

Microsoft

# Windows Vista

Enterprise Support (70-622)



**Smarter  
Training**

This LearnSmart exam manual presents all the skills and tools required to successfully complete the Windows Vista Enterprise Support exam (70-622). By studying this manual, you will become familiar with an array of exam-related objectives, including:

- Deploying Windows Vista
- Managing Windows Vista Security
- Configuring and Troubleshooting Networking
- Supporting and Maintaining Desktop Applications
- And more!

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

# Supporting and Troubleshooting Applications on a Microsoft Windows Vista Client for Enterprise Support Technicians (70-622) LearnSmart Exam Manual

Copyright © 2011 by PrepLogic, LLC  
Product ID: 11095  
Production Date: July 11, 2011

All rights reserved. No part of this document shall be stored in a retrieval system or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without written permission from the publisher. No patent liability is assumed with respect to the use of the information contained herein.

## 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.

LearnSmart Cloud Classroom, LearnSmart Video Training, Printables, Lecture Series, Quiz Me Series, Awdeeo, PrepLogic and other PrepLogic logos are trademarks or registered trademarks of PrepLogic, LLC. All other trademarks not owned by PrepLogic that appear in the software or on the Web Site (s) are the property of their respective owners.

## Volume, Corporate, and Educational Sales

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

**1-800-418-6789**  
[solutions@learnsmartsystems.com](mailto:solutions@learnsmartsystems.com)

## International Contact Information

**International:** +1 (813) 769-0920

**United Kingdom:** (0) 20 8816 8036

**Table of Contents****Supporting and Troubleshooting Applications on a Microsoft**

<b>Windows Vista Client for Enterprise Support Technicians (70-622)</b> .....	<b>2</b>
Warning and Disclaimer .....	2
Volume, Corporate, and Educational Sales .....	2
Abstract .....	9
What to Know .....	9
Tips .....	9
<b>Basic Installation</b> .....	<b>10</b>
Minimum Hardware Requirements .....	10
<i>Preparing the hardware</i> .....	11
Compatibility tool .....	11
Windows Vista Hardware assessment .....	11
Additional preparation steps .....	12
Upgrading .....	12
<i>Recommended upgrade path:</i> .....	12
<i>File systems</i> .....	13
<b>Deployment</b> .....	<b>13</b>
<i>Nuts and bolts of deployment</i> .....	14
Business Desktop Deployment (BDD) 2.x .....	14
Windows PE (Pre-installation Environment) .....	15
Answer Files .....	17
Light-touch and Zero-touch .....	17
<i>Summary of Deployment Tools and Techniques</i> .....	17
<i>User State Migration Tools</i> .....	18
Migration with Windows Easy Transfer .....	19
Migration with USMT .....	19
<i>Windows Deployment Services (WDS)</i> .....	21
Selecting the appropriate deployment method .....	22
Post Installation checks .....	22
Windows Activation .....	22
Troubleshooting deployment problems .....	23
<b>Applications</b> .....	<b>23</b>
Common issues with applications .....	23

<i>Tools to ease compatibility problems</i> .....	24
Windows Experience .....	25
<i>Problem Reports and Solutions</i> .....	26
<i>Compatibility mode</i> .....	27
<i>Program Compatibility Assistant</i> .....	28
<i>Program Compatibility Wizard</i> .....	29
<i>Application Compatibility Toolkit (ACT) 5.0</i> .....	29
<i>File and Registry Virtualization</i> .....	29
Troubleshooting Applications .....	30
Windows Resource Protection (WRP) .....	31
<b>Active Directory and Group Policy</b> .....	<b>31</b>
Active Directory Structure .....	31
<i>Domains and Organizational Units</i> .....	32
Group Policy .....	32
<i>Types of Group Policies</i> .....	32
<i>Group Policy Application Rules</i> .....	33
Default Application Order .....	33
<i>Group Policy tools</i> .....	33
<i>Slow links</i> .....	33
Local Group Policy .....	34
Vista group Policy .....	35
<i>Security Policy</i> .....	35
<i>Main Security Policy Settings</i> .....	36
<b>Vista Security</b> .....	<b>37</b>
Security background .....	37
OS security enhancements .....	38
<i>NTFS settings</i> .....	38
<i>User Account Control (UAC)</i> .....	39
Access Tokens .....	39
Split tokens .....	39
Tasks which only require standard user privileges .....	40
Tasks which need administrative privileges to run .....	41
Gaining administrative privileges .....	41
Controlling UAC .....	43

---

<i>Windows Integrity Control (WIC)</i> .....	45
Integrity levels .....	46
Internet Explorer 7 (IE7) Protected mode .....	47
<i>Windows Resource Protection (WRP)</i> .....	48
Service management .....	48
Drivers .....	49
<i>Managing Services</i> .....	50
General tab .....	51
Log On tab .....	52
Recovery tab .....	52
Dependencies tab .....	53
Vista service security enhancements .....	54
Using a less authoritative set of service credentials .....	54
Session separation .....	54
Service Isolation .....	55
<i>USB management</i> .....	55
File Security .....	56
<i>Simple File Sharing</i> .....	57
<i>Public folder</i> .....	57
<i>Traditional Access Model</i> .....	58
Share level permissions .....	59
NTFS permissions .....	60
Rules .....	60
<i>Contrasting permissions</i> .....	61
<i>Disks and File Systems</i> .....	61
Dynamic and Basic Disks .....	61
File Systems .....	61
<i>Auditing</i> .....	62
Windows Firewall .....	64
Rules .....	64
<i>Firewall Management tools</i> .....	65
Windows Firewall in Control Panel .....	65
<i>Windows Firewall with Advanced Security</i> .....	67
Windows Defender .....	68

