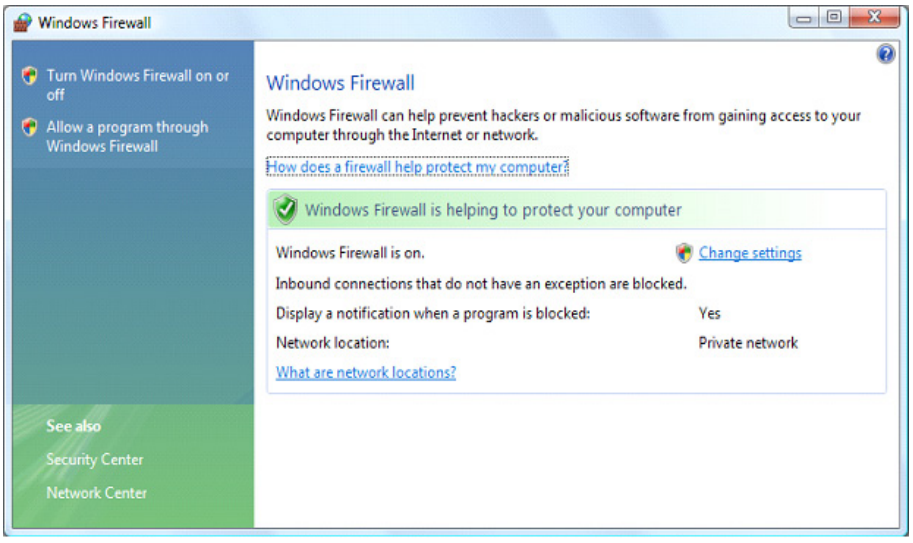

Figure 6 – Windows Firewall dialog box

Windows Firewall is a stateful, host-based firewall that allows or blocks network traffic according to its configuration. Windows Firewall in Vista includes enhancements for better protection and more advanced configuration, including:

- **Inbound Rules** – helps protect your computer from other computers making an unsolicited connection to it.
- **Outbound rules** – helps protect your computer by preventing your computer from making unsolicited connections to other computers.
- **Connection-specific rules** – enable a computer administrator to create and apply custom rules based on a specific connection.

Understanding Windows Firewall settings

The Windows Firewall Control Panel is designed to be easy to use, with several configuration options and a simple interface. There are three settings on the General tab in Windows Firewall. The following table lists the settings and explains when you should use them:

Setting	Description
On (recommended)	This setting is selected by default. When Windows Firewall is on, most programs are blocked from communicating through the firewall. If you want to unblock a program, you can add it to the Exceptions list (on the Exceptions tab). For example, you might not be able to send photos in an instant message until you add the instant messaging program to the Exceptions list.
Block all incoming connections	This setting blocks all unsolicited attempts to connect to your computer. Use this setting when you need maximum protection for your computer, such as when you connect to a public network in a hotel or airport, or when a computer worm is spreading over the Internet. With this setting, you are not notified when Windows Firewall blocks programs, and programs on the Exceptions list are ignored. When you select Block all incoming connections, you can still view most Web pages, send and receive e-mail, and send and receive instant messages.
Off (not recommended)	Avoid using this setting unless you have another firewall running on your computer. Turning Windows Firewall off might make your computer (and your network, if you have one) more vulnerable to damage from hackers and malicious software (such as worms).

Note: If some firewall settings are unavailable and your computer is connected to a domain, your system administrator might be controlling these settings through Group Policy.

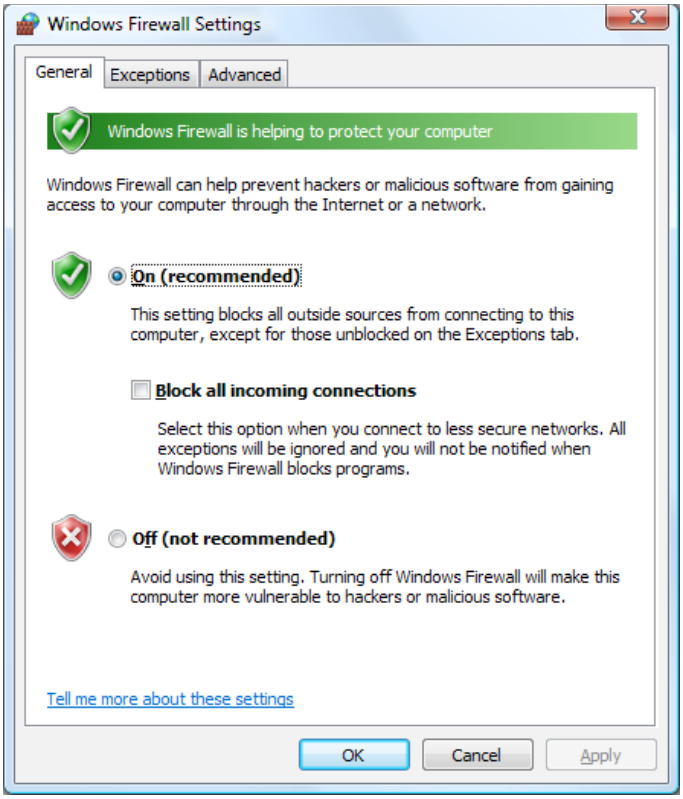

Figure 7 – Windows Firewall Options dialog box

Windows Firewall with Advanced Security Management

Windows Firewall with Advanced Security provides a number of ways to implement settings on both local and remote computers, and can be configured in the following ways:

- Configure a local or remote computer by using either the Windows Firewall with Advanced Security snap-in or the Netsh advfirewall command.
- Configure Windows Firewall with Advanced Security settings by using the Group Policy Object Editor or by using the **Netsh advfirewall** command.

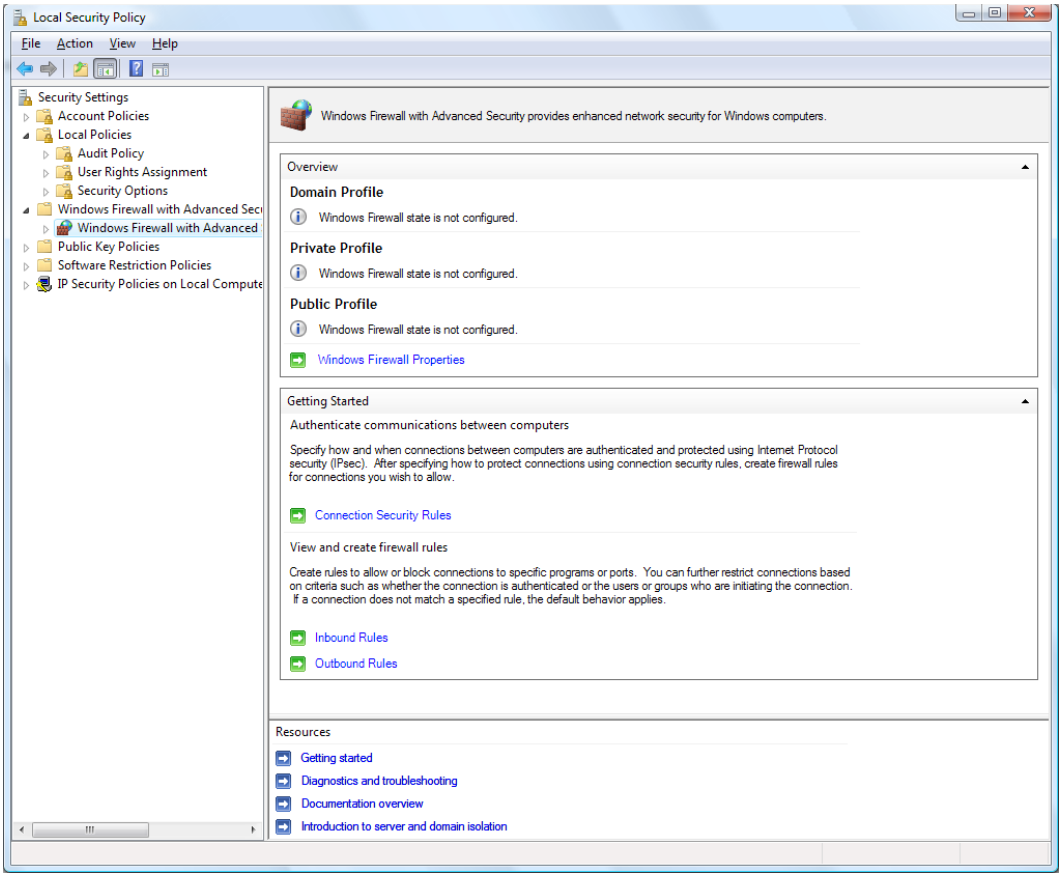

Figure 8 – Windows Firewall with Advanced Security

To open the Windows Firewall with Advanced Security in Control Panel, navigate to **Start -> Control Panel -> System and Maintenance -> Administrative Tools**. Double click **Windows Firewall with Advanced Security.**

Follow the steps below to use the Netsh advfirewall command-line tool:

1. Before you use Netsh advanced firewall commands, you need to run an elevated command prompt. Navigate to **Start -> All Programs -> Accessories**. **Right-click** the command prompt icon and click **Run as administrator**. At the UAC Prompt, click **Continue.**
2. To enter the **Netsh advfirewall** context, at the command prompt type: netsh.
3. When you enter the Netsh context, the command prompt will display the netsh prompt. At the netsh prompt, type advfirewall.
4. After you are in the advfirewall context, you can type specific commands. Commands include the following:
    - **export** – exports the current firewall policy to a file.
    - **help** – displays a list of available commands.
    - **import** – imports a policy from the specified file.

- **reset** – restores Windows Firewall with Advanced Security to the default policy.
- **show** – shows the properties for a particular profile. For example:
  - show allprofiles
  - show domainprofile
  - show privateprofile
  - show publicprofile

In addition to the commands available for the advfirewall context, advfirewall also supports four subcontexts. To enter a subcontext, type the name of the subcontext at the Netsh advfirewall prompt. The available subcontexts are:

- **consec** allows you to view and configure computer security connection rules.
- **firewall** allows you to view and configure computer security connection rules.
- **Monitor** allows you to view monitoring configuration.

Detailed information on configuring Windows Firewall with Advanced Security can be found at the Microsoft TechNet Web site article "Getting Started with Windows Firewall with Advanced Security."

Configuring Network Connectivity

Network Connectivity overview

Windows Vista streamlines the process of connecting to networks and enables you to connect to any type of network, whether it is a local wireless network, a corporate network through a virtual private network (VPN) or a remote access service (RAS), or through dial-up—all in one easy-to-find place. To open the Set up a connection or network dialog box, navigate to **Start -> Network -> Network and Sharing Center**. Click on **Connect to a network**. The dialog box shown in *Figure 9* will appear.

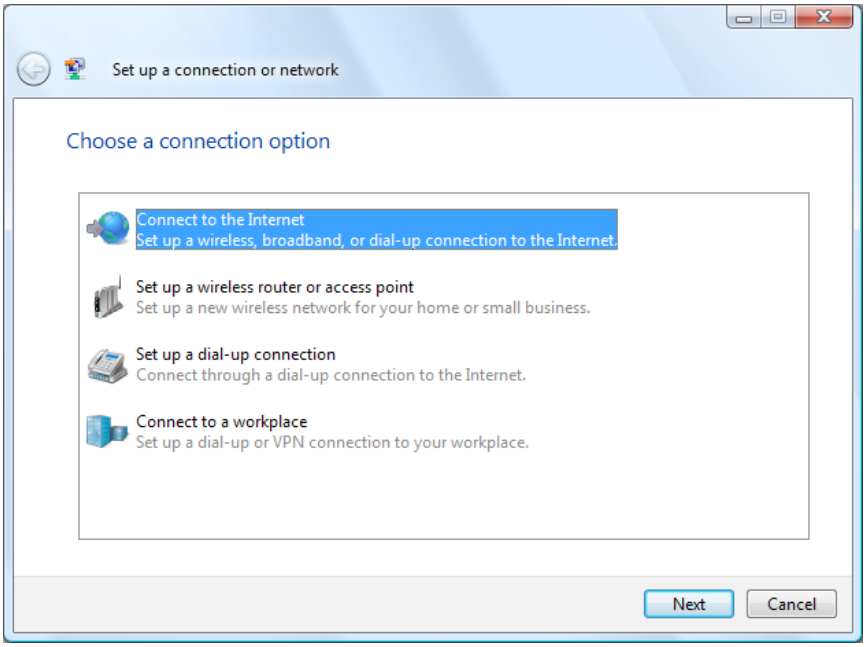

Figure 9 – Set up a connection or network dialog box

With Window Vista, wireless networking is also more secure, with enhanced support for the latest wireless security protocols, including Wi-Fi Protected Access 2 (WPA2, or 802.11i). To improve the overall user experience, rather than showing multiple pop-up notifications, Windows Vista shows a system tray on the lower right side of the screen with a single icon that indicates when wireless networks are available. Windows Vista also provides an easy way to create direct, computer-to-computer (ad hoc) wireless connections to enable sharing and peer-to-peer applications, even when you're not connected to the Internet. All of these connections can be configured from the "Set up a connection or network" dialog box.

Network Awareness

Network Awareness is a Windows Vista platform that reports changes in network connectivity to supported applications. This provides a seamless and contextually relevant networked experience. As you connect to different networks, applications that support Network Awareness can modify settings and the user experience based on that network. For example, when you switch from your home network to a wireless network at your neighborhood coffee shop, your firewall settings can change so other users cannot see your computer and your shared files.

Networking—Key Features

The table below provides a brief overview of the Windows Vista networking features:

Feature	Brief Description
Connecting interface	A single, easy-to-use interface for viewing and connecting to all available wireless networks, corporate (VPN and RAS) connections and dial-up connections. Helpful wizards are also available when you set up these connections for the first time.
Network Awareness	A platform that reports changes in network connectivity to supported applications, enabling a customized user experience for each network.
Network and Sharing Center	A central, easy-to-use place for quickly viewing network status and important network settings.
Network Diagnostics	Diagnoses network problems when they occur and suggests solutions.
Network Explorer	Browse all computers and devices on the network. The speed and reliability of discovering networked computers, servers, and devices are significantly improved compared to Windows XP.
Network Map	A visual map of the network that displays computers and devices as well as the ways in which they are connected. Broken connections are clearly displayed on the map, and you can use Network Diagnostics to help diagnose the problem and find possible solutions.
Network Setup Wizard	Easy, self-guided wizard that recognizes when supported networking hardware is connected, helps you create a network, guides use of the Windows Connect Now technology to create a secure wireless network and easily connect devices and computers to it. Rather than writing these settings down, you can transfer them with a USB flash drive or an Ethernet cable.

Networking Addressing Basics

Transmission Control Protocol/Internet Protocol (TCP/IP) is the default network protocol in Windows Vista. TCP/IP uses a specific addressing scheme and name resolution process to communicate between connected systems. Windows Vista maintains support for IPv4, the most common in network protocol. Vista includes support for IPv6, the latest version of IP.

This dual-natured support is provided through a dual-IP-layer architecture. Both protocols are enabled by default. IPv6 traffic is tunneled across an IPv4 network and vice versa.

IPv4

IPv4 uses a 32-bit address usually represented as a four-part number. Each part is separated by a period (i.e., 254.0.0.1). This method of representation is most commonly known as dotted decimal notation. Because each IPv4 address includes both network and host addressing, a subnet mask is required to distinguish the network address from the host address.

Numerous Internet resources exist that can provide additional information on IPv4.

IPv6

Because of the rapid and somewhat unexpected growth of the Internet, the IPv4 address space was unable to keep up with demand. IPv4 only supports approximately four billion unique addresses. IPv6 was developed to address this problem of limited addresses. IPv6 supports an extremely large number of addresses (approximately $3.4x10^{38}$ addresses).

IPv6 has a 128-bit address divided along 16-bit boundaries. Each 16-bit segment converts to a 4-digit hexadecimal number. A colon is used to separate each hexadecimal number. The resulting representation is colon-hexadecimal notation.

Here is an example of an IPv6 address in binary form:
00100001110110100000000011010011000000000000000000010111100111011000000101010101000000
00011111111111111110001010001001110001011010

This binary address is then divided along 16-bit boundaries like this:
0010000111011010–0000000011010011–0000000000000000–0010111100111011–0000001010101010–
0000000011111111–1111111000101000–1001110001011010

Each 16-bit block is then converted to hexadecimal and separated by colons. The binary address above is displayed like this:
21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A

To further simplify the representation of IPv6 addresses, leading zeroes within each 16-bit block are removed in a process called zero-suppression. Thus, with zero-suppression, the address is now displayed like this:
21DA:D3::2F3B:2AA:FF:FE28:9C5A

IPv6 does not use a separate subnet mask like IPv4; instead, it has a fixed prefix that contains specific routing and subnet information.

IPv6 provides a number of benefits for TCP/IP-based network connectivity, including:

- **Large address space** – the 128-bit address space potentially provides every device on the Internet with a globally unique address.
- **Efficient routing** – the IPv6 network packet supports hierarchical routing infrastructures, which enables more efficient routing than IPv4.
- **Straightforward configuration** – IPv6 can use both Dynamic Host configuration Protocol for IPv6 (DHCPv6) and local routers for automatic IP configuration.
- **Enhanced security** – the IPv6 standard provides better protection against address and port scanning attacks. All IPv6 implementations support IPsec for protection of IPv6 traffic.

Configuring networking by using the Network and Sharing Center

Windows Vista puts you in control of your network experience with the **Network and Sharing Center**. This versatile platform allows you to check connection status, see your network visually or troubleshoot a connection problem. The Network and Sharing Center, shown in *Figure 10* below, provides useful information about the network your computer is connected to and verifies whether it can successfully reach the Internet. It presents this information in a visual summary form, called the "Network Map," so you can immediately see your connectivity to the network and to the Internet. If a computer on the network loses Internet connectivity, you can see which connection is down and then use Network Diagnostics to help determine the cause of the problem and find possible solutions.