<i>Software Explorer</i> .....	70
Internet Explorer (IE) .....	71
<i>Tools menu</i> .....	71
Pop-ups .....	71
Phishing .....	71
<i>Internet Options</i> .....	72
Security tab .....	72
Privacy options .....	74
SSL and TLS .....	75
<b>Monitoring Windows Vista .....</b>	<b>76</b>
Reliability and Performance Monitor .....	77
<i>Performance Monitor</i> .....	77
<i>Reliability Monitor</i> .....	78
<i>Data collector sets</i> .....	79
<i>Reports</i> .....	79
Event Logs .....	80
<i>Types of Event Logs</i> .....	81
Windows Logs .....	81
Applications and Services Logs .....	81
<i>Managing Event logs</i> .....	82
Retention Policy .....	82
<i>Event Subscriptions</i> .....	83
To configure computers for Event Forwarding .....	83
To configure subscriptions .....	83
Task Scheduler .....	84
<i>Schedules</i> .....	85
BitLocker .....	85
Additional security .....	86
Encryption system .....	87
Active Directory and BitLocker .....	89
Supporting BitLocker on systems without a TPM .....	89
<i>Boot Process Integrity Check</i> .....	90
Implementing BitLocker .....	92
<i>Hardware requirements</i> .....	92

Key storage .....	92
Disk configuration .....	92
<i>Managing</i> .....	92
<b>Vista Networking .....</b>	<b>93</b>
<i>GUI enhancements</i> .....	93
<i>Network Protocols added</i> .....	93
<i>Network Protocols removed</i> .....	94
<i>Other features</i> .....	94
Workgroups and Domains .....	94
<i>Authentication problems</i> .....	95
Basic TCP/IP .....	96
<i>IP Version 6</i> .....	96
<i>Network Services</i> .....	96
DNS .....	96
WINS .....	96
DHCP .....	96
NAT .....	97
Proxying .....	97
Firewall .....	97
<i>Testing and Troubleshooting IP</i> .....	97
IPCONFIG .....	97
Ping .....	98
To test a TCP/IP configuration by using the ping command .....	99
Tracert .....	99
PathPing .....	99
NetStat .....	99
NBTStat .....	100
Network and Sharing Center .....	100
<i>Network Profile</i> .....	101
Options available on each profile .....	102
Profile selection .....	102
<i>Network Awareness</i> .....	103
<i>Network Setup Wizard</i> .....	103
<i>Network Diagnostic Framework (NDF)</i> .....	104

---

Manually running NDF.....	105
<i>Network Map</i> .....	106
<i>Network Explorer</i> .....	106
Wireless Networking.....	107
<i>Wireless terminology</i> .....	107
<i>Configuring wireless connections</i> .....	108
Adding a wireless network.....	109
Remote Access .....	109
<i>Creating connections</i> .....	110
<i>Authentication protocols</i> .....	111
<i>VPN protocols supported by Windows Vista</i> .....	112
<i>Internet Connection Sharing (ICS)</i> .....	112
<b>Windows Update</b> .....	<b>113</b>
<i>Troubleshooting</i> .....	114
<b>Practice Questions</b> .....	<b>115</b>
<b>Answers and Explanations</b> .....	<b>123</b>



## Abstract

This Exam Manual, for the 70-622 exam, has been written to cover exam objectives as published by Microsoft. Rather than covering each objective individually, we have grouped common concepts together so that topics are only covered once.

Microsoft is notorious for including questions outside an exam's stated syllabus, so we have used our experience to include brief descriptions of topics which you may encounter in the exam, even though, officially, this should not happen. With the release of Windows Vista, Microsoft drastically changed the entire operating system structure. The Graphical User Interface (GUI), functionality, and the core code have all seen drastic revision. We have attempted to write the notes such that they will be easily understandable if you are familiar with Windows XP or if you have little experience with Windows Vista - we hope you find this manual useful and that it is a worthwhile tool in your exam preparation.

## What to Know

Microsoft's exam 70-622 Supporting and Troubleshooting Applications on a Microsoft Windows Vista Client for Enterprise Support Technicians is the single exam required to become a Microsoft Certified Information Technology Professional (MCITP) on Enterprise Support Technology for the Microsoft Windows Vista platform. The exam is multiple choice, in the realm of fifty questions, and is considered to be of mid-level difficulty.

The Domains covered by this exam include:

- Deploying Windows Vista
- Managing Windows Vista Security
- Managing and Maintaining Systems That Run Windows Vista
- Configuring and Troubleshooting Networking
- Supporting and Maintaining Desktop Applications

## Tips

Allocate plenty of study time and dedicate at least an hour a night, preferably several hours, to getting hands on experience with Windows Vista administration before your exam. Familiarize yourself with the logistics of the exam as well as how Microsoft's Windows Vista can be used in practical application. The PrepLogic Practice Exams provide a similar test environment to that of the Microsoft exam format, and can serve as an invaluable preparatory tool.

## Basic Installation

A basic installation is a fresh install performed off the Windows Vista DVD.

### Minimum Hardware Requirements

<b>CPU</b>	32 or 64 bit 800Mhz
<b>RAM</b>	512MB
<b>Disk</b>	20GB partition with at least 15GB free
<b>Video</b>	800 x 600 VGA
<b>Aero Interface</b>	GPU with support for DirectX 9 graphics with: WDDM Driver 128 MB of graphics memory (minimum) Pixel Shader 2.0 in hardware 32 bits per pixel

**Recommended specifications are as follows:**

- **CPU:** 1 GHz or faster
- **RAM:** 1GB
- **HD Space:** 40GB

## Preparing the hardware

You need to ensure your computer's hardware is compatible with Windows Vista.

### Compatibility tool

When the Vista DVD starts, you will be given the option to start the installation immediately, or to run the **Compatibility Tool** (requires a connection to the Internet):



The Vista DVD opening screen showing the transfer and checking options

**Tip:** The **Hardware Compatibility List (HCL)** has been replaced by the **Windows Marketplace** website.

### Windows Vista Hardware assessment

The **Windows Vista Hardware Assessment** is a utility which locates computers across a network then performs a detailed inventory of the computers' hardware specifications using **Windows Management Instrumentation (WMI)**.

The utility uses the gathered information to generate a report detailing every computer's readiness for a Windows Vista installation, where to find Vista-compatible drivers for each computer's various devices, and provide recommendations for hardware upgrades where appropriate.

The Windows Vista Hardware Assessment tool does not require the deployment of agent software on the computers being inventoried and assessed. It provides a secure, quick and easy way to determine which networked computers are Windows Vista ready.

### Additional preparation steps

- Switch off BIOS virus detection
- Switch on BIOS power management
- Switch on BIOS PnP

## Upgrading

Microsoft recommends performing a fresh install of the Windows Vista operating system, then transferring the User's settings to the new install, using either **Windows Easy Transfer** (one offs) or the **User State Migration Tool** for larger migrations.