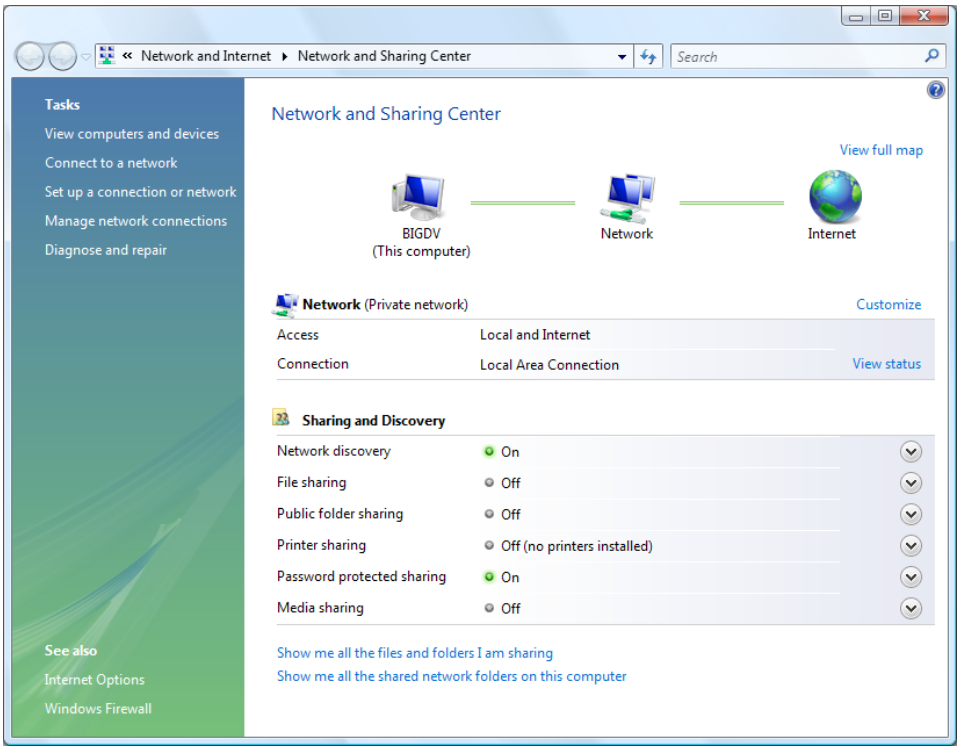

Figure 10 – Networking and Sharing Center

Configure network addressing

As with earlier Microsoft operating systems, Windows Vista allows you to configure network address either as a manual, static address or a dynamic address assigned using Dynamic Host Configuration Protocol (DHCP). Network addresses are configured by navigating to the **Properties** section of your Local Area Connection dialog box. shown in *Figure 11* below.

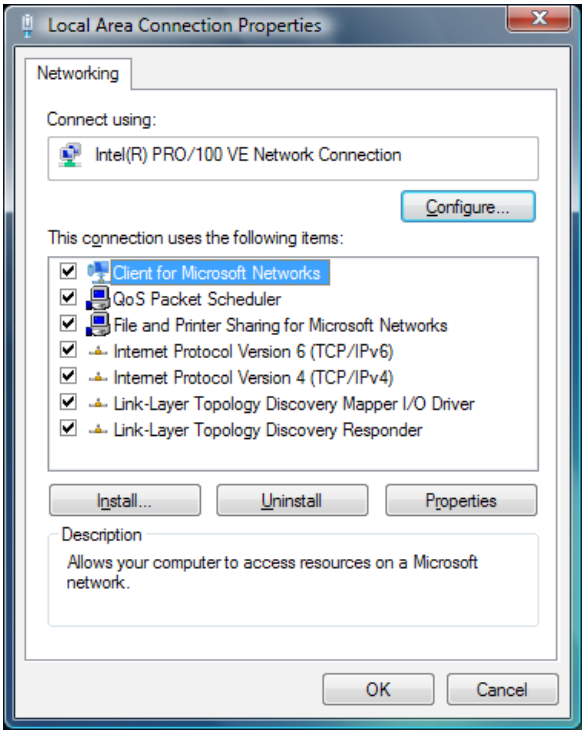

Figure 11 – Local Area Connection Properties

Static Configuration

You can manually configure static IP configuration for each computer in your network. This IP configuration should include the following:

- IP address
- Subnet mask
- Default gateway
- DNS server

There are several disadvantages to using a static configuration. First, each computer must be manually configured, which can be extremely time-consuming for larger networks. Additionally, this method increases the chance of human error.

Dynamic Host Configuration Protocol (DHCP)
DHCP enables you to assign automatic IP configurations for large numbers of computers, without having to input information manually. The DHCP service receives requests for IP configuration from computers configured to assign an IP address automatically and assigns IP information from scopes that you have defined for each subnet in your network. The DHCP service identifies the subnet that the request came from and assigns IP configuration from the relevant scope. Windows Vista supports DHCP for both IPv4 and IPv6.

As in Windows XP, when you configure your Windows Vista computer to obtain an IP address from DHCP, you can use the Alternate Configuration tab to control behavior if a DHCP server is not available. If a DHCP server is not available, and an alternate address has not been assigned, Windows Vista will automatically assign itself an IP address from the Automatic Private IP Addressing (APIPA) range of 169.254.0.0 - 169.254.255.255 within the default Class B subnet mask of 255.255.255.0. When your system is assigned an APIPA address, it cannot communicate outside of the local subnet, as a default gateway is not assigned.

Change TCP/IP settings
Follow the steps below to configure you TCP/IP addressing:

1. Navigate to Network Connections: **Start -> Control Panel -> Network and Internet -> Network and Sharing Center -> Manage Network Connections**.
2. **Right-click** the connection you wish to change and then click **Properties**. **Note**: Administrator permission is required.
3. Open the **Networking tab**. Under the "This connection uses the following items" section, choose either Internet Protocol Version 4 (TCP/IPv4) or Internet Protocol Version 6 (TCP/IPv6), and then click **Properties**.
4. To specify IPv4 IP address settings, (see *Figure 12*), do one of the following:
    - **To obtain IP settings automatically**: click "Obtain an IP address automatically," and then click **OK**.
    - **To specify an IP address**: click "Use the following IP address," and then, in the IP address, Subnet mask, and Default gateway boxes provided, type the desired IP address settings.
5. To specify IPv6 IP address settings, (see *Figure 13*), do one of the following:
    - **To obtain IP settings automatically**: click "Obtain an IPv6 address automatically," and then click **OK**.
    - **To specify an IP address**: click "Use the following IPv6 address," and then, in the IPv6 address, Subnet prefix length, and Default gateway boxes provided, type the desired IP address settings.
6. To specify DNS server address settings, do one of the following:
    - **To obtain a DNS server address automatically**: click "Obtain DNS server address automatically," and then click **OK**.
    - **To specify a DNS server address**: click "Use the following DNS server addresses," and then, in the Preferred DNS server and Alternate DNS server boxes provided, type the desired addresses of the primary and secondary DNS servers.
7. To change DNS, WINS, and IP settings, click **Advanced**.

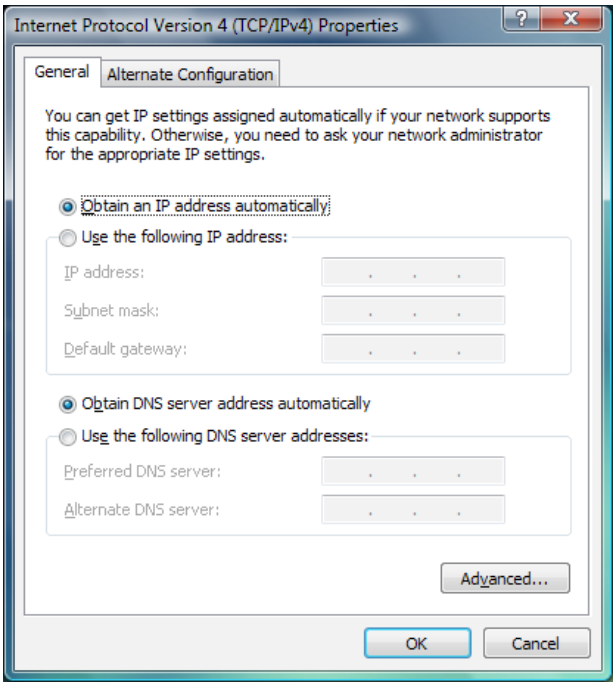

Figure 12 – Configure IPv4 addressing

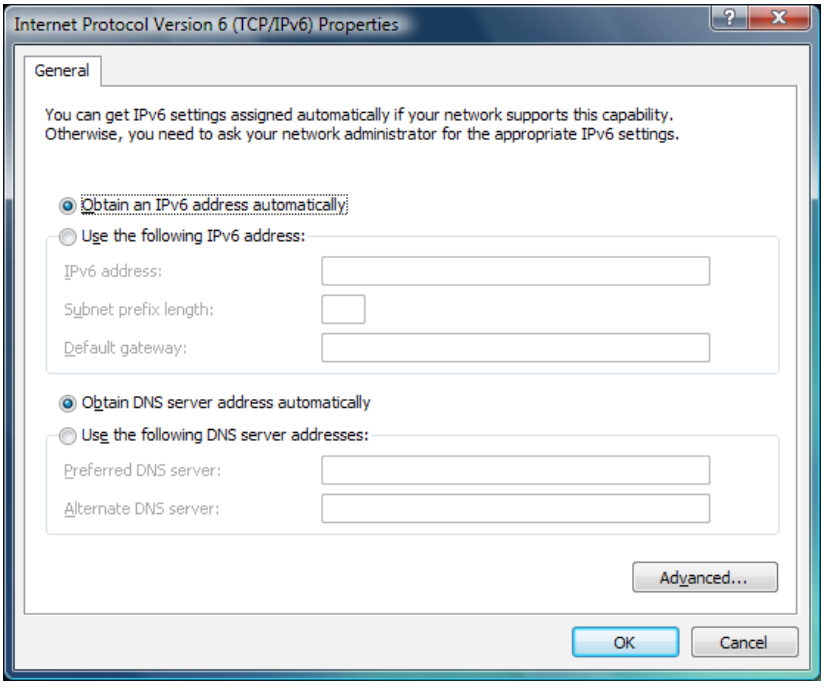

Figure 13 – Configure IPv6 addressing

Troubleshoot connectivity issues

Troubleshooting connection problems can be a challenge because there are so many possible causes. First, try these steps:

1. Click to open **Network Diagnostics**.
    - Make sure that all wires are physically connected (i.e., make sure your modem is connected to a working phone jack, either directly or through a router).
    - If you're trying to connect to another computer, make sure that computer is on and physically connected to the network.
2. If the problem began after you installed new software, check your connection settings to see if they have been changed.
3. Click to open Network Connections.
    - Right-click the connection, and then click Properties. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.
    - Verify that the proper protocols are installed and configured correctly.

Network Map

Sometimes, multiple wired and wireless computers and devices connected to a network can be difficult to visualize, especially if your network has a problem. In order to ease network troubleshooting, Windows Vista provides a new feature called the Network Map. The map is a graphical interpretation of every device on the network and how each device is connected.

To open the Network Map tool, navigate to **Start -> Control Panel -> Network Map**.

Diagnostic tools and Utilities

Windows Vista includes several utilities and TCP/IP tools that can be used to diagnose network problems. Some of these utilities and tools are:

- **Windows Network Diagnostics** – Provides diagnostics and automatic correction of networking problems. This utility will offer a description of the problem and any possible solutions to the problems. In spite of the tool's ease-of-use, some problems may require manual intervention from the user.
- **IPCONFIG** – As with previous versions of Windows, ipconfig is a command-line tool that displays TCP/IP configuration. The most commonly used switches include:
    - /release – releases IP address information for the specified adapter.
    - /renew – refreshes IP address information for the specified adapter.
    - /all – displays all TCP/IP configuration information.
- **PING** – As with previous versions of Windows, ping is a command-line tool used to verify IP-level connectivity to another computer or host. The command sends and receives packets (the default is four) of information to a specified computer or host and times the return of each packet.
    - For example: ping google.com, ping 64.233.187.99

- **TRACERT** – As with previous versions of Windows, tracert is a command-line tool used to discover the path taken to a destination computer by a packet of information. The path displayed is a list of all router interfaces between a source and destination.
- **NSlookup** – Displays information used to diagnose DNS infrastructure issues. This tool can confirm a connection to a DNS server and displays any required records.

If Windows Network Diagnostics cannot resolve the problem, Microsoft recommends that you follow a logical troubleshooting process using the tools available in Windows Vista. Follow the steps below to troubleshoot network connectivity problems:

1. Consult Windows Network Diagnostics.
2. Check the local IP configuration using IPCONFIG.
3. Diagnose two-way communications with a remote system using PING.
4. Identify each hop (router) between two systems using TRACERT.
5. Verify the computers DNS configuration using NSlookup.

For more troubleshooting tips, open Windows Help and Support, search for Network and Sharing Center and select the topic "Troubleshoot network and Internet connection problems."

Configure Remote Access

The Remote Desktop Connection feature in Windows Vista enables easier remote access to any resource or application that an organization has made available to its users. For example, if a salesperson requires remote access to a financial application or a customer relationship management (CRM) application, Windows Vista enables the corporate information technology (IT) manager to place an icon for that application on the desktop. The user simply clicks the icon, and an automatic Terminal Services Remote Program connection is made back to the company over the Internet and to the Terminal Server in Windows Server "Longhorn," with no need for a VPN.

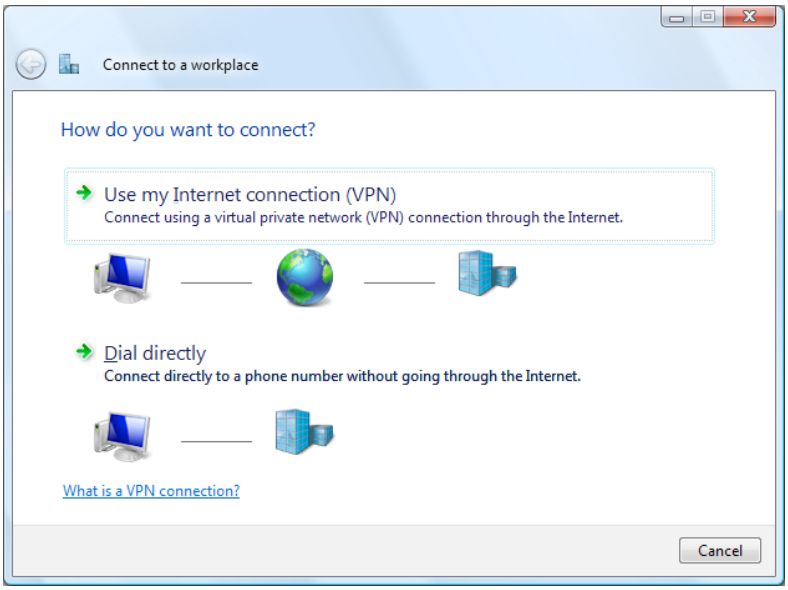

Figure 14 – Connect to a workplace dialog box

Remote access to business networks is becoming more important as businesses become increasingly more mobile; therefore, support for remote access technologies is critical for the modern operating system.

Windows Vista supports two remote access technologies that enable you to access business data from remote locations with appropriate security:

- **Remote Desktop** – Enables secure remote access to selected corporate resources without the need for a VPN connection. IT managers choose which resources to make available, and users simply click a desktop icon to make the connection and access the application or information.
- **Terminal Services Gateway** – Provides secure remote access to corporate resources over the Internet from a home PC.

To open the **Connect to a Workplace** dialog box (*Figure 14*), navigate to **Start -> Network -> Network and Sharing Center**. Click on **Connect to a network** followed by **Connect to a workplace**. Remote connections connect individuals or groups to a network from a remote location. Windows Vista includes two types of remote connection:

- **Dial-up** – A dial-up connection is a point-to-point connection to a remote access server that provides access to network resources or a connection to an Internet Service Provider (ISP), which then allows access to the Internet. The client dials a number that is answered and authenticated by the remote access server. If you create a dial-up connection to an ISP, you can then create a VPN through the dial-up connection to a remote access server that enables access to resources on a remote network.
    - To configure a dial-up connection you must have the following information:
    - The correct phone number for the network you are dialing.
    - A valid username and password for the network you are dialing.
    - The user must have dial-in permissions for the network you are dialing.
- **Virtual Private Network (VPN)** – A VPN is a secure channel (or tunnel) through an insecure network, such as the Internet, relying on encryption technologies to keep the connection secure. The VPN client authenticates to the remote access server, at which time they negotiate the tunneling and encryption technologies. Vista supports the following technologies:
    - **Tunneling**: Point-to-Point Tunneling Protocol (PPTP) and Layer 2 Tunneling Protocol (L2TP).
    - **Encryption**: Microsoft Point-to-Point Encryption (MPPE) and IP Security (IPSec). In addition, Windows Vista also supports VPN tunnels that use Layer 2 Tunneling Protocol (L2TP) and IP security (IPsec).
    - A VPN connection uses both private and public networks to create a network connection. There are two main types of VPNs:
        - **Network** – for example, a branch office connected to their corporate headquarters.
        - **Host** – for example, a mobile worker using their laptop to connect securely to their business network over a dial-up or via public Wi-Fi access.
    - To configure a VPN connection you must have the following information:
        - The correct name or IP address of the VPN server.
        - The correct tunneling protocol configured for the connection.
        - The correct encryption protocol configured for the connection.

- A valid username and password for the remote network that has dial-in access to the network.
- The correct authentication protocol configured for the connection.

Configuring Applications Included with Windows Vista

Microsoft Windows Vista includes many new, bundled applications along with new versions of old favorites. Some of the new and revised applications are listed below:

- Windows Mail, a replacement for Outlook Express.
- Windows Contacts, a replacement for Windows Address Book (WAB).
- Windows Calendar, a new application.
- Windows Fax and Scan, an integrated faxing and scanning application.
- Windows Meeting Space, the replacement for NetMeeting.
- Windows Photo Gallery, a photo and video library management application.
- Windows Movie Maker.
- Windows DVD Maker.

Configure and troubleshoot media applications

Windows Vista incorporates new versions of Windows Media Player and Windows Media Center that provide additional functionality and an enhanced user experience.

Windows Media Player Taskbar

To get started, refer to *Figure 15*, below. Each tab corresponds to a different task. The arrow that appears below each tab provides you with quick access to options and settings related to that task.