### Recommended upgrade path:

Existing Platform	Vista Business/Vista Enterprise	Vista Ultimate
XP Professional	✓	✓
XP Home	✓	✓
XP Media Center	×	✓
XP Tablet	✓	✓
XP Professional 64	×	✓

You cannot upgrade from Windows 2000 or Windows 9.x.

You can upgrade from Windows XP (both 32 bit and 64 bit versions).

When upgrading, make sure that both the hardware and the software are Vista compatible.

## File systems

When dual booting, consideration must be given to the C:\ drive, which is the **active partition** used by the BIOS. Every OS installed on a computer needs to be able to read C:\ as that is where the start-up files will reside. When dual booting, you will need to select a file system for C:\ that is compatible with all OSs installed. For the exam, the following table will be sufficient:

File System	NTFS	FAT16	FAT32
<b>Operating System</b>	NT4SP4	DOS	Windows 95 (later)
	Windows 2000	Windows 9x	Windows 98/Me
	Windows XP	NT4SP4	Windows 2000
	Windows Vista	Windows 2000	Windows XP
		Windows XP	Windows Vista
		Windows Vista	

Microsoft recommends using NTFS first, followed by FAT32, then FAT16. Remember that NT4 cannot use FAT32 and Windows9x (Windows95, Windows 98 and Windows Me) cannot use NTFS.

Do not use dynamic disks if dual booting.

## Deployment

Deployment is the process of installing multiple copies of Windows Vista automatically, usually over several computers on a network. The automation replaces the process of manually answering questions asked by the setup process. Compared to the manual installation system, deployment methods frequently allow you more flexibility in how Windows Vista is installed. The manual method of installation allows you to make the following choices:

- The size of the disk partitions
- The name of the computer
- Standard or customized networking

If you require any additional configuration, you need to deploy Windows Vista.

Deployment also gives you the opportunity to install applications after the operating system completes its installation. This is an alternative to Group Policy deployment, or Microsoft Systems Management Server (SMS).

## Nuts and bolts of deployment

The following are key concepts to understand when answering exam questions on deployment:

### Business Desktop Deployment (BDD) 2.x

BDD is a suite of tools that can be used to provide a deployment solution. For example, BDD provides a scripting tool to create scripts and a series of checklists so that you can plan your deployment. Additionally, you can use BDD to:

- Automate the creation and deployment of images
- Create an inventory of hardware and software
- Customize applications and package them for deployment
- Manage the automatic deployment system
- Secure the desktop configuration
- Test applications for compatibility problems and minimize the effect of this

BDD consists of the following tools:

Tool	function/use
<b>Deployment Workbench (BDDWorkbench)</b>	The framework/environment for running the other BDD configuration tools
<b>Windows Automated Installation Kit (Windows AIK)</b>	Consists of two tools: <ul style="list-style-type: none"> <li>• Windows System Image Manager (creates scripts)</li> <li>• Windows PE2 Kit (customizes Windows PE)</li> </ul>
<b>Pre-installation Environment 2.0</b>	Pre-installation environment
<b>User State Migration Tool (USMT)</b>	Tools to migrate the User State Data between a user's original computer and a new Vista machine
<b>Windows Deployment Services (WDS)</b>	The successor to Remote Installation Services (RIS), WDS allows the deployment of images to machines without any OS installed and without the use of Windows PE

**Windows PE (Pre-installation Environment)**

Windows PE is a complete “mini-OS,” which is network and Windows Vista aware. It is a small program (approx 250Mb) and can be installed on a USB memory stick or other device. Microsoft envisions Windows PE being used in the following situations.

- As a means to boot a target system to install an image
- As a diagnostic platform

In both cases you will need to boot Windows PE, there are a number of methods:

- Boot from the installation DVD
- Boot from a USB device onto which Windows PE has been installed (your PC must support booting from USB devices in the BIOS)

For deployment Windows PE provides the following command line tools:

Tool	function
<b>BCDEdit</b>	Editor for Boot Configuration Data (BCD), which controls which OS in a multiboot system will be the default. <b>Note:</b> BCD replaces Boot.ini
<b>Bootsect</b>	Resets the boot file pointer on the active partition. For Vista to boot, the BIOS needs to load BOOTMGR. Previous versions of Windows used NTLDR. <b>Note:</b> Bootsect replaces FixFAT and FixNTFS.
<b>Diskpart</b>	Command line disk partition tool.
<b>DrvLoad</b>	Installs additional drivers that requires INF files.
<b>Oscdimg</b>	Creates an ISO file of the PE environment. This can then be burned onto a CD to create a self booting disk.
<b>PEimg</b>	Makes changes to a PE image.
<b>Wpeinit</b>	Initializes Windows PE <b>Note:</b> replaces the Factory.exe -winpe command.
<b>ImageX</b>	Manages image file deployment.

### Windows Imaging Files (WIM)

A Windows Vista Image is held in a \*.WIM. The WIM file contains all necessary information for a proper Windows Vista installation. The new image format used by WIM has several advantages over previous systems:

Improvement	Caused by
<b>Fewer files</b>	<p>A WIM file may contain multiple (i.e., both 32 bit and 64 bit) images.</p> <p>Images are hardware independent.</p> <p>Images are independent of the disk structure.</p> <p>Applications can be included.</p>
<b>Efficient file size</b>	<p>WIM uses compression and in files holding multiple images, stores common files only once (this is known as <b>single instancing</b>).</p>
<b>Easier maintenance</b>	<p>Images can be updated (such as adding service packs or updates) without the need for a target machine.</p> <p>The image can be deployed without deleting the existing contents of the disk.</p> <p>Microsoft has provided an API for develop to manipulate image files.</p>

To create an image you perform the following steps:

- Configure the source computer by installing Windows Vista plus any applications you wish to include.
- Configure the security and other settings such as drivers and updates, as required.
- Create an image from the source.
- Install the image onto selected target computers.

You can create the image by booting Windows PE on the source computer, then running **ImageX**. The image can then be copied to a network share, as Windows PE is network capable. After this, the image can be copied to a bootable CD-ROM, or onto a USB storage device such as a memory stick. The image can then be accessed by booting Windows PE on the target machine connected to the image file.

The target hardware will need to meet the Windows Vista hardware specification in addition to having at least 15GB of free disk space.

If using removable media to store the image, make sure you include the setup file, **Autounattend.xml** in the root. Setup searches all installable media for this file.

A typical image will be 2GB or greater. Therefore, when installing across the network, bandwidth must be capable of allowing for a file of this size. 100Mbps LANs and faster are suitable — deploying over a WAN is not recommended by Microsoft.



### Answer Files

An answer file is a script file used by the Windows Vista setup program to provide the information that the user normally provides during setup.

Windows Vista answer files are:

- XML files (instead of the text files used previously).
- Created with **Windows System Image Manager** (Windows SIM).

Previous versions of Windows used a combination of setup files and a UDF file. Windows Vista uses only the one setup file. This can be inserted on removable media using the default name **Autounattend.xml**.

### Light-touch and Zero-touch

There are a number of different techniques Microsoft provides to aid deployment. They can be grouped into two general classes:

<b>Light Touch Installation (LTI)</b>	<p>Some manual intervention is needed such as setting up a profile or installing applications.</p> <p>Light Touch installations can be initiated from:</p> <ul style="list-style-type: none"> <li>• The network</li> <li>• Bootable CD/DVD disks</li> <li>• Bootable USB storage devices (Memory Sticks, Hard drives etc)</li> </ul>
<b>Zero touch Installation (ZTI)</b>	<p>Deployment is 100% automated, including applications, if required. Mandatory unique labels, such as the computer name, are handled by the deployment process.</p> <p>Zero Touch requires Microsoft SMS 2003.</p>

## Summary of Deployment Tools and Techniques

Tool/Technique	Description
<b>Scripting</b>	Creating a script file to provide answers to the questions Windows Setup asks during installation and setup.
<b>Windows deployment Server</b>	An automated system which “downloads” an image to a computer.
<b>Image server</b>	A server hosting that builds images on a shared folder. These can be downloaded as required.
<b>Sysprep</b>	A method of creating a partial image, which is then transferred to the hard disks of new machines. When the machines first boot they complete the installation.

<b>SMS</b>	System Management Server. Complete automation of deployment.
<b>Windows Easy File Transfer</b>	The replacement for <b>Files and Settings Transfer Wizard</b> . A way of transferring user configuration settings and data from an old computer to a new model running Windows Vista. This is used in a “one off” scenario.
<b>USMT</b>	User State Migration Tool. This is a more complex, but more flexible, utility that performs the same task as Windows Easy Transfer. This is typically used in an enterprise rollout scenario.

Windows Easy File Transfer is most appropriate when you are migrating to one system, such as when a technician needs to replace an unstable computer with new hardware. Microsoft recommends using USMT as a departmental deployment tool, in which you roll out Windows Vista to many users at the same time.

## User State Migration Tools

The User State is the data and settings associated with one particular user. Most of the settings are located in the User's profile, which can be accessed by the following system variables:

%Userprofile%

%Homepath%

By default the User State consists of:

- Desktop
- My Documents
- Screen saver
- Mouse and Keyboard settings
- Internet Explorer settings
- Microsoft Office Settings

Settings related to hardware, such as drivers, dlls and executable files are not migrated. This includes the applications themselves. Passwords are also not migrated.

There are two tools included with Windows Vista that can be used to transfer the User State:

- Windows Easy Transfer
- User State Migration Tool (USMT)

Windows Easy File Transfer should be used for casual or “ad hoc” transference. Examples are:

- A user receives a new Vista system to replace their existing system
- A User's computer is exhibiting intermittent faults and needs replacing

USMT is a more detailed and sophisticated solution. USMT uses command line tools instead of the graphical Wizard used by Easy Transfer. Typically, USMT will be used during a mass migration, such as when a whole section or department is migrated to Windows Vista.

### Migration with Windows Easy Transfer

You can migrate settings from Windows XP and Windows Vista, plus some settings from Windows 2000 (not system or application settings); versions of Windows before this are not supported.

Data can be transferred by the following means:

- A special USB-USB cable
- Across the network
- On removable media such as a USB memory stick

### Migration with USMT

Windows Vista (both 32 and 64 bit) uses the User State Migration Tool 3.0. The previous version (2.0) will not work on Vista.

USMT 3.0 can be used to transfer files from any of the following versions of Windows:

- Windows 2000 Professional SP4
- Windows XP Home SP2
- Windows XP Professional SP2 (32 or 64 bit)
- Windows Vista (32 bit, 64 bit and Itanium-based Vista)

USMT uses two command line tools:

Tool	function
<b>ScanState</b>	Scans the original computer and saves the User State Data to a network share or other mass storage device.
<b>LoadState</b>	Retrieves the User State Data and loads it onto a new computer

By default USMT 3.0 transfers the following:

User Profile:	All Users profile
<ul style="list-style-type: none"> <li>• <b>My Documents</b></li> <li>• <b>My Video</b></li> <li>• <b>My Music</b></li> <li>• <b>My Pictures</b></li> <li>• <b>Desktop Settings</b></li> <li>• <b>Desktop files</b></li> <li>• <b>Start Menu</b></li> <li>• <b>Quick launch settings</b></li> <li>• <b>Favorites</b></li> </ul>	<ul style="list-style-type: none"> <li>• <b>Shared documents</b></li> <li>• <b>Shared Videos</b></li> <li>• <b>Shared Music</b></li> <li>• <b>Shared Desktop files</b></li> <li>• <b>Shared Pictures</b></li> <li>• <b>Shared Start Menu</b></li> <li>• <b>Shared Favorites</b></li> </ul>

By default, files with the following extensions are migrated:

accdb	dot	mpp	pp*	qel	scd	vsd	xl*
ch3	dqy	on*	pre	qph	sh3	wk*	
csv	iqy	oqy	pst	qsd	slk	wpd	
dif	mcw	or6	pub	rtf	txt	wq1	
doc	mdb	po*	qdf	rqy	vl*	wri	

USMT does not migrate drivers, so mobile and portable devices will not work on the new system until new drivers have been obtained and installed.

## Windows Deployment Services (WDS)

WDS is a service that holds images and then makes them available across the network, on request. Users are verified by Active Directory to ensure they have the requisite permission to install a given image.