Figure 15 – Windows Media Player tabs

As you switch between various tabs and views in the Player, you can use the Back and Forward buttons on the left side of the taskbar to retrace your steps.

To play a file in your library

1. Click the **Library** tab (see *Figure 16*, below) and then browse or search for the item that you want to play.
    - If the library doesn't display the media type you are looking for (for example, music is displayed instead of video), on the address bar click the **Select a category** button on the far left and choose a different category.
2. Do one of the following:
    - Drag an item to the List pane. You can drag individual items (such as one or more songs) or collections of items (such as one or more albums, artists, genres, years, or ratings) to the List pane.
        - If the List pane is not visible, click the **Show List Pane** button, near the search box.
        - If the List pane already contains other items, you can clear the contents by clicking the **Clear List Pane** button.
    - Double-click the item to begin playing it.
        - Depending upon what you double-click, several items might be played. To play a single item, drag the item to List pane instead.

Note: If the Player can't play a particular file, the issue may be related to media usage rights.

Use the address bar to switch to a specific category (i.e., music, pictures, or video) and then select a view for the selected category in the **Navigation** pane. For example, switch to the Music category and then click "Genre" in the Navigation pane to see all of your music organized by genre. You can drag items from the Details pane to the List pane to create a playlist.

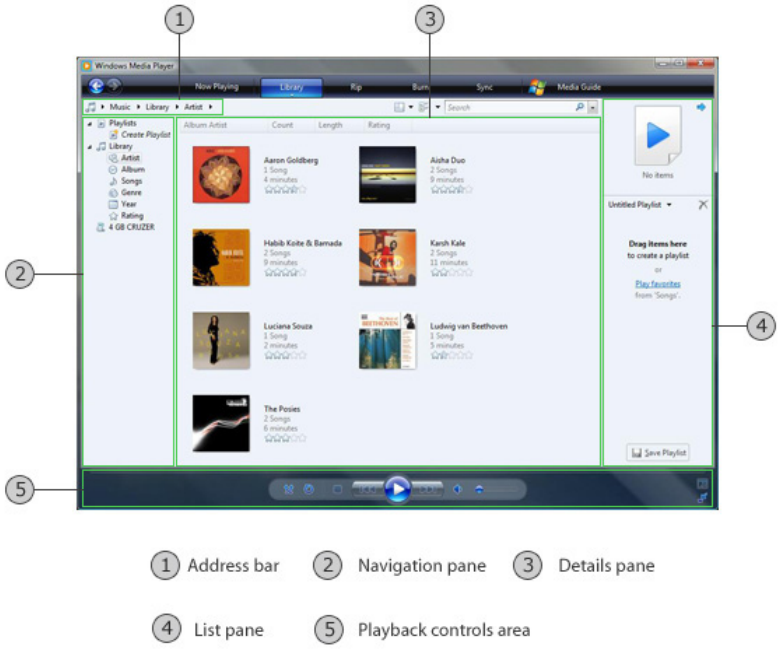

Figure 16 – Library view

In addition to using the Library tab to play an audio or video file in you library, you can use this tab to do any of the following:

- Find items in the library
- Add items to the library
- Remove items from the library
- Create and play playlists
- Add or edit media information
- Add or change album art

Viewing the Classics Menus
The Classic Menus in Windows Media Player (previously known as the menu bar) provides you with access to most of the Player functions. These are hidden by default.

Although many of the functions in the Classic Menus also appear in the drop-down menus below the Now Playing, Library, Rip, Burn, and Sync tabs, you might want to show the Classic Menus to access the less frequently used commands that only appear on the File, View, Play, Tools, and Help menus.

Follow the steps below to either show or hide the Classics Menus:

- **To show the Classic Menus**, right-click an empty area of the taskbar or to the left of right of the playback controls and choose **Show Classic Menus** from the context menu. Alternately, the keyboard shortcut for this command is **CTRL-M**.
- **To hide the Classic Menus**, open the **View** menu and choose **Classic Menus**. Again, **CTRL-M** will hide the classic menus.

Securing Windows Media Player
Digital media content often contains script commands with instructions to enhance the playback experience. For example, a script command may open your Internet browser and display a related Web page while Media Player plays back content. Unfortunately, some digital media content contains malicious script commands that attempt to perform unwanted actions on your computer or send you to web sites intended to gain access to your personal information. Windows Media Player contains a number of security features designed to protect your computer.

The following table outlines the security configuration options for Windows Media Player that are located in the **Options** dialog box on the **Security** tab:

Security Option	Action
Run script commands when present	This option specifies whether to allow URL and FILENAME script commands to run when you play digital media content that contains them. URL script commands display web pages; FILENAME script commands open a specified digital media file. This option is disabled by default.
Run script commands and rich media steams when the Player is in a Web page	This option specifies whether to allow URL and FILENAME script commands to run when you play digital media content embedded in a Web page. This option is enabled by default. **Note**: Disabling this option may prevent rich-media streams from running.
Play enhanced content that uses Web pages without prompting	This option specifies whether to notify you when you are about to play digital media content that has been enhanced with Web pages. Because some content can contain malicious Web pages, Windows Media Player will prompt you to verify that you want to proceed when enhanced digital media content is detected. Enabling this option will remove conformation prompts.
Show local captions when present	Windows Media Player supports Synchronized Accessible Media Interchange (SAMI) captioning of media content. SAMI content can be located on the Internet, your hard disk, or your CD or DVD. During playback, Windows Media Player accesses the content to locate and display SAMI captions. Enabling this option allows access to SAMI content in all of the content zones available to your computer. Disabling this option (default) will limit access to the Internet zone.
Zone Settings	This button opens the Security tab of the Internet Options dialog box, which lists zone settings that control which types of content to display in Windows Media Player. **Note**: Changing settings may affect how Windows Media Player features operate or prevent information from being displayed. Changes to the zone settings will also affect other programs that rely on the Internet options security zones.

In addition to the above security settings, Windows Media Player has a number of settings that affect the privacy of your media information and Player usage. Most of these settings can be located on the Privacy tab of the Options dialog box.

To access the Privacy tab, click the arrow below the Now Playing tab, click More Options and then click the Privacy tab. Settings found in this location include:

- Display media information from the Internet.
- Update music files by retrieving media info from the Internet.
- Download usage rights automatically when I play or sync a file.
- Automatically check if protected files need to be refreshed.
- Set clock on devices automatically.
- Send unique Player ID to content providers.
- Cookie settings.
- Save file and URL history in the Player.
- Cache clearing options.

Note: Some of these settings may also be controlled by Group Policy settings.

Troubleshooting Windows Media Player
The following self-help options are the first steps you should take to troubleshoot a problem:

- Help Documentation
    - Search for relevant topics in Windows Media Player Help by starting Windows Media Player and pressing F1.
- View the list of Windows Media Player components installed on your computer
    - You can access Technical Support Information from the About Windows Media Player dialog box.

Note: If the Help menu is not visible, enable the classic menus (CTRL-M).

Numerous self-help options are available from the Windows Media Player Web site, including:

- **How-to articles** – Learn how to perform common tasks in Windows Media Player 11, such as burning and copying content from CDs and DVDs, synchronizing songs to portable music players, and downloading music and videos from online stores.
- **FAQs** – Browse frequently asked questions about Windows Media Player.
- **Newsgroups** – Ask other Windows Media Player users for assistance.
- **Readme page** – Review the Windows Media Player 11 system requirements and known issues.
- **Knowledge Base (KB) articles** – Search for Windows Media Player related Knowledge Base articles.
- **Media Advice columns** – Browse the Media Advice columns or submit a question to be answered in a future column.

Windows Media Center

Windows Media Center (*Figure 17*) enables you to manage and play back all your digital media through one interface, including live and recorded TV, movies, music and pictures, by using the Windows Media Center menu system and remote control. Windows Media Center in Windows Vista includes enhancements for expanded support of digital and High-Definition Cable TV, and FM and Internet radio stations, as well as options for multi-room access to your entertainment through Media Center Extenders, including Xbox 360.

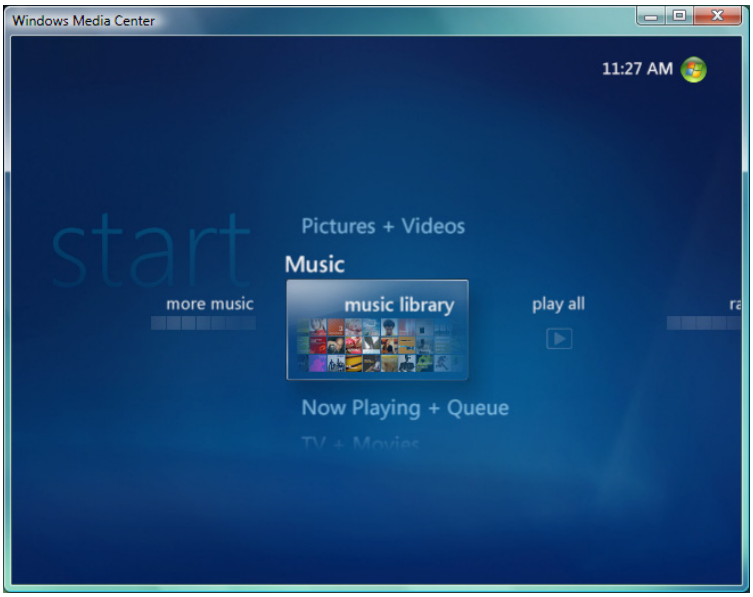

Figure 17 – Windows Media Center start screen

The first time that you use Windows Media Center you must go through a setup Wizard. This process will configure the behavior of Windows Media Center on your computer, although you can skip many of the options and configure them at a later time. Once the configuration is complete the application will open to the Start screen.

Windows Media Center configuration options

In Windows Media Center, you can choose which partner programs are displayed in the Start screen. This allows you to quickly find programs that you use regularly. When a new program is installed, it will appear automatically in the associated category (Music, TV, or Pictures + Videos). The next program that is registered in that category will replace the one before it. Hiding a program does not uninstall the program.

To show or hide a program, from the **Start** screen, go to **Tasks -> Settings -> General -> Program Library Options**. Choose **Edit Program Library**.

1. **To hide a program**, clear the check box next to the program.
2. **To show a program**, select the check box next to the program.
3. Click Save to save your changes.

To have only one program appear on the Start screen, from **Start**, go to **Online Media -> Program Library**. Right-click the program you want to appear. On the context menu click **Add to Start Menu**. Click **Yes**.

Change the default music or video player
After installing a new music or video player, you might find that your music and videos open in the new program instead of your original program. You can modify the settings in Windows so that your music and videos open in your favorite player.

1. Open the folder that contains the file you want to change.
2. **Right-click** the file, and then click **Open With**.
3. Choose the program that you wish to use.
4. Enable the "Always use the selected program to open this kind of file" check box, and then click **OK**.

Note:

- The most common music file types include: WMA, MP3, OGG, M3U, and WPL.
- The most common video file types include: MPG, AVI, WMV, and QT.

Other configuration options for Windows Media Center may be found by scrolling left or right to Settings. Configuration options include:

- General
- TV
- Pictures
- Music
- DVD
- Extender
- Library Setup

Configure Windows Mail

Windows Mail (*Figure 18*) is the Vista tool for e-mail exchange and newsgroup access.

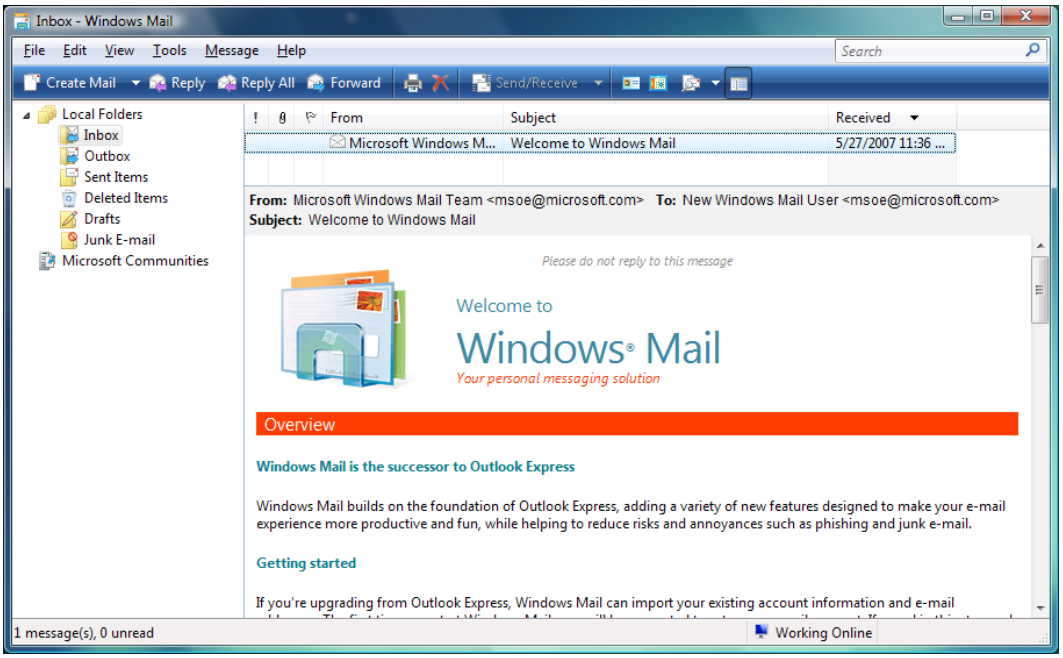

Figure 18 – Windows Mail main window

The table below describes the key features found in Windows Mail:

Feature	Description
Instant Search	Allows users to search across all email messages instantly.
Junk Mail Filter	Automatically screens email to identify and separate out junk mail.
Newsgroup features	Provides access to Usenet newsgroups.
Phishing Filter	Analyzes email to detect fraudulent links and to help protect users from identity theft.
Reliability	Uses new storage technology to provide increased reliability.

Add or remove a Windows Mail account

Windows Mail, as in Outlook Express, supports multiple email accounts. For instance, you may want a single personal e-mail account or you might also add your work e-mail account and some newsgroups as well. Windows Mail makes managing multiple accounts easy by putting each account in its own folder.

Windows Mail supports three types of accounts: mail, news (newsgroups), and directory services. Directory services are online address books that are typically offered by organizations such as colleges and businesses.

To add a Windows Mail account

1. Click to open Windows Mail.
2. Click the Tools menu, and then click Accounts, the dialog box shown in *Figure 19* will appear.
3. Click Add, choose the type of account you want to add, click Next, and then follow the instructions.

To remove a Windows Mail account

1. Click to open Windows Mail.
2. Click the Tools menu, and then click Accounts, the dialog box shown in *Figure 19* will appear.
3. Click the account you want to remove, and then click Remove.

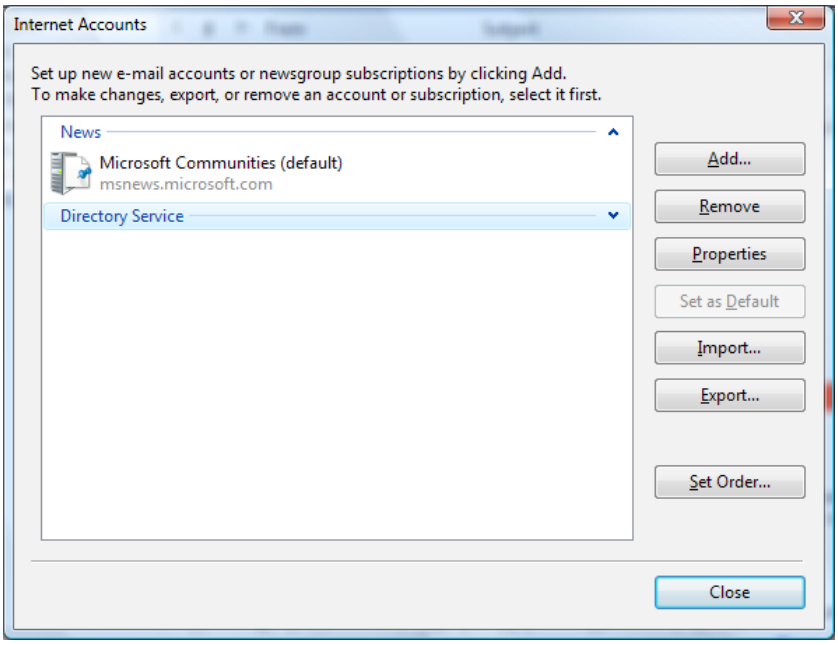

Figure 19 – Windows Mail Internet Accounts dialog box

Block spam and other unwanted e-mail

Windows Mail helps you manage your Inbox to keep it free of unwanted e-mail messages in the following ways:

- The junk e-mail filter is designed to catch obvious, unsolicited commercial e-mail messages (often called "spam") and move them to a special Junk e-mail folder. You can increase or decrease the junk e-mail protection level based on how much junk e-mail you receive.
- You can move e-mail messages erroneously marked as Spam from the Junk e-mail folder back to your Inbox.
- You can block messages from specific e-mail addresses by adding them to the Blocked Senders list.
- You can prevent the blocking of messages from specific e-mail addresses by adding them to the Safe Senders list.

Change the junk e-mail protection level

1. Open Windows Mail.
2. Click the **Tools** menu, and then click **Junk e-mail Options.** The dialog box shown in *Figure 20* will appear.
3. Select the protection level you want:
    - **No Automatic Filtering**. Enabling this option stops junk e-mail protection altogether, with the exception of messages coming from domain names and e-mail addresses on your Blocked Senders list.
    - **Low**. Enabling this option blocks only the most obvious junk e-mail messages.
    - **High**. Enabling this option will block as many as possible; however, you should periodically review the messages in your Junk e-mail folder to ensure that there are not any legitimate e-mail messages that might have been moved there as well.
    - **Safe List Only**. Enabling this option will block all messages from domains and email addresses not on your Safe Senders list.