WDS requires a network configured as follows:

- TCP/IP
- Active Directory
- DNS
- DHCP

The computer that will receive an image from the WDS server does not need to have an OS installed on it. The computer needs to be PXE 2.0 (Pre-execution Execution Environment version 2.0) compatible and configured in BIOS to boot from the network. PXE obtains an IP address, is contacted by the WDS server, and offers images to the user.

The Pre Execution Environment is a system whereby hardware can install an OS automatically. The PXE system requires an IP-based network with Active Directory, DNS, and DHCP configured. A RIS or WDS Server containing images will also be needed. On the client, PXE routines may be embedded in the system BIOS or the NIC firmware (in which case the BIOS needs to have the **Network Boot** option configured). As an alternative, PXE may be loaded from the server onto removable media. For more information refer to [this TechNet article](#).

As an alternative to PXE, the client can boot from Windows PE.

Installing an image using WDS

- Client boots and obtains an IP address from DHCP.
- The WDS Server recognizes this, contacts the client, and downloads the CIW (Client Installation Wizard).
- The CIW gathers the User ID and transmits it to the WDS server that checks it against AD to see which images (if any) the user has authority to install.
- A list of all permitted images is displayed on the client and the user chooses one.
- The hard disk is partitioned (into a single partition), formatted, and the image installed.
- The client boots, the image starts and uses **Unattend.xml** to configure itself.

## Selecting the appropriate deployment method

There are a number of ways to deploy Windows Vista. The chosen method should fit the circumstances to make the process as efficient as possible:

Deployment method	Situation
<b>Install off the Vista DVD</b>	Single basic installation typically a “one off” or where the network is un-sophisticated.
<b>Customized image on DVD</b>	Where there is a requirement for several identical builds, perhaps with applications; in this case the network connection may be poor or unreliable.
<b>Customized image from a network share</b>	Where there is a requirement for several identical builds, perhaps with applications. The network should be of good quality.  A Windows Deployment Server can be used to provide a choice of several versions.
<b>SMS</b>	While all the other methods automate deployment to some degree, only SMS allows a completely hands-free deployment. Use this method when you wish to manage deployment without any human intervention.

## Post Installation checks

Use the Windows Event logs to check for installation issues. The Network Diagnostics Framework (NDF) can be used to test for correct network connectivity. Use Disk Manager to check that all partitions have been created correctly.

### Windows Activation

After installation, Vista must be activated by or before a grace period consisting of 30 days. If not activated by that time, Vista will enter what Microsoft describes as Reduced Functionality Mode, with the following features disabled:

- Aero GUI
- Windows Defender
- Windows ReadyBoost

Additionally, a persistent “nag screen” is displayed, reminding you that your copy of Vista is not activated and that it must be activated before the user can take advantage of Vista’s full functionality.

Sites using volume licensing can make use of either Multiple Activation Key (MAK) in which Microsoft directly performs activation or Key Management Services (KMS) to perform the activation in-house.

## Troubleshooting deployment problems

1. Ensure that the installation media is fault free.
2. Use the **ImageX/verify** command to receive error messages during image deployment.
3. Use only compatible drivers, 3<sup>rd</sup> Party services and applications.
4. Loadstate and Scanstate (the USMT tools) can be configured to generate report logs. When using Loadstate make sure that there is enough room on the target partition to receive the data. If a path does not exist, Loadstate will restore the data to %SystemDrive%.
5. Chkdsk can be used to check for file system integrity.
6. If, after deployment, the computer refuses to boot and generates an “**Inaccessible boot devices**” error message, then you may have a faulty storage drive.

## Applications

### Common issues with applications

According to Microsoft, the most common issues running legacy applications on Windows Vista are:

Issue	ramifications
<b>System Permissions</b>	Many legacy applications require higher privileges to install and run than were granted to a standard user. Previously, users were made members of the Local Administrators or Power Users group. User Account Control (UAC) in Vista can stop this from being effective. UAC is a method of securing administrator accounts so that they cannot be inadvertently used by malware; UAC is described later in this manual.
<b>Access permission</b>	Applications need permission to write to disk folders and registry keys. For many years, Microsoft has been advising application writers not to use sensitive OS folders such as %systemroot%. Slowly, with each successive OS release, Microsoft has been tightening up the access control lists of sensitive folders and keys. Vista has made significant changes in this area. While this makes the whole system more immune to hacking, legacy applications which breach Microsoft's well established guidelines may fail to install or run correctly.

## Tools to ease compatibility problems

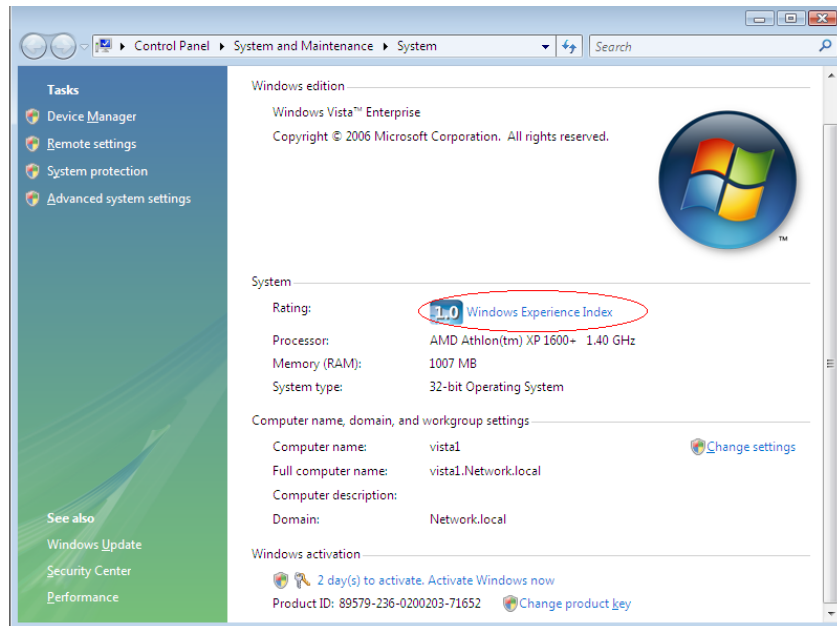
Microsoft has a number of tools to help you keep your old applications running on Vista:

Tool/technique	Provides
<b>File and Registry Virtualization</b>	Allows legacy applications to write to what they consider to be system areas without actually doing so.
<b>Standard User Analyser Tool</b>	Monitors an application which is running under Standard User credentials and suggests configuration changes to make it work properly.
<b>Application compatibility Toolkit</b>	A set of tools which can be used to analyze and fix legacy applications (including marking them as requiring elevated privileges to run).
<b>Microsoft Online Crash Analysis (MOCA)</b>	MOCA is designed to help cure BSOD problems. In Windows Vista, you have the option to connect to a Microsoft website and upload data. The crash settings are analyzed and a response with suggestions to fix the problem is provided.
<b>Windows Error Reporting (WER)</b>	When a program stops, Microsoft asks you to submit the details to them. They will work with interested parties to resolve the problem. WER can be configured to check for solutions periodically through the <b>Problem Reports and Solutions</b> console.
<b>Application Compatibility wizard</b>	This wizard is run from within the OS and may be triggered automatically. It is a wizard that lets you configure the main areas that cause compatibility problems.
<b>Application Compatibility properties</b>	A manual version of the wizard described above.

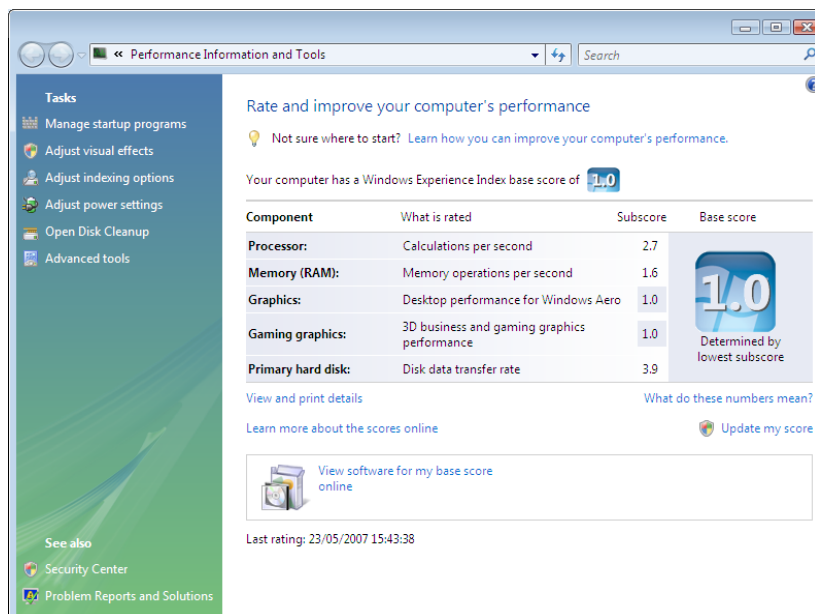


## Windows Experience

Vista will test the hardware in a given system and work out a score indicating how powerful the system as a whole is. You can find the rating by selecting **Properties** from **My Computer** entry on the start menu.



Clicking on **Windows Experience Index** provides more detailed information:

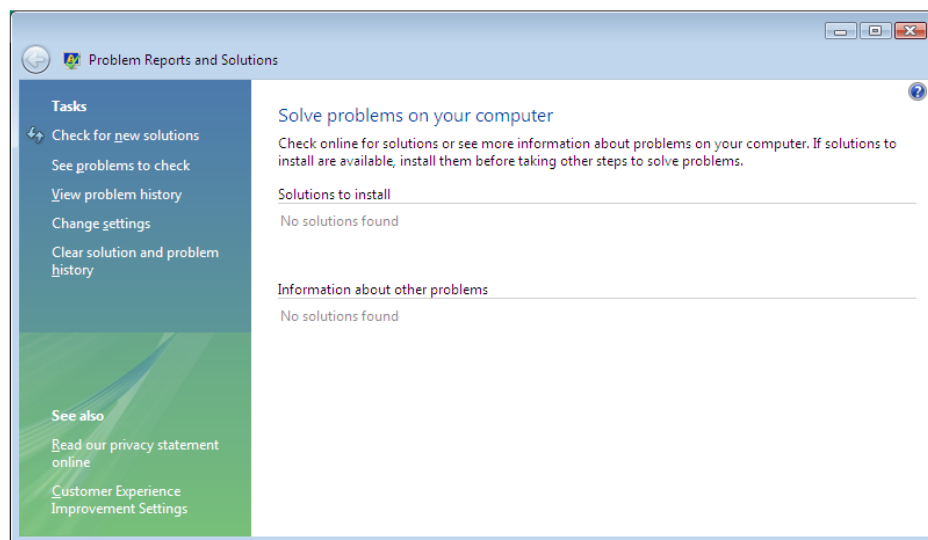


Microsoft equates numbers to the following capabilities:

score	system is capable of
1-2	General office tasks such as running MS Office, browsing the Internet etc. Will not be powerful enough to handle the more demanding multimedia applications (such as HD-DVD) or the Aero interface.
3	Should be capable of running Aero and some advanced Vista features.
4+	Can support all the advanced features of Vista, especially graphic improvements.

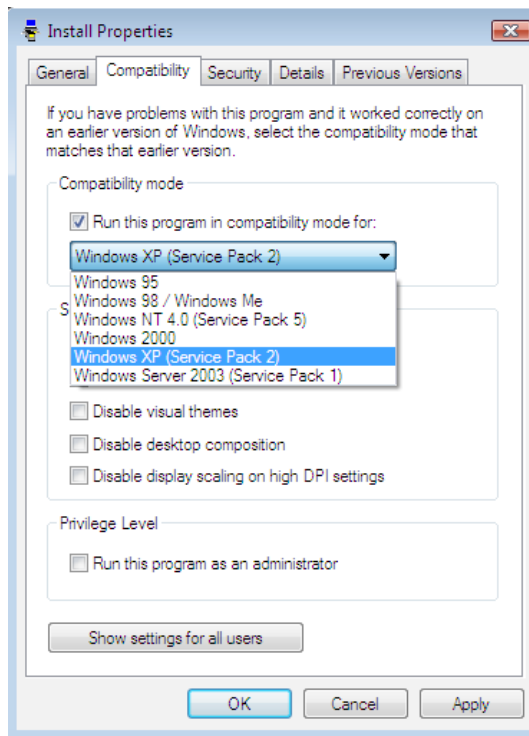
When Vista was released the highest scores found were "5". As hardware continues to improve, expect the Windows Experience Index to generate higher numbers.