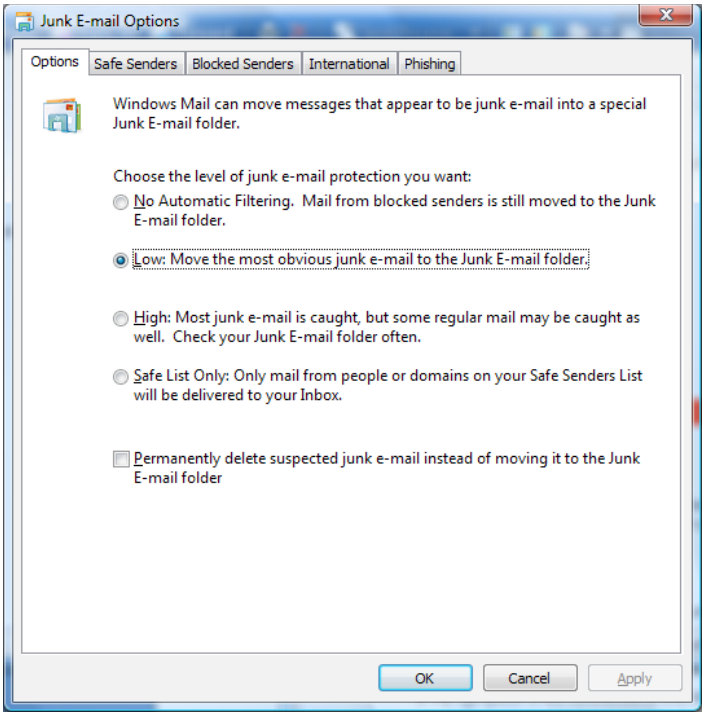

Figure 20 – Windows Mail Junk E-mail options dialog box

Move a message from the Junk e-mail folder to your Inbox

1. Open Windows Mail.
2. Click the **Junk e-mail** folder.
3. Click the message that you want to move to your Inbox.
4. Open the **Message** menu, point to Junk e-mail, and then click **Mark as Not Junk**.

Note: Though marking a message as not junk will move that message to your Inbox, future messages from that sender might still end up in the Junk e-mail folder. To prevent this from happening, add the sender to the Safe Senders list.

Set the Windows Mail security level

Some of the e-mail messages you receive in Windows Mail might contain web browser add-ons or scripts, which could pose a security risk. You can disable add-ons and scripts by choosing a restrictive security level, or you can view most content of this type by choosing a moderate security level.

1. Open Windows Mail.
2. Open the **Tools** menu, click **Options**, and then click the **Security** tab.
3. Under **Virus Protection**, choose a security zone:
   - Click **Internet Zone** if you want to allow scripts and add-ons to run.
   - Click **Restricted Sites Zone** to create a more secure environment; this is the recommended setting.

Note: You can also adjust the security level of these and other zones in Internet Explorer. The settings that you choose for these zones in Internet Explorer also apply to Windows Mail. For more information, see Change Internet Explorer security settings.

Configure Windows Meeting Space

Windows Meeting Space gives you the ability to share documents, programs, or your desktop with other people. Some of the advantages of this application are:

- You can share your desktop or any program with other meeting participants.
- You and other meeting participants can distribute and co-edit documents.
- You can pass notes to other participants.
- You can connect to a networked projector to give a presentation.

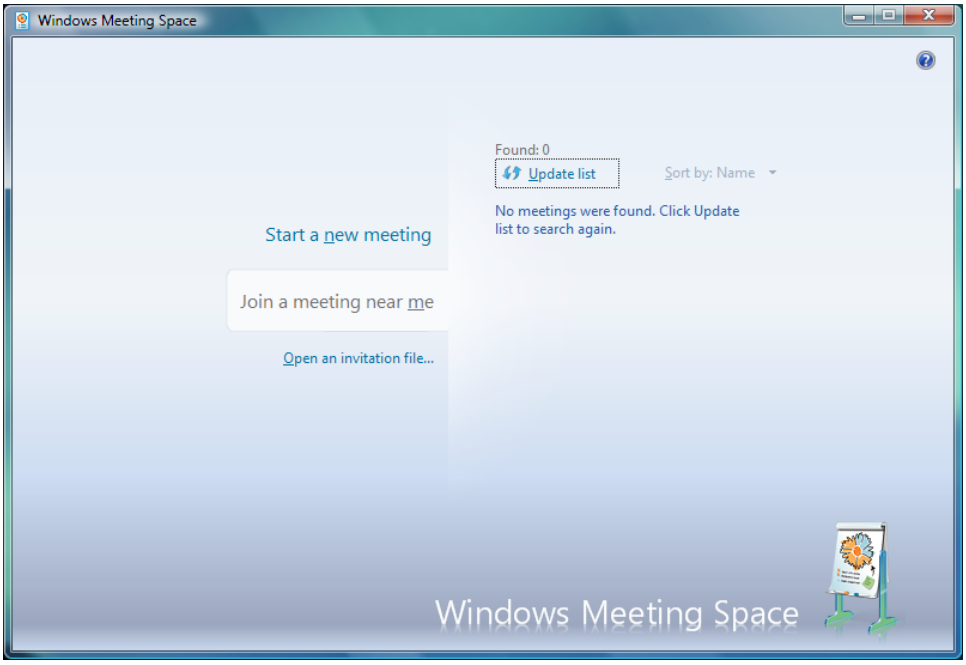

Figure 21 – Windows Meeting Space main window

Windows Meeting Space uses peer-to-peer technology to automatically create an ad hoc network (if it can't find an existing network). This enables the application to function in a wide variety of environments (i.e., a conference room, a favorite hotspot, or a place where no network exists). With Windows Meeting Space, you can join a meeting that someone else sets up, or you can start a new meeting and invite other people to join it.

The table below describes the features found in Windows Meeting Space (shown in *Figure 21*, above):

Feature	Brief Description
Anywhere, anytime face-to-face collaboration	Supports both infrastructure and ad hoc wireless networks.
Auditing	Auditing of particular meeting activities.
Compatibility	Any file or application can be broadcast or streamed—not just Microsoft applications.
Domain password requirements integration	Meeting passwords must comply with domain user password requirements.
Multi-party file sharing and collaboration	Everyone can change and save files; one saved change is replicated immediately to everyone other participant.
Password protection	The session initiator decides who can join the session.
People Near Me and Sessions Near Me	Check availability of others on the network and invite them to join your collaboration group, or search for relevant sessions and ask to join.
Shared control of presentations	Allows the initiator to pass control to other users, who can make revisions even while the original is being broadcast from the initiator's computer.

Configuring Windows Meeting Space

The first time you open Windows Meeting Space, you will be prompted to turn on some services and sign in to People Near Me (see *Figure 22* below).

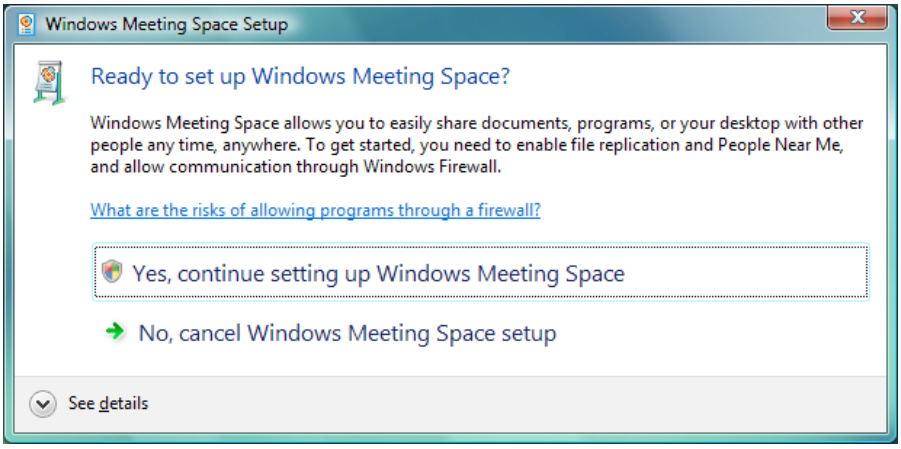

Figure 22 – Windows Meeting Space configuration screen

Joining or initiating a meeting in Windows Meeting Space.

If you know there's a meeting in progress that you want to join, click **Join a meeting near me**. Or, if you know that someone has sent you an invitation file, click **Open an invitation file**. Otherwise, click **Start a new meeting**. Windows Meeting Space enables face-to-face collaboration from 2 to as many as 10 people over a wired network, a wireless local area network (WLAN) or an ad hoc wireless network.

Note: The option to start a new meeting is not available in Windows Vista Home Basic.

Follow one of the three methods below to invite people to a meeting:

- By selecting names in the "Invite people" dialog box.
    1. In a meeting, click **Invite people**.
    2. Select the check box beside the name of each person you want to invite, and then click Send invitations.
- By sending an invitation in e-mail.
    1. In a meeting, click Invite people.
    2. In the Invite people dialog box, click **Invite others**, and then click **Send an invitation in e-mail**.
- By creating an invitation file.
    1. In a meeting, click Invite people.
    2. In the Invite people dialog box, click Invite others, click **Create an invitation file**, and save the file.
    3. Give the invitation file to the person you want to invite, either by making it available on a network share that the person can access, by e-mailing it, or by providing it on removable media.

After inviting participants to your meeting you will need to share a document or your desktop with the meeting participants. Click **Share a program or your desktop**, and then select the item you want to share. You might also want to distribute handouts (files) to meeting participants. Click **Add a handout**, and then select the file you want to share.

During a sharing session, you are the only person who has control of your desktop and programs. If you want to temporarily pass control to another participant, you can do so; however, you can always take back control, either by clicking **Take Control** or by pressing **the Windows logo key + ESC**.

Windows Meeting Space security

Windows Meeting Space was designed with security in mind. Invitations and participant authentication are handled by using certificates derived through a common password exchange and verification between the session creator and other attendees. Some additional security features in Windows Meeting Space are detailed below:

- Respects current security constraints
    - By default, Windows Meeting Space requires passwords to be the equivalent strength of a domain user account password. (This requirement can be turned off for the entire Peer Grouping infrastructure and Windows Meeting Space. By disabling this requirement, passwords for meetings must only be eight characters in length.) Windows Meeting Space abides by the rules set up for the Attachment Manager. This allows an administrator to limit the file types that can be shared via Windows Meeting Space, in the same way the administrator limits the file types that can be sent via a mail client such as Microsoft Office Outlook (or Windows Mail).
- Flexible Group Policy and auditing controls
    - Windows Meeting Space respects system Group Policy settings (that is, the ability to create ad-hoc wireless networks) and provides the ability to disable the entire feature or particular aspects (i.e., file sharing). The built-in logging feature can track usage, activity, etc., to the event log during a Windows Meeting Space session.

Configure Windows Calendar

Windows Calendar overview

The Windows Calendar (*Figure 23*) is a flexible, easy-to-use calendar included with the Windows Vista operating system. It enables you to plan and manage all of your activities and coordinate your schedule with others. Windows Calendar also includes a feature that allows you to create a personal task list and to receive automatic notifications and reminders about specific tasks or upcoming appointments.

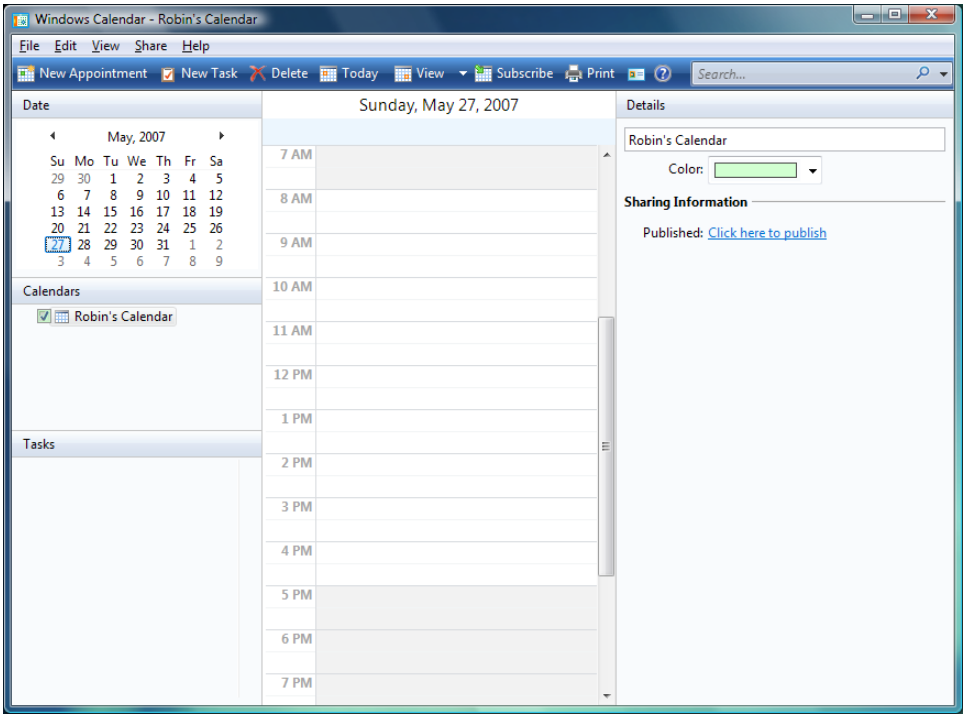

Figure 23 – Windows Calendar main menu

To view the Windows Calendar, click the clock in the Notification area of the Taskbar. If the clock is not visible, follow the steps below:

1. Right-click the Taskbar, and then click Properties.
2. Open the Notification Area tab, select the Clock check box, and then click OK.

Configuring Windows Calendar

To change the calendar view
You can view your calendar by day, work week, week, or month. To change the calendar view open the **View** menu, and then choose the view you want. A check mark appears next to the view you select.

To view the details pane
If you can't see the details of a task, date or calendar, open the **View** menu, and then click **Details Pane** so that a check mark appears. To close the Details pane, click Details Pane again — the check mark disappears.

To create a calendar

1. Open the **File** menu, and then click **New Calendar**.
2. In the **New Calendar** box, type the name you want for the calendar, and then press **Enter**.
3. To choose the color of your appointments: in the Details pane, click **Color**, and then choose the color you want.

Windows Calendar also allows you to set up individual calendars for multiple people. This is especially helpful for families or other groups who share a single PC. Windows Calendar makes it easy for people who use the same computer to coordinate their personal schedules by letting them compare information from any or all personal calendars, side-by-side in a single view.

Subscribe to a Calendar
Many major sports teams, television and radio shows, and academic institutions offer calendars on the Internet. When you subscribe to one of these calendars, you can set how often your personal calendar is updated with the subscription calendar's event dates. Windows Calendar works with calendars in the iCalendar format (.ICS). To subscribe to a calendar, click **Subscribe** on the toolbar and then follow the instructions.

Publishing a Calendar
The iCalendar compatibility of Windows Calendar also makes it easy to publish your own calendar on the Internet through a web host. If you like, you can publish your personal schedule with password protection, so only designated friends and family members can access and view your calendar.

1. Open the **Share** menu and click **Publish**.
2. In the Calendar name box, type the calendar name that you want to share.
3. In the Location to publish calendar box, enter the location (such as a website) where you want to publish the calendar.
4. Review any other options, and then click Publish.

Note: To see locations where you can publish your calendar online, click "Where can I publish this calendar?"

Configure Windows Fax and Scan

Overview

Windows Fax and Scan enables you to use your computer to fax and scan documents and pictures. The program is divided into Fax view and Scan view.

- In Fax view (*Figure 24*), you can send and receive faxes, create cover pages, and forward faxes as e-mail attachments. You can send and receive faxes in two ways:
  - By using an analog modem. **NOTE**: You cannot send or receive faxes over a digital phone line.
  - By using a fax server. **NOTE**: You must have the network address for the server and permission to connect to it.
- In Scan view, you can scan documents and pictures, create and save scanning preferences for reuse, and send scanned documents and pictures as fax or e-mail attachments.
  - To scan documents and pictures you must have access to the appropriate hardware. This might be a local or a network scanner; in both cases you may need to install driver software to use the scanner from your computer.

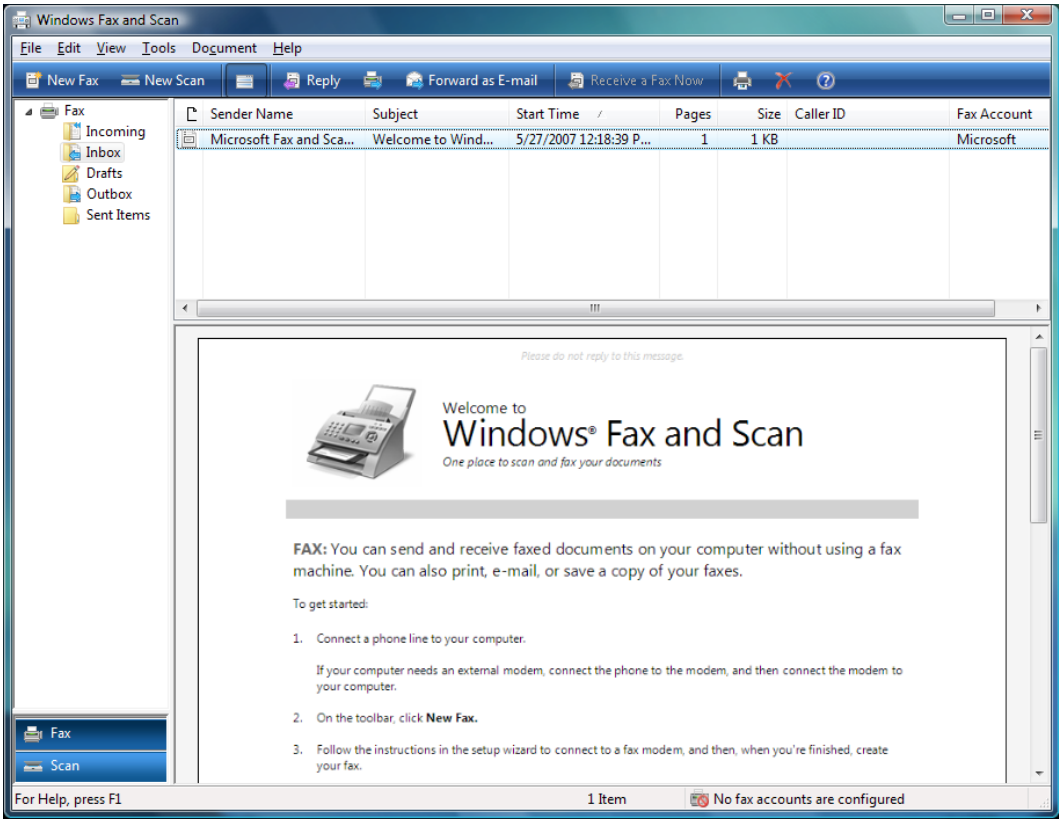

Figure 24 – Windows Fax and Scan, Fax view main menu

Windows Fax and Scan can be found, by default, on the main **All Programs menu** of the Windows Vista Business and Windows Vista Ultimate editions. It can be installed as an optional component in Windows Vista Enterprise.