## Problem Reports and Solutions



You can configure your system to update Microsoft on the problems you are experiencing. Microsoft uses this information to discover what needs to be fixed and assigns a priority for programmers. In return, Microsoft publishes solutions that your system can automatically pick up and apply.

## Compatibility mode



Compatibility Mode is used by Windows Vista to “fool” an application into believing that it is on an earlier version of Windows. This may persuade some applications to run when they take exception to Windows Vista.

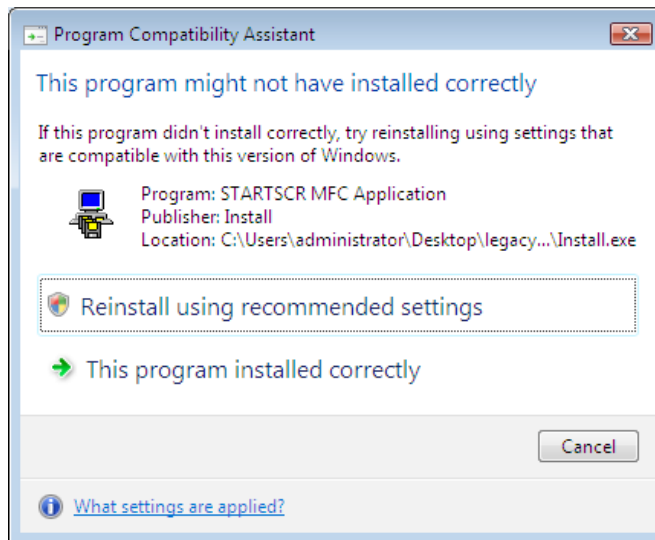
Compatibility mode is much the same as in Windows XP, with the exception that the OS versions have changed slightly.

Compatibility mode is useful for 32 bit applications running in **User Mode**, if they are not effective on Kernel Mode components, such as drivers.

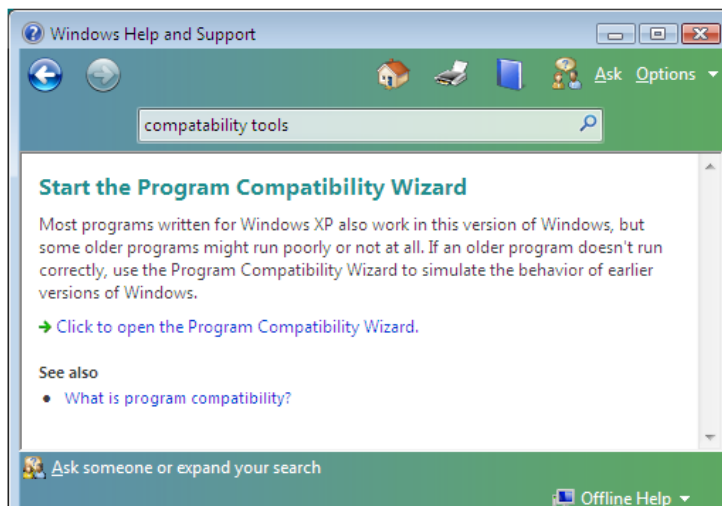
You also have the option to run the application under administrative privileges.

## Program Compatibility Assistant

The Program Compatibility Assistant should start up automatically when Vista detects that a legacy program failed to install.



The assistant uses a database of settings — you can add to this database using the **Application Compatibility Toolkit**.



## Program Compatibility Wizard

The Compatibility Wizard takes you through the steps of configuring Vista to run a legacy application, making adjustments for known problem areas.

The Compatibility Wizard is started from help:

## Application Compatibility Toolkit (ACT) 5.0

The Application Compatibility tool kit is available from Microsoft and can perform the following actions:

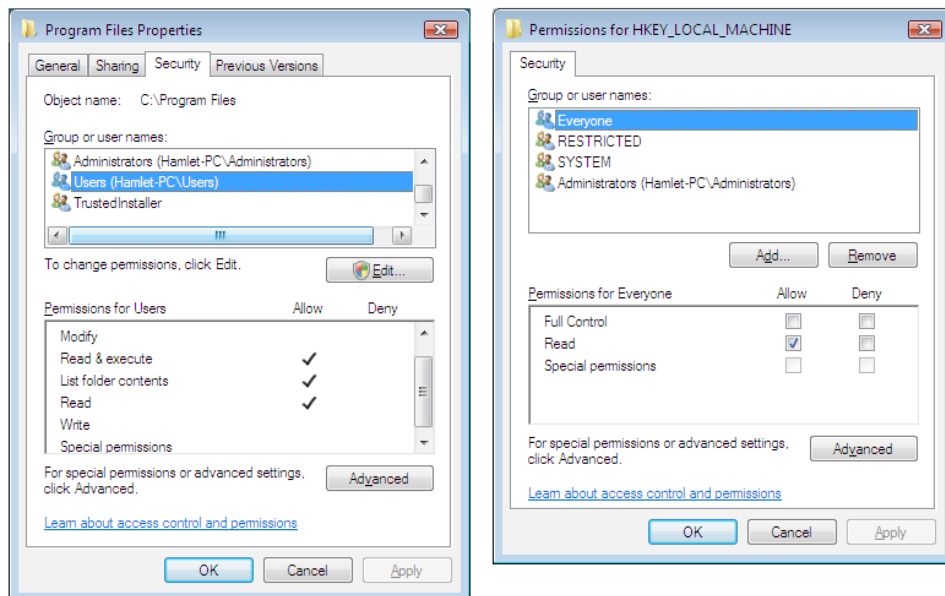
- Investigate networked computers and identify the applications installed on them.
- Report on proposed deployments and spotlight potential compatibility problems.
- Manage compatibility evaluators and settings.
- Create reports of application compatibility.
- Transmit compatibility information to the **Online Compatibility Exchange**.

## File and Registry Virtualization

File and Registry Virtualization is seen by Microsoft as an interim fix to solve the problem of software poorly written for the Vista environment.

Microsoft's guidelines state that applications:

- should store registry information by writing to HKEY\_CURRENT\_USER (not HKEY\_LOCAL\_MACHINE).
- should not place data files under the **Program Files** folder.