The table below details some of the key features found in Windows Fax and Scan:

Feature	Brief Description
Drag-and-drop functionality	Makes it easy to file and sort all of your faxes and scanned files.
Fax and scan routing	Allows you to create routing lists of designated email addresses and server shares to automatically receive copies of scanned documents.
Live Preview	Lets you see how a document will look before you scan it and adjust settings instantly to get it just the way you want it.
One-click faxing and scanning	Makes faxing and scanning documents as easy as using email.

Configuring Windows Fax and Scan

Windows Fax and Scan offers several preset categories and folders to help you organize your faxes and scanned documents; additionally, you can create customized folders. To file faxes and scans, you simply drag and drop them into the appropriate folder. Terminology and functionality familiar to users of other Windows applications make using Windows Fax and Scan simple and intuitive.

In addition, Windows Fax and Scan supports multiple user accounts on the same computer. This is particularly useful for small businesses that have several employees sharing a single computer. Different employees can log on to the same computer to send faxes, and each one will be appropriately recognized and identified as the sender of his or her own faxes.

Faxing

To send and receive faxes using a modem

Before you begin, make sure that you've attached an analog phone line to your computer. You can't use a digital phone line to send or receive faxes.

If your computer has a built-in fax modem, Windows will automatically detect it during the setup process. You can connect to one local fax modem only, although you can connect to multiple fax servers or devices on a network. If you have an external fax modem, follow the manufacturer's instructions for attaching it to your computer. Make sure that the modem is turned on before taking these steps.

1. Navigate to **Start -> All Programs -> Windows Fax and Scan**
2. To use Fax view, at the bottom of the left pane, click **Fax**.
3. If you're connecting to a fax device for the first time, click **New Fax** on the toolbar and then follow the instructions in the Fax Setup Wizard.

If you've already connected to one or more fax servers or devices on a network and want to connect to a modem, navigate to **Tools -> Fax Accounts** and choose **Add**. Follow the instructions in the Fax Setup Wizard.

NOTE: To set up your computer to send faxes only, click "I'll choose later; I want to create a fax now in the Fax Setup Wizard." Keep in mind that by choosing this option, you will be able to send faxes but you will not be able to receive them.

To send and receive faxes using a server
Before you begin, make sure that your computer is connected to the network. Also, make sure that you know the network address of the fax server (for example, \\mycompanyfaxserver) and that you have permission to connect to it.

1. Navgiate to **Start -> All Programs -> Windows Fax and Scan**.
2. Click Fax at the bottom of the left pane.
3. Open **Tools** and then click **Fax Accounts**.
4. Click **Add**, and then, in the Fax Setup Wizard, click **Connect to a fax server on my network** and follow the instructions.

Scanning

Windows Fax and Scan offers one-click scanning of documents and images from locally connected or network-connected scanners and multifunction print/scan/fax devices. Windows Fax and Scan lists all of your scanned files, plus other useful information such as the scanner used to create the file and the day and time the document was scanned.

There are several adjustable settings for scanned documents available: paper size, color control, resolution, etc.; these settings are then stored as a **scan profile**. Windows Fax and Scan allows you to create and store multiple scan profiles, making it easy to achieve consistent quality with every scan.

Before you do a full scan of a document, you can use the **Live Preview** feature to see how it will appear on your computer after the final scan. Live Preview creates a low-resolution cached image of the document that you can easily modify. It allows you to experiment with changes and view them instantly.

You can connect a scanner directly to your computer (a *local scanner*), or you can connect to a scanner that is installed on and shared over a network (a *network scanner*). In both cases, you might need to install a driver or programs for using the scanner on your computer.

To add a local scanner
Refer to the scanner manufacturer's documentation before attempting to connect a local scanner. If the scanner has a universal serial bus (USB) connector, you can typically plug it into your computer and Windows will automatically install the driver. Some scanners may require additional software before plugging in the USB connector, while others might require you to turn on the scanner before or during the installation process.

To add a network scanner
Before you begin, make sure that you know the scanner model and manufacturer name, and that your computer is connected to the network. Windows will automatically detect the scanner and add it to the Network folder on your computer.

1. Navigate to **Start -> Network**.
2. Right-click the appropriate scanner and choose **Install**.
3. Follow the on-screen instructions.

Note: If Windows could not add the scanner to your Network folder automatically, check the information that came with the scanner to see how to install it.

Configure Windows Sidebar

Windows Sidebar overview

Windows Sidebar (*Figure 25*) is new Vista feature that provides mini-programs (called **gadgets**) in an easy to access bar on the side, bottom or top of your desktop. For example, you can use gadgets to display a picture slide show, view continuously updated headlines, or look up contacts.

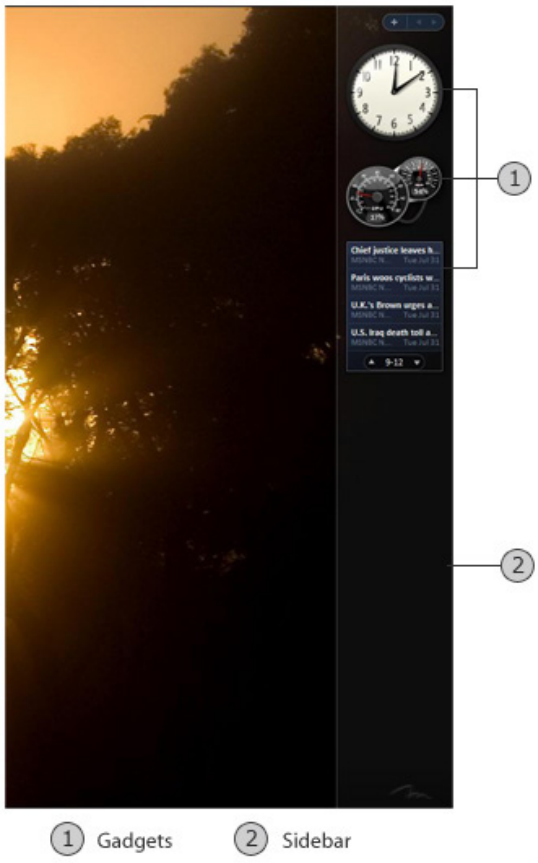

Figure 25 – Windows Sidebar and gadgets

Windows Sidebar configuration

Windows Sidebar configuration options enable you to ensure that Windows Sidebar appears when Windows Vista starts, is displayed on top of other windows, or is hidden from view. You can position Sidebar on the left, right, or top of the screen and, in a multi-monitor environment, you can specify on which monitor Windows Sidebar displays. You can add or remove gadgets according to user requirements, and organize gadgets over several pages. If you prefer to work from the desktop, you can remove gadgets from the Windows Sidebar and store them on the desktop instead. If you remove all of the gadgets you can choose to hide the Windows Sidebar.

To configure Windows Sidebar options, **right-click** any blank area of the Sidebar. This will bring up the Windows Sidebar configuration menu (*Figure 26*). The options in this menu allow you to:

- Order Gadgets
- Add Gadgets
- Change Sidebar Properties, (*Figure 27*).
- View Sidebar help
- Close the Sidebar

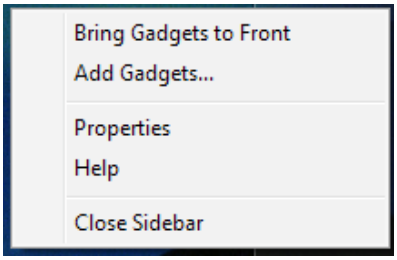

Figure 26 – Windows Sidebar configuration menu

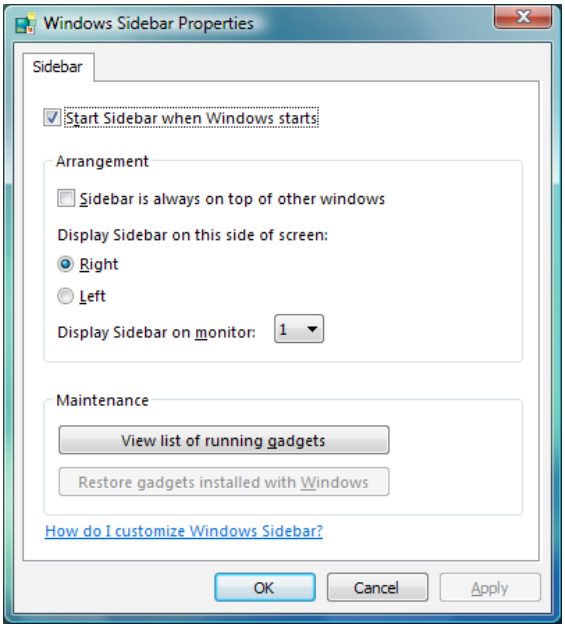

Figure 27 – Windows Sidebar Properties menu

Windows Sidebar Gadgets

Gadgets are mini-applications with a variety of possible uses. They can connect to web services to deliver business data, weather information, news updates, traffic maps, Internet radio streams, and even slide shows of online photo albums. Gadgets can also integrate with your applications to provide streamlined interaction. For example, a gadget can give you an at-a-glance view of all your online instant messaging contacts, the day view from your calendar, or an easy way to control your media player. Gadgets can also have any number of dedicated purposes. They can be calculators, games, sticky notes, and more.

Figure 28 - Windows Sidebar Gadget galery

Initially Windows Sidebar displays three Gadgets: the Clock, the Slide Show, and the Feed Viewer. Windows Vista comes with an essential set of gadgets to get you started, and you can easily download more from an online gadget gallery. This gallery hosts gadgets from a wide variety of developers and publishers.

Before a gadget can be added to Sidebar, it must be installed on your computer. Follow the steps below to see which gadgets are installed on your computer:

1. At the top of Sidebar, click the plus (+) sign (*Figure 30*) to open the Gadget Gallery.
2. Click the scroll buttons to see all installed gadgets.
3. Select a gadget and then click **Show details** to see information at the bottom of the dialog box.
4. To uninstall a Gadget, simply right-click on the Gadget and select **Uninstall**.

Figure 29 – Add Gadget button

NOTE: If you uninstall gadgets that came with Windows, you can restore them to the Gadget Gallery by following these steps:

1. Navigate to **Start -> Control Panel -> Appearance and Personalization -> Windows Sidebar Properties**.
2. Click "Restore gadgets installed with Windows."

To configure an individual Gadget, drag the mouse pointer over the Gadget. When you point to a Gadget, two buttons will appear near its upper-right corner: the **Close** button and the **Options** button (see *Figure 30*, below).

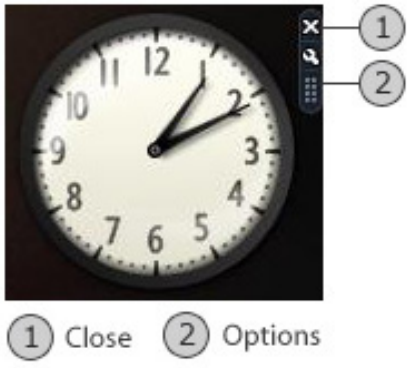

Figure 30 – Windows Sidebar Clock Gadget

Each Windows Sidebar Gadget has a unique configuration menu which controls that gadget's behavior. For example, the Slide Show Gadget can be configured to use specific folders as a source for images, to display images for a specified length of time, and to use a preferred transition effect.

Maintaining and Optimizing Systems That Run Windows Vista

Windows Vista introduces new diagnostic tools designed to help resolve problems with memory, networking, and startup failures. These new tools are collectively known as the **Windows Diagnostic Infrastructure** (WDI), designed not only to identify existing problems, but also to detect impending failures and alert you to take corrective or mitigating action. In many instances, if the tool is unable to resolve the problem, it provides easy-to-understand reports which should assist a Technology Specialist with resolving the problem. Some of these new tools are listed below:

- Performance Information and Tools
- Reliability and Performance Monitor
- Windows Memory Diagnostics
- Windows Network Diagnostics
- Windows Problem Reports and Solutions
- Startup Repair

Troubleshoot performance issues

Performance is a measure of how quickly a computer completes application and system tasks. Performance problems occur because of lack of available resources, including:

- The access speed of the physical hard disks.
- The amount of memory available to all running processes.
- The fastest speed of the processor.
- The maximum throughput of the network interfaces.
- How much of the resources the individual applications consume.
- Faulty or misconfigured components consuming resources.

Performance Information and Tools lists tasks that can help improve the performance of your computer, and it also shows information about your computer's performance capabilities.

To open Performance Information and Tools, navigate to **Start -> Control Panel -> System and Maintenance -> Performance Information and Tools**.

The left pane of Performance Information and Tools includes tasks that can help you improve your computer's performance. The following table describes these tasks:

Task	Description
Manage startup programs	Some programs start themselves automatically when you start Windows. Too many of these programs opening at the same time can slow down your computer. To disable these programs from startup and improve performance, use **Windows Defender**.
Adjust visual effects	You can optimize performance by changing how menus and windows appear.
Adjust indexing options	Indexing options can help you find what you're looking for quickly and easily on your computer.
Adjust power settings	Change power-related settings so that your computer resumes from power-saving settings more efficiently; adjust battery usage for portable computers.
Open Disk Cleanup	This tool deletes unnecessary or temporary files on your hard disk so you can increase the amount of storage space you have.
Advanced tools	Access advanced system tools, such as Event Viewer and System Information. View notifications about performance-related issues and what to do about them. For example, if Windows detects a driver is reducing performance, click the notification to learn which driver is causing the problem and view help on how to update the driver. Issues are ordered by impact.

Troubleshoot reliability issues by using built-in diagnostic tools

Reliability is a measure of how often a system deviates from configured, expected behavior. Reliability problems occur as the result of the following:

- Application crashes.
- Service freezes and restarts
- Driver initialization failures.
- Operating system failures.

Reliability and Performance Monitor

Windows Vista Reliability and Performance Monitor can be used to gain an overview of system performance as well as to access more detailed information in order to pinpoint the source of the problem. This tool enables you to:

- Track the performance impact of applications and services.
- Generate alerts and take action when user-defined thresholds are exceeded.

The following tools are included with the Reliability and Performance Monitor:

- **Resource Overview** – provides a quick overview of the average performance of the system. CPU utilization, disk activity, network interface activity, and memory usage are displayed graphically, enabling you to see problem components at a glance. Additional information is available for each component by expanding a detailed section which shows the services and applications utilizing the resource.
- **Performance Monitor** – provides a visual display of built-in Windows performance counters, either in real time or historically. Performance Monitor includes the following features:
  - Multiple graph views
  - Custom views that can be exported as Data Collector Sets (DCS).
- **Reliability Monitor** – a useful tool that provides a timeline of changes in the system and its reliability as well as detailed information to help pinpoint how to achieve optimal system reliability. Includes the System Stability Chart, which overviews system stability yearly in daily increments. All error and warning messages are included.
- **Data Collector Sets (DCS)** – a custom set of performance counters, event traces, and system configuration data that you define and save so that you can run and view as a single, portable component. A DCS can be used on its own, grouped with other DCSs and incorporated into logs or viewed in Performance Monitor. You can also configure a DCS to generate alerts when it reaches thresholds and it can be used by third-party applications. A DCS can be configured to run at a scheduled time, for a specific length of time, or until it reaches a predefined size.
- Reports – Users of Server Performance Advisor in Windows Server 2003 can now find the same kinds of diagnosis reports here. Report generation time is improved and reports can be created from data collected with any DCS. This enables Technology Specialists to repeat reports and assess how changes have affected performance or the report recommendations.

Follow the steps below to configure the Performance Monitor display:

1. **Right-click** in the Performance Monitor display area and choose **Properties**.
2. Make the desired configuration changes.
3. To see the effect of your changes without re-opening the Properties dialog box, you can click **Apply** after any modification.
4. When you are finished, click **OK**.

You can save the information in your current Performance Monitor display as a web page or an image by following the steps below:

- To save the current Performance Monitor display as a **web page**:
  1. **Right-click** in the Performance Monitor display area and click **Save Settings As**.
  2. Choose a directory where you want to save the file.
  3. Type a name for the saved display file, and then click **OK**.
- To save the current Performance Monitor display as an image:
  1. **Right-click** in the Performance Monitor display area and click **Save Image As**.
  2. Choose a directory where you want to save the file.
  3. Type a name for the saved display file, and then click **OK**.

Additional considerations

- You can also access Performance Monitor properties by pressing **CTRL+Q**, or by clicking the **Properties** button in the toolbar.
- If there are no counters in the current display, you can open the **Add Counters** dialog box by selecting the **Data** tab and clicking **Add**.
- You can open log files or log databases from the Performance Monitor properties in the **Source** tab. It is possible to open multiple log files simultaneously.

Windows Memory Diagnostics

The Windows Memory Diagnostics tool works with Microsoft Online Crash Analysis to monitor your computer for symptoms of defective physical memory. If the Memory Diagnostics tool identifies a memory problem, Windows Vista will avoid using the affected portion of physical memory to enable the operating system to start successfully and to avoid application crashes.

If the Windows Memory Diagnostics tool detects any problems with physical memory, Microsoft Online Crash Analysis automatically prompts you to run the tool. You can choose whether to restart your computer and check for problems immediately or to schedule the check for the next time the computer restarts.

When the computer restarts, Windows Memory Diagnostics tests the computer's physical memory. When the test is finished, you are provided with an easy-to-understand report detailing the problem. Information is also written to the event log for future analysis.

The Windows Memory Diagnostics tool can also be run manually from Administrative Tools in Control Panel; you are given the same choices — to run the tool immediately or to schedule it to run when the computer restarts.

To access advanced diagnostic options, press **F1** while the test is running. Press the **Tab** key to move between different advanced options. When you have selected your options, press **F10** to start the test. Advanced options include:

- **Test mix**: Choose what type of test you want to run.
- **Cache**: Choose the cache setting you want for each test.
- **Pass Count**: Type the number of times you want to repeat the tests.

Windows Network Diagnostics

The Windows Network Diagnostics tool runs automatically when it detects a problem. You can also choose to run the tool manually by using the **Diagnose** option on the Local Area Connections Status property sheet.

If Windows Vista detects a problem that can be repaired automatically, it will do so; if not, the user is directed to perform simple steps to correct the problem without having to call for support.

Windows Problem Reports and Solutions

The Windows Problem Reports and Solutions tool works in conjunction with Windows Error Reporting Services to provide a history of attempts to diagnose problems on your computer. If an error occurs while an application is running, Windows Error Reporting Services will prompt the user to choose whether to send error information to Microsoft over the Internet. If information is available that will help the user solve the problem, Windows displays a message to the user with a link to that information. The Problem Reports and Solutions tool enables you to track this information and recheck to find new solutions.

Once the Windows Memory diagnostics tool or the Windows Network Diagnostics tool has run, you can use the Problem Reports and Solutions tool to see the problem report details, or to recheck for a solution to a problem.

To access Problem Reports and Solutions, navigate to **Start -> Control Panel -> System and Maintenance -> Problem Reports and Solutions**. From the Tasks menu in the Problems Reports and Solutions tool, you can:

- Check for new solutions
- View problems to check (opens by default)
- View the problem history
- Change the settings
- Clear the solution and problem history

Startup Repair

The Windows Vista Startup Repair tool is designed to automatically fix many common problems and enable a Technology Specialist to quickly diagnose and repair more complex startup problems. When Startup Repair runs, it scans the computer for the problem and then attempts to fix it so that the computer can start correctly.

When a startup failure is detected, the system automatically starts the Startup Repair tool. The Startup Repair tool then performs diagnostics and analyzes startup log files to determine the cause of the startup failure. Once the Startup Repair tool determines the cause of the failure, it attempts to automatically fix the problem.

The Startup Repair tool can automatically repair the following problems:

- Incompatible drivers
- Missing or corrupted startup configuration settings
- Corrupted disk metadata

After the operating system is repaired, Windows Vista notifies you of the repairs and provides a log so that you determine the steps the Startup Repair tool performed.

If the Startup Repair tool is unable to resolve startup errors, the system is rolled back to the last known working state. If the Startup Repair tool cannot automatically recover the system, it provides diagnostic information and support options to make further troubleshooting easier.

You can start the Startup Repair tool manually from the Windows Vista installation disc. After you start the computer from the DVD, menus will be displayed that enable you to access the manual repair tools.

Note: Startup Repair cannot fix hardware failures, such as a failing hard disk or incompatible memory, nor does it protect against virus attacks. Startup Repair is not a backup tool, so it cannot help with recovering data files. Startup Repair was not designed to fix Windows installation problems.

Configure Windows Update

Windows Update is a service that helps to keep your computer up-to-date and more secure by providing software updates. The update service can be run automatically or manually.

The Automatic Updates feature of Windows Update downloads and installs the following:

- **Important Updates** that include security updates and critical performance updates.
- **Recommended Updates** that help fix or prevent problems or expand the functionality of Windows applications.

You can turn on Automatic Updates during Vista's initial setup, or you can configure it at any later time. Select from the following Windows Update preference options:

- Automatically download and install
- Download and prompt user to install
- Notify user and prompt to download
- Do not use automatic updates

The recommended option is *Automatically download and install*. This option downloads updates and installs them at a scheduled time (3:00 AM by default). If you turn off your machine before the scheduled time, you can install the updates as part of the shutdown process. If you computer is in hibernate or standby mode and plugged into a power supply, Windows will activate your computer to install the updates.

Alternatively, you can configure Windows Update to download updates automatically, but install them manually. This option enables you to select which of the downloaded updates to install. Any updates you choose not to install are hidden, so that you are not repeatedly prompted to install the same unwanted update. Hidden updates can be accessed through the **Restore Hidden Updates** option and installed at a later date.

Finally, you can configure Windows Update to notify you that updates are available, but let you choose when to download and install them. This option also enables you to hide updates that you do not wish to install. Microsoft does not recommend the *Do not use automatic updates* setting.

Windows Update downloads updates for your computer in the background while you are online. If the Internet connection is interrupted before an update is fully downloaded, the download process continues once the connection is available. Although installation of updates occurs automatically in the background, when it occurs depends on the configuration options you choose. Most updates will occur seamlessly, with the following exceptions:

- If an update requires a restart to complete installation, you can schedule it for a specific time.
- When a software update applies to a file in use, Windows Vista can save the application's data, close the application, update the file, and then restart the application. The user may be prompted to accept an End User License Agreement (EULA) as the application restarts.

The Windows Update control panel enables you to manage your updates in a number of ways. You can scan for the latest updates, review details about each update, restore hidden updates, and access your update history. You can also access the Windows Update Preference Options by using the **Change Settings** option in the Windows Update control panel. The settings in the Windows Update Control Panel are as follows:

- Check for updates
- Change settings
- View update history
- Restore hidden updates
- Windows Ultimate Extras

Windows Vista Ultimate edition includes Windows Ultimate Extras, which are programs, services, and premium content for Windows Vista Ultimate. Windows Update notifies you when new downloads become available.

Configure Data Protection

Because there are so many security threats which can endanger data, Windows Vista has improved support for data protection at the document, file, directory and machine level. These features include (but are not limited to):

- **Integrated Rights Management client** – allows organizations to enforce policies regarding document usage.
- **Encrypting File System** – enhanced in Windows Vista to allow storage of encryption keys on smart cards, providing better protection.
- **BitLocker Drive Encryption** – adds machine-level data protection.

BitLocker Drive Encryption

Turning on BitLocker Drive Encryption (BitLocker) can help protect all files stored on the drive Windows is installed on.

Unlike Encrypting File System (EFS), which enables you to encrypt individual files, BitLocker encrypts the entire system drive, including the Windows system files necessary for startup and logon. You can log on and work with your files normally, but BitLocker can help block hackers from accessing the system files they rely on to discover your password, or access your hard disk by removing it from your computer and installing it in a different computer. BitLocker can only help protect files that are stored on the drive that Windows is installed on. If you store files on other drives, you can help protect those files with EFS.

When you add new files to a drive with BitLocker enabled, BitLocker encrypts them automatically. Files remain encrypted only while they are stored on the encrypted drive. Files copied to another drive or computer are decrypted. If you share files with other users, such as through a network, these files are encrypted while stored on the encrypted drive, but they can be accessed normally by authorized users.

During computer startup, if BitLocker detects a system condition that could represent a security risk (for example, disk errors, a change to the BIOS, or changes to any startup files), it will lock the drive and require a special BitLocker recovery password to unlock it. Make sure that you create this recovery password when you turn on BitLocker for the first time; otherwise, you could permanently lose access to your files.

You can turn off BitLocker at any time, either temporarily by disabling it, or permanently by decrypting the drive. Follow the steps below to turn BitLocker on or off:

- **To turn on BitLocker**:
    1. Open BitLocker. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.
    2. Click **Turn On BitLocker**. This opens the BitLocker setup wizard. Follow the instructions in the wizard.

    NOTE: You might have to address one or more BitLocker hardware requirements before you can turn on BitLocker.
- **To turn off** (or temporarily disable) **BitLocker**:
    1. Open BitLocker. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.
    2. Click **Turn Off BitLocker**. This opens the BitLocker Drive Encryption dialog box. To decrypt the drive, click **Decrypt the volume**. To temporarily disable BitLocker, click **Disable BitLocker Drive Encryption**.

Before you can turn on BitLocker Drive Encryption you need to make sure that your computer's hard disk has the following:

- **At least two volumes**. If you create a new volume after you have already installed Windows, you will have to reinstall Windows before turning on BitLocker.
- One volume is for the operating system drive (typically drive C:) that BitLocker will encrypt, and one is for the active volume, which must remain unencrypted to start the computer. The size of the active volume must be at least 1.5 gigabytes (GB). Both partitions must be formatted with the NTFS file system.

Note: The terms *partition* and *volume* are often used interchangeably. On most computers, they are the same: one partition equals one volume. On larger computer systems, however, it is possible to have a single volume span several partitions. BitLocker installs on a simple volume, where one volume equals one partition.

If you do not already have two partitions, you can use the BitLocker Drive Preparation Tool to help get your system ready for BitLocker by creating the required second partition.

Because BitLocker stores its own encryption and decryption key in a hardware device that is separate from your hard disk, your computer must have one of the following:

- A computer with Trusted Platform Module (TPM) – a special chip in some newer computers that supports advanced security features. If your computer was manufactured with TPM version 1.2 or higher, BitLocker will store its key in the TPM.
- A removable USB memory device, such as a flash drive. If your computer doesn't have TPM version 1.2 or higher, BitLocker will store its key on the flash drive.

Note: Some BitLocker features and settings can be enabled by Group Policy settings.

Configuring and Troubleshooting Mobile Computing

A mobile PC user faces many challenges that a desktop computer user seldom encounters. A desktop computer user typically has a reliable power source, and is connected to a single network. A mobile PC user must manage transitions as they move from place to place. Windows Vista addresses the unique needs of mobile PC users by providing several new and enhanced features.

Configure Mobile Display Settings

Mobility Center

Mobility Center consists of several of the most commonly used mobile PC settings. Depending on your system, the following display setting tiles appear in the Mobility Center window:

- **Brightness** – Move the slider to temporarily adjust the brightness of your display. To adjust the display brightness settings for your power plan, click the icon on the tile to open **Power Options** in Control Panel.
- **Screen Rotation** – Change the orientation of your Tablet PC screen, from portrait to landscape, or vice versa.
- **External Display** – Connect an additional monitor to your mobile PC or customize the display settings.
- **Presentation Settings** – Adjust settings, such as the speaker volume and the desktop background image, for giving a presentation.

Mobility Center can be opened using one of the following methods:

- Navigate to **Start -> Control Panel -> Mobile PC -> Windows Mobility Center**.
- Click the battery meter icon in the notification area of the Windows taskbar and then click Windows Mobility Center.
- Press the Windows logo key + X.

Mobile computer users often have to reconfigure their display settings for meeting or conference presentations. Windows Vista includes a group of **Presentation Settings** that can be applied with a single click when you connect to a display device. When you are event is concluded, you can return to your previous setting with one click on the notification area icon.

When Presentation Settings are turned on, the mobile PC stays awake and system notifications are turned off. You can also choose to turn off the screen saver, adjust the speaker volume, and change the desktop background image. These settings are automatically saved and applied every time you give a presentation, unless you manually turn them off.

Presentation Settings can be turned on using one of the following methods:

- Navigate to **Start -> Control Panel -> Mobile PC -> Windows Mobility Center**. Then, on the Presentation Settings tile, click Turn on.
- Connect the mobile PC to a network projector. *- or -*
- Connect the mobile PC to an additional monitor. Then, in the **New Display Detected** dialog box, select the "Turn on presentation settings check box," and click **OK**.

Note: To turn Presentation Settings on or off for the current monitor or projector the mobile PC is connected to, follow these steps:

1. Navigate to **Start -> Control Panel -> Mobile PC -> Windows Mobility Center**.
2. On the **Presentation Settings** tile, click the Change Presentation Settings icon.
3. In the Presentation Settings dialog box, click **Connected displays**.
4. In the Current Displays dialog box, select or clear the "I always give a presentation when I use this display configuration" check box. Click **OK**.

Presentation Settings automatically turn off when you disconnect your mobile PC from a network projector or additional monitor, and when you shut down or log off from your mobile PC. You can also manually turn Presentation Settings off as follows:

1. Navigate to **Start -> Control Panel -> Mobile PC -> Windows Mobility Center**.
2. On the Presentation Settings tile, click **Turn off**.

Follow the steps below to customize Presentation Settings:

1. Navigate to **Start -> Control Panel -> Mobile PC -> Windows Mobility Center**.
2. On the Presentation Settings tile, click the Change Presentation Settings icon.
3. In the Presentation Settings dialog box, adjust settings for giving a presentation, and click **OK**.

Working with multiple monitors

When you connect your mobile PC to an external display, Windows Vista opens the New Display Detected dialog box, where you can select one of the following display options:

- **Mirrored**. Duplicates, or "mirrors," your desktop on each display. Mirrored is the default display option. It's useful when you plan to use your mobile PC to give a presentation on a projector or a fixed display in a conference room, such as a wall-mounted plasma display or a TV-type monitor.
- **Extended**. Extends your desktop across all displays. This option is useful if you want to increase your work space.
- **External display only**. Shows your desktop on all external monitors, but not on your mobile PC's display. This display option is useful if you want to conserve battery power. You can also use this option when you play a DVD on a mobile PC that supports full-screen video playback on only one display.

When you connect an additional monitor to your mobile PC, Windows automatically detects the monitor and displays your computer's desktop. You can then choose how you want your desktop to appear and customize the display settings, such as screen resolution and color depth. Follow the steps below when connecting another monitor:

1. Physically connect the monitor to your mobile PC.
    - If Windows can't identify the monitor, open the New Display Detected dialog box by using one of the following methods:
        - Press the keyboard shortcut that enables the additional display. This is usually **Function+F4**, **F5**, or **F8**. Otherwise, check the information that came with your mobile PC.
        - Navigate to **Start -> Control Panel -> Mobile PC -> Windows Mobility Center**. Then, on the External Display tile, click Connect display.
2. In the New Display Detected dialog box, select one of the following display options: **Mirrored**, **Extended**, **External Display Only** (see the beginning of this section for a detailed explanation), and then click **OK**.
3. If Windows can't identify the monitor that you connect, it automatically applies the last display settings that you used for that type of monitor and asks whether you want to keep the settings. Click **OK** to keep these settings.
    - If you click Cancel or do nothing, the Display Settings dialog box appears so that you can manually choose the display settings.
    - **Note**: To select different display settings at any time, open Display Settings in Control Panel.
4. Navigate to **Start -> Control Panel -> Appearance and Personalization -> Personalization -> Display Settings**. Adjust the settings to your preference.

Troubleshooting multiple monitors

When you connect an additional monitor to your computer, the Start button and taskbar are located by default on the primary display –your computer display. If you want the Start button and taskbar to appear on a different display, you must designate that display as the primary display by following the steps below:

1. Navigate to **Start -> Control Panel -> Appearance and Personalization -> Personalization -> Display Settings**.
2. On the Monitor tab, click **Identify Monitors**. The display that is identified by the number "1" is the primary display.
3. Click the numbered icon that represents the display that you want to designate as the primary display, and then select the "This is my main monitor check box." **NOTE**: In Display Settings, the primary display is also called the main monitor.
4. Click **OK**.
5. When prompted to keep the settings, click **Yes**.

When you try to drag a window from one display to another, the window may stop when it reaches the edge of the screen because the displays might not be correctly aligned. You should check the display alignment to ensure that the numbered icons that represent the displays are correctly aligned. Follow the steps below to check the display alignment:

1. Navigate to **Start -> Control Panel -> Appearance and Personalization -> Personalization -> Display Settings**.
2. On the Monitor tab, make sure that the numbered icons that represent the displays are aligned the way that you want, either side by side or top to bottom.

Note: If the screen resolution is different for each display, the icons won't be the same size. For example, an icon on a display set to a 1024 × 768 screen resolution appears larger than an icon on a display with a lower resolution, such as 800 × 600.

Configure Mobile Devices

Windows Vista includes tools which enable you to connect a variety of mobile devices to your computer and synchronize data. The mobile devices supported by Microsoft Vista include:

- **Personal Digital Assistant (PDAs)** – A PDA is a handheld device that can range in function from a simple personal organizer to a fully functioning mobile computer. Input for the device is typically achieved by using a stylus on a touch screen, a keyboard, or a combination of both.
- **Windows Mobile devices** – Windows Mobile devices are available in either Pocket PC or Smartphone forms and feature the familiar Windows user interface and applications. Windows Mobile devices also include Windows Media Player and typically feature mobile phone, Bluetooth, and Wi-Fi capability. Input for Windows Mobile devices is typically achieved by using a stylus on a touch screen, a keyboard, or a combination of both. The Windows Mobile operating system also supports voice commands.
- **Portable media players** – A portable media player is a small, battery-powered device containing either flash memory or a hard disk drive on which you can play digital media files. Some devices have a screen. Media is copied to the device from the computer running Windows and can come from your own CD/DVD collection or be purchased and downloaded from the Internet.
- **Mobile phones** – A mobile phone is a portable telephone, usually cellular or satellite in nature. Many mobile phones now have some PDA and media player functionality. Input for the device is usually a numerical keypad, though some phones can use styluses.

Mobile devices are generally connected to your computer either via a physical medium (i.e., USB cable or docking cradle), or through a wireless connection (i.e., infra-red, Bluetooth, or Wi-Fi). Most mobile devices ship with a USB cable or cradle and most modern computers come equipped with infra-red or Bluetooth.

Before you can synchronize information with devices, you must set up **sync partnerships**. You can also enable a schedule to automatically synchronize content. Windows Vista includes the Sync Center to help you manage connections, partnerships, and schedules. The Sync Center can also be used to troubleshoot sync relationships.

Windows Vista Sync Center enables you to initiate a manual sync, stop an in-progress sync, view the status of all current sync activities, and receive notifications to resolve conflicts. Sync Center does not replace third-party sync tools or functionality. For example, a Windows Mobile device will still use its own infrastructure, Windows Mobile Device Center, to physically synchronize the data between it and a Windows Vista computer. Windows Mobile Device Center is the replacement for previous Windows versions' ActiveSync. If you want to change the granular sync settings for any relationship, Sync Center simply directs you

to the Windows Mobile Device Center or, in the case of a partner device, to that third party's data-management settings infrastructure.

Follow the steps below to sync with different types and brands of mobile devices using Sync Center:

1. Turn on the device and plug it into your computer. If it is a wireless device, make sure that a wireless connection is established between the device and your computer, or physically connect it with a Universal Serial Bus (USB) cable.
2. Open Sync Center. Navigate to **Start -> All Programs -> Accessories -> Sync Center**.
3. In the left pane of Sync Center, click "Set up new sync partnerships."
4. Click the name of the device in the list of available sync partnerships.
5. On the toolbar, click **Set Up**.
6. Select the settings and schedule to determine how and when you want to sync your device with your computer.
7. To start syncing immediately, click "View sync partnerships," select the device, and then, on the toolbar, click **Sync**.

Notes:

- If your device does not appear in this list, try connecting it again or turning it off and on followed by clicking the refresh button in Sync Center. If the device still does not appear, go to the next section of this help topic for possible explanations.
- Some sync partnerships do not have any sync settings or a schedule that you can adjust.

If you are unable to get a device to work with Sync Center, it may help to check if your device is listed in Device Manager. Even if Windows recognizes your device, it might not be compatible with Sync Center. To check this, see Open Device Manager. Otherwise, try these troubleshooting tips:

- Check the contents of a device before attempting to sync it with your computer.
- You can sync your contacts with some mobile devices. To sync contacts with a mobile device, the device must be able to read the .contact file that Windows creates for each individual contact. The device must also be compatible with Sync Center.
- To sync a Windows Mobile device with a computer running Windows Vista, you must use Windows Mobile Device Center software. The first time you plug a Windows Mobile device into a computer that is connected to the Internet and running Windows Vista, Windows Mobile Device Center will automatically download and install. After you set up your device to sync in Windows Mobile Device Center, the sync results will appear in Sync Center.

Configure Tablet PC software

A Tablet PC is a type of notebook computer equipped with a touch-sensitive screen designed to interact with a complementary pen-shaped stylus. It is a fully functional laptop computer with a screen that turns and folds into the keyboard. You can use the pen directly on the screen just as you would a mouse to select, drag, and open files, or in place of a keyboard to handwrite notes. Unlike a touch screen, the Tablet PC screen only receives information from the pen; you can't use your finger to interact with the device. The Tablet PC uses a device called a digitizer, which interprets the movements of the stylus and turns them into mouse or cursor movement. Windows Vista includes several new features that can help you be more efficient with your Tablet PC.

Tablet PC Settings tool

Tablet PC settings are configured by using the **Tablet PC Settings** tool located under Mobile PC in the Control Panel. The following table provides a description of the tabs available to you and their function:

Tab	Function
General	Configure on-screen menus for left-handed or right-handed users and calibrate the effectiveness of your tablet pen.
Buttons	Customize the actions of some tablet buttons.
Handwriting Recognition	Configure Tablet PC handwriting recognition. The Tablet PC can adapt to your handwriting style, resulting in a more productive end-user experience. There are two sections found under this tab: **Personalization** and **Automatic Learning**.
Display	Manually change screen orientation. Most Tablet PCs have hardware buttons for changing screen orientation, so this tab also allows you to change the order in which screen orientation is changed when this button is used.
Other	Change pen and input device settings.

You can customize the actions that tablet buttons perform on some Tablet PCs. Most tablet buttons can perform primary and secondary actions. Press the button once, quickly, to perform the primary action. Press and hold the button to perform the secondary action. Follow the steps below to customize tablet buttons in Windows Vista:

1. Navigate to **Start -> Control Panel -> Mobile PC -> Tablet PC Settings**.
2. Open the **Buttons** tab.
3. In the Button settings list, tap the name of the screen orientation for which you want to change your button settings.
4. In the Tablet button list, tap the name of the tablet button that you want to customize. **Note**: If you don't know the name of the button you want to customize, tap a tablet button name in the button list to view the picture of where the button is located on your Tablet PC.
5. Tap **Change**.
6. In the **Press** list, tap the name of the action that you want the button to perform.

- or –

In the **Press and hold** list, tap the name of the action that you want the button to perform.

7. If you select an action that requires more information, enter the appropriate information under Settings.
8. Tap **OK** twice.

It is important to note that not all tablet buttons can be customized. Follow the steps below to view which tablet buttons are customizable:

1. Navigate to **Start -> Control Panel -> Mobile PC -> Tablet PC Settings**.
2. Open the Buttons tab. The names of the tablet buttons that you can customize appear in the Tablet button list.

Tablet PC Input Panel

Included in Windows Vista is the Tablet PC Input Panel tool used to enter text and other symbols with the digital pen instead of the keyboard. There are two ways to display the Input Panel:

- An icon for the Input Panel appears in a small tab docked on the left edge of the screen. Hover the mouse pointer over the tab to display it, and then click the icon or any part of the tab.
- Move the pen over any area in which you can enter text (such as a text box). In most cases, the Input Panel icon appears near the text entry area. Click the icon when it appears.

Note: You can also add an icon for the Input Panel to the Vista taskbar. Right-click the Taskbar, and then click Toolbars, Tablet PC Input Panel.

The Windows Vista Input Panel comes with a few options. Click Tools and then click Options in the menu that appears. The following is a list of some of the settings:

Setting	Description
Auto Complete (Settings Tab)	When activated, the input panel automatically completes recognized handwriting in the first few characters. Click the displayed banner with the completed entry to automatically insert it.
Show the Input Panel Tab (Opening Tab)	Toggles the Input Panel tab on and off.
You Can Choose Where the Input Panel Tab Appears (Opening Tab)	Choose between "On the Left Edge of the Screen" (default) and "On the Right Edge of the Screen."
New Writing Line (Writing Pad Tab)	Slider specifies how close to the end of the writing line you want to write before text wraps to a new line automatically.
Gestures (Gestures Tab)	Activating this option enables Vista's new "scratch-out" gestures: • Strikethrough: A horizontal line through text. • Vertical: An M- or W-shaped gesture through text. • Circular: A circle or oval around text. • Angled : An angled line through text.
Password Security (Advanced Tab)	Controls security features when using the pen to enter passwords. For instance, the High setting switches to an onscreen keyboard and doesn't allow the writing pad for entering password information.

Pen Flicks

Windows Vista enhances pen functionality by adding **pen flick** gestures. These gestures make it easy to quickly navigate and perform shortcuts. You can customize pen flicks to perform many functions, which increases your efficiency and make pen use feel more natural. To make pen training easier, Windows Vista includes a tutorial that presents the essentials of using a tablet pen to perform these shortcuts. Navigate to **Start -> All Programs -> Tablet PC -> Pen Flicks Training**.

You can customize pen flicks to perform functions that you use on a regular basis. For example, if you frequently use keyboard shortcuts, such as CTRL+F5 or ALT+TAB, you can assign a pen flick action to do this for you. Follow the steps below to customize pen flicks:

1. Navigate to **Start -> Control Panel -> Mobile PC -> Pen and Input Devices**.
2. Tap the **Flicks** tab.
3. Select the "Use flicks to perform common actions quickly and easily" check box, choose Navigational and editing flicks, and then tap **Customize**.
4. Pen flick actions appear on the menu, with one action for each direction.
5. Do one of the following:
    - To change a pen flick action, select it on the menu.
    - To restore default pen flick actions, tap Restore defaults.

If you are having problems using pen flicks, try the following actions:

- Make sure that the "Use flicks to perform common actions quickly and easily" check box is selected on the Flicks tab of Pen and Input Devices in Control Panel.
- Make sure that you're performing pen flicks with a tablet pen rather than a mouse.
- To view your pen flicks settings, tap the Pen Flicks icon in the notification area of the Windows taskbar.
- If only navigational flicks are enabled, make sure that you're moving your tablet pen in one of the four active directions. To view your pen flicks settings, tap the Pen flicks icon in the notification area of the Windows taskbar.
- Make sure that you are not trying to perform a pen flick over an ink-enabled surface, such as Tablet PC Input Panel or Windows Journal. If you try to perform a flick over an ink-enabled surface it will be interpreted as an ink stroke rather than a pen flick.
- Make sure the application that you are using responds to pen flicks. To check this, try performing a pen flick in an application that *does* accept pen flicks, such as Internet Explorer.
- If you're still having trouble performing pen flicks, it may be helpful to practice using pen flicks (see information about the **Pen Flicks Tutorial**, in the first paragraph of this section).

Configure Power Options

Battery Meter

With Windows Vista, you have more control over how your computer uses and manages power than ever before. One handy tool for monitoring and configuring your power settings is the **Battery Meter**. Displayed in the notification area of the Windows taskbar, the Battery Meter helps you manage your computer's power consumption by indicating how much charge is remaining on your battery and which power plan your computer is using. You can also use the Battery Meter to apply a different power plan. Although the Battery Meter is more commonly used with mobile PCs, it can also appear on a desktop computer if the computer is plugged into a USB uninterruptible power supply (UPS) or other short-term battery device.

When you hover over the battery icon, you can see the percentage of battery charge remaining and the power plan that Windows is using.

Note: Many mobile PCs are equipped with more than one battery. Click the battery icon to see the charge remaining on each battery. Hover over the icon to see the combined charge.

The Battery Meter also indicates whether the mobile PC is plugged in or running on battery power. When the charge on your battery is low, the Battery Meter displays a notification directly above the battery icon.

The battery icon changes appearance to display the current state of the battery so that you can see how much charge remains. When the battery charge is above 25 percent, the battery icon is green. When the battery charge reaches 25 percent, a yellow triangle with an exclamation point (!) appears above the green battery icon. When the charge reaches the low-battery level, a red circle with a white "X" appears above the green battery icon.

When you click the battery icon, the Battery Meter indicates how much charge remains. From the Battery Meter, you can also switch to a different type of power plan (for example, from a plan that optimizes system performance to a plan that saves power).

To change a power plan's settings or to select a power plan that isn't shown on the Battery Meter, click **More power options**.

Power Options

Windows Vista Power Options enable the user to conserve a mobile computer's battery life by changing the following performance options:

- **CPU speed** – Reducing the speed of the processor reduces its power consumption.
- **Display brightness** – The lower the brightness setting, the lower the power usage.

Most CPU manufacturers build speed control mechanisms into their products. For example:

- Intel uses a series of technologies called SpeedStep which allows Windows Vista to dynamically control the clock speed of the processor and lower the core voltage.
- AMD uses a technology called PowerNow which allows for software control of processor clock speed and core voltage.
- Transmeta and Via also provide similar processor speed control functions in their processors.

Windows Vista has three, default power plans that are designed to maximize computer and battery performance. These plans provide single-click access for changing a variety of system settings to optimize power or battery usage, and include alternate settings for running the mobile device from either AC or DC power. The three plans are:

- **Balanced** – This plan balances energy consumption and system performance by adapting the computer's processor speed to your activity. It provides the best balance between power and performance.
- **Power saver** – This plan saves power on your mobile computer by reducing system performance. Its primary purpose is to maximize battery life by lowering system performance.
- **High performance** – This plan provides the highest level of performance on your mobile computer by adapting processor speed to your work or activity and by maximizing system performance. It also consumes more power.

In addition to the plans listed above, you can customize or create additional power plans for various scenarios by using Power Options in the Control Panel. Some hardware manufacturers supply additional power plans and power options.

Practice Questions

Chapter 1 Installing and Upgrading Windows Vista

1. An entire department of computers is to be migrated from Windows XP to Windows Vista, a roll-out that will occur in phases over the next few months. Individual user data must be preserved, but you must first identify applications, devices and system information. How might you achieve this task?

   Select the best answer.

   - ❍ A. Use the Windows Vista Compatibility Evaluator in the Application Compatibility Toolkit.
   - ❍ B. Use the Inventory Collector in the Application Compatibility Toolkit.
   - ❍ C. Use the Standard User Analyzer portion of Application Compatibility Toolkit.
   - ❍ D. Use the Setup Analysis Tool portion of Application Compatibility Toolkit.

2. When a Windows Vista installation fails to boot or start up, there is usually an accessible means to fix it. You encounter such a problem. What are your options?

   Choose the best TWO answers.

   - ❑ A. Use the Windows Preinstallation Environment utility.
   - ❑ B. Use the System Preparation utility.
   - ❑ C. Use the ImageX tool.
   - ❑ D. Use the Windows Recovery Environment utility.
   - ❑ E. Use the BCDEdit utility.

3. Microsoft and select licensed resellers offer an upgrade path to different versions of Windows Vista for users who purchase licenses online. This helps reduce the number of installation disks in circulation and applies to Home Basic, Home Premium and Business editions. How might you receive this upgrade if you qualify?

   Select the best answer.

   - ❍ A. Use the Windows Upgrade Advisor.
   - ❍ B. Use the Windows Anytime Upgrade.
   - ❍ C. Use the Windows Automatic Update.
   - ❍ D. Use the Windows Online Update.

4. You upgrade a system that contains a layered service provider from a previous version of Windows Vista. The system loses network connectivity when configured for dynamic address assignment. How would you verify that this upgrade is the probable issue?

   Select the best answer.

   - ❍ A. Open a command prompt with administrator rights, issue netsh winsock reset and check the listings.
   - ❍ B. Open a command prompt, issue ipconfig and check for a 169.254.x.x IPv4 address.
   - ❍ C. Unplug and reinsert the network card, check for a loose cable and try to ping a nearby host.
   - ❍ D. Call the Internet Service Provider and contact a network administrator.

Chapter 2 Configuring and Troubleshooting Post-Installation System Settings

1. You create a Complete PC Backup image for a Windows computer that does not contain an NTFS partition. Later, during a restore procedure, you elect to format and repartition the disk but the backup fails to produce a workable OS. What should you do to avoid this situation? Each answer represents a part of the complete solution.

   Choose the best TWO answers.

   - ❑ A. Roll back the computer to a last known good state and then create the backup image.
   - ❑ B. Convert the partition to NTFS.
   - ❑ C. Upgrade the Windows Vista installation from the install media.
   - ❑ D. Choose to format and repartition the drive during the restore operation.
   - ❑ E. Launch the Startup Repair tool from the installation medium.

2. One of the Windows Vista computers experiences Internet Explorer 7 application freezes and you suspect either incompatible browser add-ons or extensions, or perhaps malicious software is the cause. How do you best determine if this is the case?

   Select the best answer.

   - ❍ A. Start Internet Explorer Protected Mode.
   - ❍ B. Enable Internet Explorer Phishing Filter.
   - ❍ C. Start Internet Explorer (No add-ons) mode.
   - ❍ D. Enable Internet Explorer Enhanced Security Configuration mode.

3. A single Windows Vista computer is shared among a number of coworkers and administrative staff. All users may share folders but none may use another's resources. What are the best options for this scenario?

   Choose the best TWO answers.

   - ❑ A. Create a single user account for every employee and several administrator accounts.
   - ❑ B. Create separate user accounts for each employee and one administrator account.
   - ❑ C. Enable Printer sharing in the Networking and Sharing Center.
   - ❑ D. Enable Public folder sharing in the Networking and Sharing Center.
   - ❑ E. Enable Network discovery in the Networking and Sharing Center.

Chapter 3 Configuring Windows Security Settings Features

1. Your enterprise network environment runs standard user desktops that leverage delegated installation technologies like Group Policy Software Install. Application installers that require elevated privileges trigger elevation prompts. How might you turn these off?

   Select the best answer.

   - ❍ A. Open User Account Control and change Behavior of the elevation prompt for administrators to No prompt.
   - ❍ B. Open User Account Control and enable Run all users, including administrators, as standard users.
   - ❍ C. Open User Account Control and disable Elevate on application installs.
   - ❍ D. Open User Account Control and disable Validate signatures of executables that require elevation.

2. Your network enforces account lockouts that trigger after a predetermined number of failed login attempts and you want to ensure service to legitimate account holders. This might be achievable by specifying some amount of time that failed login attempts are tracked. How might you control this aspect?

   Select the best answer.

   - ❍ A. Enable a Local Security Policy and establish an Account Lockout Policy threshold.
   - ❍ B. Enable a Local Security Policy and establish an Account Lockout Policy for Reset account lockout after.
   - ❍ C. Enable a Local Security Policy and establish an Account Lockout Policy duration.
   - ❍ D. Enable a Local Security Policy and establish an Account Lockout Policy restart.

3. You must configure applications to operate with standard user privileges, by default, and possibly alert the user when an application is attempting to operate with administrator privileges. How can you enforce this default behavior?

   Choose the best TWO answers.

   - ❑ A. Use Standard User privileges.
   - ❑ B. Use Windows Service Hardening.
   - ❑ C. Use Admin Approval Mode.
   - ❑ D. Use Network Access Protection.
   - ❑ E. Use Parental Controls.

4. Your organizational network security policy mandates public key infrastructure signature checks on any interactive process or binaries that request elevation of privilege. This is controlled through local certificates. How might you configure Windows Vista to enforce this behavior?

   Select the best answer.

   - ❍ A. Open User Account Control and enable Elevate on application installs.
   - ❍ B. Open User Account Control and enable Validate signatures of executables that require elevation.
   - ❍ C. Open User Account Control and enable Elevate on application installs.
   - ❍ D. Open Advanced System Settings and enable Data Execution Prevention.

Chapter 4 Configuring Network Connectivity

1. As an administrator, your daily routine is greatly simplified where configuration settings are set once and replicated or reproducible elsewhere. Windows Vista supports a few ways to transfer network settings among computers. How might you achieve this goal?

   Choose the best TWO answers.

   - ❑ A. Save network settings to a USB drive and apply elsewhere.
   - ❑ B. Have systems automatically download Wireless Network Group Policy extensions at startup.
   - ❑ C. Use File Sharing to distribute copies of network settings to all clients.
   - ❑ D. Use Network and Sharing Center to dial-in remote configurations.
   - ❑ E. Use Dial-up and Internet Connections to propagate remote configurations.

2. Computers on a Windows Vista network fail to resolve Universal Naming Convention (UNC) paths among local computers. Usually, this occurs as the result of incompatible or incorrectly configured network settings or problems with Windows Internet Naming Service (WINS) or DNS. What action might you perform to resolve this issue?

   Select the best answer.

   - ❍ A. Disable Windows Firewall.
   - ❍ B. Add UDP port 137 to the Windows Firewall exceptions list.
   - ❍ C. Disable Windows Defender.
   - ❍ D. Add UDP and TCP port 53 to the Windows Firewall exceptions list.

3. The built-in Administrator account is disabled by default in Windows Vista, which means it cannot log into safe mode. A specially-configured user account can log in to create a local administrator account where one does not already exist. What action should you perform to accomplish this goal?

   Select the best answer.

   - ❍ A. Enrollment of a specified user account as Domain Admins group.
   - ❍ B. Configure a specified account's user profile.
   - ❍ C. Enrollment of a specified user account in Group Policy.
   - ❍ D. Configure a specified account's network profile.

Chapter 5 Configuring Applications Included with Windows Vista

1. One of your standard users reports slow performance and power consumption penalties caused by Windows Aero activity on the desktop, which you promptly confirm. Which action do you take to disable Windows Aero?

   Choose the best TWO answers.

   - ❑ A. Change the color scheme to either Windows Vista Basic or Windows Vista Standard.
   - ❑ B. Open Window Color and Appearance and uncheck Enable transparency.
   - ❑ C. Open Window Color and Appearance and change the theme.
   - ❑ D. Run Windows Experience Index, select Adjust visual effects and disable Windows Aero.
   - ❑ E. Open Window Color and Appearance and lower the color intensity.

2. Your users often receive email in non-native languages with unusual character sets. You would like to restrict communications to a specific language or set of languages. What should you configure to achieve this?

   Select the best answer.

   - ❍ A. Configure the Windows Mail settings for Junk E-mail Options entries.
   - ❍ B. Configure Windows Mail junk e-mail options International language settings for Blocked Encodings List entries.
   - ❍ C. Configure Windows Mail settings for Blocked Top-Level Domain List entries.
   - ❍ D. Configure Windows Mail settings for Phishing Filter entries.

3. Photo or image editing users of Windows Vista often tag and rate pictures and include custom metadata to describe or define their images and video collections. Some users may even need basic features like adjusting, cropping and resizing images. What application should you configure for their use?

   Select the best answer.

   - ❍ A. Setup Windows Movie Maker and create a media directory.
   - ❍ B. Use Windows Snipping Tool and use a default media repository.
   - ❍ C. Use Windows Sideshow and create a media directory.
   - ❍ D. Use Windows Photo Gallery and use a default media folder.

4. Some users have difficulty properly handling unverified messages delivered to their Windows Mail inbox. Unsuspecting attachments often result in malware outbreaks that are otherwise easily avoidable. What action should you take to prevent this situation?

   Select the best answer.

   - ❍ A. Configure Windows Mail settings for Phishing Filter properties.
   - ❍ B. Configure Windows Mail to block potentially problematic attachments.
   - ❍ C. Configure Windows Mail to block content based country of origin.
   - ❍ D. Configure Windows Mail to block content based on language preferences.

Chapter 6 Maintaining and Optimizing Systems that Run Windows Vista

1. Windows Vista includes a basic file backup feature that copies only personal user files and data, not the entire operating system and its supportive applications. This native application can also schedule automated backups to remote network locations. What is this application called?

   Select the best answer.

   - ❍ A. Complete PC Backup.
   - ❍ B. Shadow Copy.
   - ❍ C. Automatic Backup.
   - ❍ D. System Restore.

2. Windows Vista includes a recovery plan to restore a corrupted computer to a workable state. Configuration changes, incompatible applications or unchecked malware may be a few of the causes that corrupt the computer. What would you use to return a corrupted system to normalcy?

   Select the best answer.

   - ❍ A. Shadow Copy.
   - ❍ B. Complete PC Backup.
   - ❍ C. Automatic Backup.
   - ❍ D. System Restore.

3. A Windows Vista computer is completely corrupt and none of the built-in operating system recovery and restoration options are directly available. You need to wipe out the entire setup in its current, non-functional state and restore from a backup copy instead. What option do you have for this task?

   Select the best answer.

   - ❍ A. Boot from the install DVD and invoke Startup Repair.
   - ❍ B. Boot from the install DVD and invoke System Restore.
   - ❍ C. Boot from the install DVD and invoke Windows Complete PC Restore.
   - ❍ D. Boot from the hard drive and select Last Known Good Configuration.

4. A computer suddenly fails to boot into the Windows Vista desktop and you want to try one final recovery procedure. No backups have been made, the installation media is not always accessible and only the boot-time options are consistently at your disposal. What option do you have for this task?

   Select the best answer.

   - ❍ A. Boot from the install DVD and choose Repair your computer.
   - ❍ B. Boot from the drive and choose Last Known Good Configuration.
   - ❍ C. Boot from the install DVD and invoke Windows Complete PC Restore.
   - ❍ D. Boot from the drive and run System Restore.

Chapter 7 Configuring and Troubleshooting Mobile Computing

1. There are other methods of conserving notebook power, apart from conservative power profiles and settings. Special considerations can be made, particularly for notebooks used during presentations. What action should you take?
Select the best answer.

   - ❍ A. Connect an external monitor and configure Mirrored mode in Windows Mobility Center.
   - ❍ B. Connect an external monitor and configure External display only in Windows Mobility Center.
   - ❍ C. Connect an external monitor and configure Extended mode in Windows Mobility Center.
   - ❍ D. Connect an external monitor configure Duplicate mode in Windows Mobility Center.

2. A Windows Vista notebook has become unstable following a recent hardware upgrade. You suspect an internal mini-PCI wireless card is the culprit, which is unnecessary for normal operation of the computer. What corrective action should you take? Each answer represents a complete solution.

   Choose the best TWO answers.

   - ❑ A. Open the Device Manager, select the troubled device properties and choose Update Driver.
   - ❑ B. Open the Device Manager, select the troubled device properties and choose Roll Back Driver.
   - ❑ C. Open the Device Manager, select the troubled device properties and choose Disable and leave the device attached.
   - ❑ D. Open the Device Manager, select the troubled device properties and choose Uninstall and detach the device.
   - ❑ E. Open the Device Manager, select the troubled device properties and choose Update Driver.

3. A sales consultant would like to make his sales data sharable offsite to third-party interests and other authorized personnel. His data does not require complex security, but does need basic encryption on specific sales data. What action do you take?

   Select the best answer.

   - ❍ A. Set up BitLocker Drive Encryption for sensitive data.
   - ❍ B. Set up Encrypted File System for sensitive data.
   - ❍ C. Set the Hidden attribute for sensitive data.
   - ❍ D. Set the Read-only attribute for sensitive data.

Answers and Explanations

Chapter 1

1. Answer: B

Explanation A. Incorrect. This evaluator identifies issues related to legacy application components no longer used by the Windows Vista operating system.

Explanation B. Correct. This application examines computers to identify installed applications and system information.

Explanation C. Incorrect. This analysis tool determines possible issues for applications running under standard user credentials in Windows Vista.

Explanation D. Incorrect. This analysis tool automates application installations and monitors actions taken by each installer to detect potential issues.

2. Answers: A, D

Explanation A. Correct. This is a bootable tool that provides features for installation, troubleshooting and recovery.

Explanation B. Incorrect. This tool prepares an installation for duplication, audit or delivery, and deployment offsite.

Explanation C. Incorrect. This is a command-line tool that enables the capture, modification and application of file-based images for rapid deployment.

Explanation D. Correct. This integrated feature is a complete diagnostic and recovery tool and a platform for custom recovery image construction.

Explanation E. Incorrect. This tool in itself will not help you identify the source of a problem, but it will help you make any necessary changes to a boot configuration-related issue.

3. Answer: B

Explanation A. Incorrect. This application examines computer hardware and software components to determine the best upgrade path to the Windows Vista family of operating systems.

Explanation B. Correct. This feature is available in the Vista control panel under System and Maintenance.

Explanation C. Incorrect. This is the built-in maintenance utility to keep Windows computers up to date with the latest fixes, patches and updates.

Explanation D. Incorrect. This is not official terminology in the Microsoft realm; however, Microsoft Updates do occur online.

4. Answer: B

Explanation A. Incorrect. This action may restore connectivity, but will not necessarily enumerate the layered network service providers.

Explanation B. Correct. This is an automatic IPv4 address assigned to a computer with no current network visibility.

Explanation C. Incorrect. This will only help identify any hardware (and possibly software) issues, but will not identify layered service providers.

Explanation D. Incorrect. The Internet Service Provider is only responsible for inter-network connectivity issues between your network and theirs, and will not be informed about your local computer settings.

Chapter 2

1. Answers: B, D

Explanation A. Incorrect. This may not actually produce a workable operating system, either. Of the options offered, it is not the best solution for this scenario.

Explanation B. Correct. Converting the partition is one step in a two step process towards correcting this problem.

Explanation C. Incorrect. This will only serve to further corrupt the operating system installation.

Explanation D. Correct. Formatting and repartitioning the drive is one step in a two step process towards correcting this problem.

Explanation E. Incorrect. This will serve only to further corrupt the backup image.

2. Answer: C

Explanation A. Incorrect. Protected Mode provides a layered defense security feature that prevents Internet Explorer from enacting lower-integrity applications, user-specific configuration changes and from attaching to higher privilege processes.

Explanation B. Incorrect. The Phishing Filter attempts to prevent untrusted, third-party sites from fooling users into revealing personal account data or confidential data.

Explanation C. Correct. Internet Explorer (No Add-ons) mode prevents add-ons, extensions and potentially malicious third-party software from loading at run-time.

Explanation D. Incorrect. This feature sets a high security level for the Internet zone to restrict activity only to trusted Web sites.

3. Answers: B, D

Explanation A. Incorrect. Ideally there should be only a single local administrator account and several individual user accounts, including those tasked with administrative duties.

Explanation B. Correct. Ideally there should be only one administrator account and several non-administrator accounts that include users capable of administrative tasks.

Explanation C. Incorrect. This network property is applicable to multiple computers sharing a single network printer, not multiple users sharing a single computer.

Explanation D. Correct. This will make shared resources in select folders visible and accessible to multiple users on the same computer.

Explanation E. Incorrect. This will enable other computers on the network to see and be seen computer, which is not the same as sharing.

Chapter 3

1. Answer: C

Explanation A. Incorrect. This option allows the Consent Admin account to perform operations that require elevated privileges without consent or credentials.

Explanation B. Incorrect. This controls operations that require privilege elevation through a series of permit or deny dialogs.

Explanation C. Correct. This will disable the unnecessary installation detection routine.

Explanation D. Incorrect. This policy enforces PKI signature checks against any interactive application that requests privilege elevation.

2. Answer: B

Explanation A. Incorrect. This feature enforces the total number of failed logon attempts permitted before account lockout triggers.

Explanation B. Correct. This setting specifies the amount of time that must elapse after a failed login attempt before the failed attempt counter is reset to 0.

Explanation C. Incorrect. The lockout duration will allow users to log in after some designated period of time following the maximum number of retries.

Explanation D. Incorrect. The current account lockout policy does not specify any such feature.

3. Answers: A, C

Explanation A. Correct. This is, by far, the best method to separate potentially bad software, or malware, from accessing elevated administrator privileges, thus preventing the large scope of damage that such applications may cause.

Explanation B. Incorrect. This security measure restricts critical Windows services from performing abnormal activities on the file system, registry, network or other resources.

Explanation C. Correct. This mode reduces the threat for some types of malware attacks, but does not provide the same level of protection as a standard user account, nor will it guarantee the software will execute without malicious action once privileges are elevated.

Explanation D. Incorrect. This security measure enforces current security updates, anti-virus signatures and other computer health requirements before accepting a remote client connection.

Explanation E. Incorrect. This will serve only to create usage monitoring reports for administrative accounting purposes.

4. Answer: B

Explanation A. Incorrect. This feature triggers elevation prompts on application installers that require administrative privileges.

Explanation B. Correct. This function ensures that only signed, verified binaries may execute on the system.

Explanation C. Incorrect. This triggers heuristic detection of application package installers that will invoke the elevation prompt on the desktop.

Explanation D. Incorrect. This security feature helps prevent damage from viruses and other security threats by monitoring application utilization of system memory.

Chapter 4

1. Answers: A, B

Explanation A. Correct. Windows includes a method of distributing common network settings among many computers using portable storage devices, such as USB drives.

Explanation B. Correct. Upon joining a domain or starting up, Windows Vista computers will acquire these settings and immediately apply them.

Explanation C. Incorrect. This will not effectively or practically resolve the issue of mass configuring Windows network settings.

Explanation D. Incorrect. This provides a per-computer means of configuring network settings; it is not effective in a large scale network environment.

Explanation E. Incorrect. This Windows XP wizard is incapable of directly sharing network settings.

2. Answer: B

Explanation A. Incorrect. Especially well-protected computers should remain behind their firewalls; there is a simple, more practical means of permitting traffic through an active one.

Explanation B. Correct. UDP port 137 is the port where WINS operates to internally map Windows host IP addresses to a private naming convention.

Explanation C. Incorrect. This application feature defends against a host of remote malware attacks but does not interfere with the operation of UNC path resolution.

Explanation D. Incorrect. This is the port where DNS operates to resolve IP addresses to human-readable host names.

3. Answer: A

Explanation A. Correct. Members of this group may administratively override local settings, particularly where no local administrator yet exists.

Explanation B. Incorrect. This method comes after some form of administrative control is established and must therefore follow some other action.

Explanation C. Incorrect. A specific group policy does not properly address the problem of needing administrative controls to override local administrative settings.

Explanation D. Incorrect. A specially configured network profile will not permit administrative override.

Chapter 5

1. Answers: A, C

Explanation A. Correct. This is one way to disable Windows Aero on the desktop.

Explanation B. Incorrect. Window transparency is a property of Windows Aero and disabling this feature will not deactivate Windows Aero.

Explanation C. Correct. This is one way to disable Windows Aero on the desktop.

Explanation D. Incorrect. Currently there is no such option path, and Windows Experience Index does not directly involve Windows Aero.

Explanation E. Incorrect. This will only darken or lighten the desktop color scheme accordingly.

2. Answer: B

Explanation A. Incorrect. This will not specifically address the issue of invalid or non-native character sets and foreign language content.

Explanation B. Correct. This will restrict messages to only a select group and eliminate the possibility for character set manipulation to the system.

Explanation C. Incorrect. This action will not directly prevent specific, non-native character sets from reaching the intended target.

Explanation D. Incorrect. This feature, which is enabled by default, will not necessarily restrict email content based on language restrictions.

3. Answer: D

Explanation A. Incorrect. This application is used to import, edit, manage and share digital video content.

Explanation B. Incorrect. This tool can be used to quickly create snapshots of the active desktop.

Explanation C. Incorrect. This will produce output for select applications on an auxiliary display.

Explanation D. Correct. This application can perform some image editing tasks and also handle motion picture footage for video editing assignments.

4. Answer: B

Explanation A. Incorrect. This default feature will prevent attempts to acquire personally identifiable information from end-users.

Explanation B. Correct. This will prevent end-users from opening unverified message attachments and thereby contaminating the computer or network with malware.

Explanation C. Incorrect. This will only deny messages originating from specific locations, not the problematic attachments.

Explanation D. Incorrect. This will only reject messages based on native language preferences.

Chapter 6

1. Answer: C

Explanation A. Incorrect. This application creates a workable image-based copy of the entire operating system, including all supportive and accessory applications.

Explanation B. Incorrect. This feature creates read-only, incremental backups for a given file, permitting a user or administrator to recover a deleted file or roll back to an earlier state for the incorrectly restored version.

Explanation C. Correct. This application creates a limited, scheduled automatic backup of personal user files and data, which can be delivered to an external or secondary disk, recordable CD or DVD media, or a remote network target.

Explanation D. Incorrect. This feature enables an administrator to restore a computer to some earlier known good state, including the removal of recently installed applications or configuration changes, without losing data.

2. Answer: D

Explanation A. Incorrect. This feature creates read-only, incremental backups for a given file, permitting a user or administrator to recover a deleted file roll back to an earlier state for the incorrectly restored version.

Explanation B. Incorrect. This application creates a workable, image-based copy of the entire operating system, including all supportive and accessory applications.

Explanation C. Incorrect. This application creates a limited, scheduled automatic backup of personal user files and data, which can be delivered to an external or secondary disk, recordable CD or DVD media, or a remote network target.

Explanation D. Correct. This feature enables an administrator to restore a computer to some earlier known good state, including the removal of recently installed applications or configuration changes, without losing data.

3. Answer: C

Explanation A. Incorrect. This function checks installations for startup problems and provides a diagnostics report.

Explanation B. Incorrect. This function restores automatically, regularly backed-up system files.

Explanation C. Correct. This function will display a list of backup target options including date, time and location of the backup file.

Explanation D. Incorrect. This function is used to irreversibly reset a computer to a former working state when recovery or restore options fail; it will not solve the problem of a completely corrupted installation.

4. Answer: B

Explanation A. Incorrect. This function of the installation DVD provides several options for repairing, recovering or restoring a corrupted system.

Explanation B. Correct. This boot-time option is used for an irreversible, one-time-only change back to a formerly working state.

Explanation C. Incorrect. This function will provide a list of backup targets where they exist.

Explanation D. Incorrect. This function requires the ability to use the desktop to restore critical system files.

Chapter 7

1. Answer: B

Explanation A. Incorrect. This is enabled by default and reproduces the configured desktop on every connected monitor.

Explanation B. Correct. This feature turns off the notebook display in favor of an external desktop monitor, thus conserving battery power.

Explanation C. Incorrect. This feature expands the current desktop to encompass one or more monitors, thus extending the usable workspace.

Explanation D. Incorrect. This is not a feature included with Windows Vista.

2. Answers: C, D

Explanation A. Incorrect. An explicit driver update may not correct the problem and leave the system unusable.

Explanation B. Incorrect. Since no previous driver is present, no roll back can occur.

Explanation C. Correct. This is one way to properly deactivate the device and maintain a usable system.

Explanation D. Correct. This is one way to effectively disable the device and leave the system usable.

Explanation E. Incorrect. The device has not yet become operational for a driver issue to be present.

3. Answer: B

Explanation A. Incorrect. This configuration will perform an all-encompassing encryption of critical system files and personal user information.

Explanation B. Correct. This will serve to encrypt only selected files and folders, which is all that is necessary for this purpose.

Explanation C. Incorrect. This will only hide the file from plain view of most applications unless configured to view such files.

Explanation D. Incorrect. This will only make files unable to be modified by editing applications.