Permissions on Program Files and HK\_LM

Vista has strict default settings which prevent these actions taking place (thus increasing the robustness of the OS); however programs not written specifically for the Vista environment will likely not work correctly.

As an alternative to manually weakening the permissions, virtualization was developed. File and Registry virtualization consists of two components:

Component	Default behavior
<b>File Virtualization</b>	<p>If an application attempts to write to:</p> <ul style="list-style-type: none"> <li>• Program Files</li> <li>• Program Files (x86)</li> <li>• %system_root%</li> </ul> <p>and does not have permission to do so, then it is invisibly vectored by Vista to a folder in the User's profile.</p>
<b>Registry virtualization</b>	<p>If an application attempts to write to:</p> <p>HKEY_LOCAL_MACHINE\SOFTWARE</p> <p>and does not have permission to do so, then it is invisibly vectored to a special key in HKEY_CURRENT_USER</p>

Vista co-ordinates the read system as well, so that the application is not aware of the redirection.

**Tip:** You can track virtualization via the **Applications and Services** log in event viewer.

## Troubleshooting Applications

Many applications require additional disk space during the installation process. If this is not available, the installation will be corrupted or it will fail.

Many applications install **kernel mode drivers**. The ability of kernel mode drivers to communicate directly with the kernel has been severely restricted in Windows Vista. Common applications which may fail for this reason are:

- Anti-virus programs
- Firewalls
- CD/DVD burning programs
- Disk management tools

You should contact the manufacturer of the software and obtain a Vista compatible version of the application.

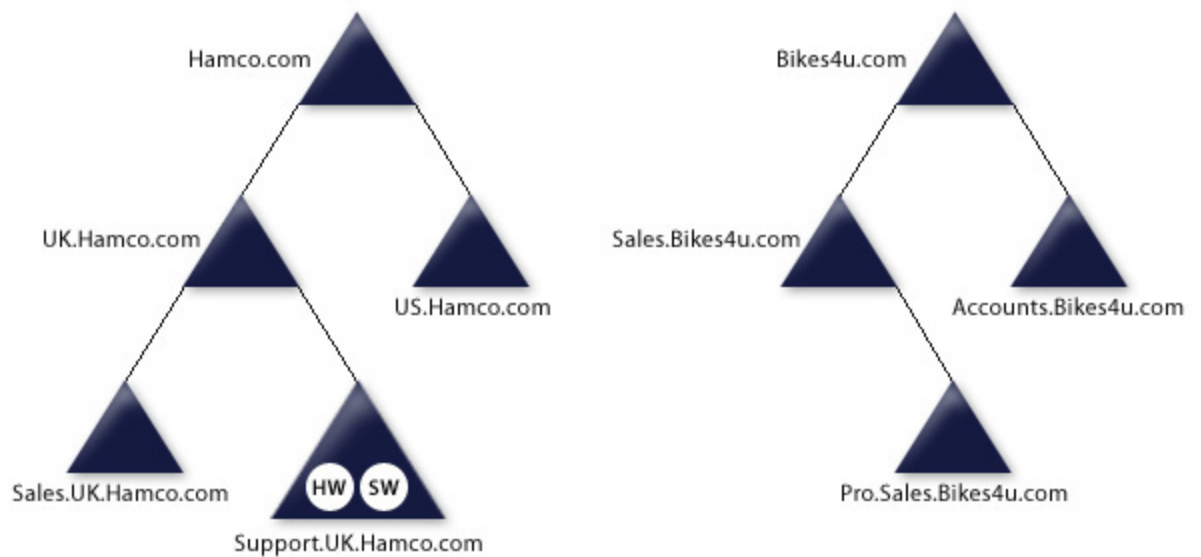
The Windows Messaging System is no longer available on Windows Vista, so applications requiring this may fail. Event Viewer and System Information should be examined when troubleshooting applications.

### Windows Resource Protection (WRP)

WRP prevents system files from being overwritten. If an application attempts this, then WRP will reinstate the changed file. Applications may fail because the file is not what they were expecting.

## Active Directory and Group Policy

### Active Directory Structure



An AD network consists of a number of items:

- **Domains**, which can contain **Organization Units (OUs)** that can be linked into **Trees** and **Forests**. All these items can be used to organize domain members together for administrative purposes.
- **Sites** are used to help preserve WAN bandwidth.
- **Global Catalogues** provide a multi-domain search facility.

## Domains and Organizational Units

The basic administrative unit of Active Directory is a **domain**. Domains are managed by the Domain Administrators, who have full control over computers in that domain.

Each domain's Domain Administrator organizes domains by creating, for example:

- User accounts
- Groups
- Computer accounts

These are used to control access to network resources.

Additionally, Domain Administrators may create Organizational Units (OUs), which are used to hold User accounts for the purpose of:

- Delegation of control
- Group Policy implementation

## Group Policy

Group Policy is a list of rules used to automatically configure or lock down a Windows Vista Computer. Typical settings available in a Group Policy are:

- Specifying desktop settings
- Controlling access to interface controls
- Distributing and managing Software
- Limiting access to the hardware

Windows Vista has included many new policies frequently aimed at managing the new features and security enhancements released with the new OS. Examples are BitLocker (a hard disk sector encryption system) and UAC controls.

## Types of Group Policies

<b>Local Policy</b>	One policy held locally on the computer. Contains the <b>Local Security Policy</b> . Some features will not be available (e.g., Software distribution).
<b>Active Directory</b>	Multiple Group Policies "flagged" in Active Directory, where they are <b>linked</b> to Sites, Domains, or OUs. Multiple Group Policies merge in turn.

Group policies consist of two halves — a computer section and a user section.



## Group Policy Application Rules

Group Policy Application Rules are managed by the Vista system. It searches for Group Policies associated with it, and its Active Directory account (if it is in an AD domain).

### Default Application Order

- Local GPOs
- Site
- Domain
- Parent OU
- Child OU

Multiple GPOs are processed from **the bottom to the top** of the GPO list. **Note:** It is possible to **Filter** a Group Policy so that it only affects specific Users or Groups.

## Group Policy tools

There are many tools to help you manage Group Policy. The most important are:

Tool	Details
<b>Secedit</b>	Command line tool used to apply security policies.
<b>GPResult</b>	Command line tool used to display which group policies affect a user and computer.
<b>GPUpdate</b>	Command line tool used to re-apply group policy settings.

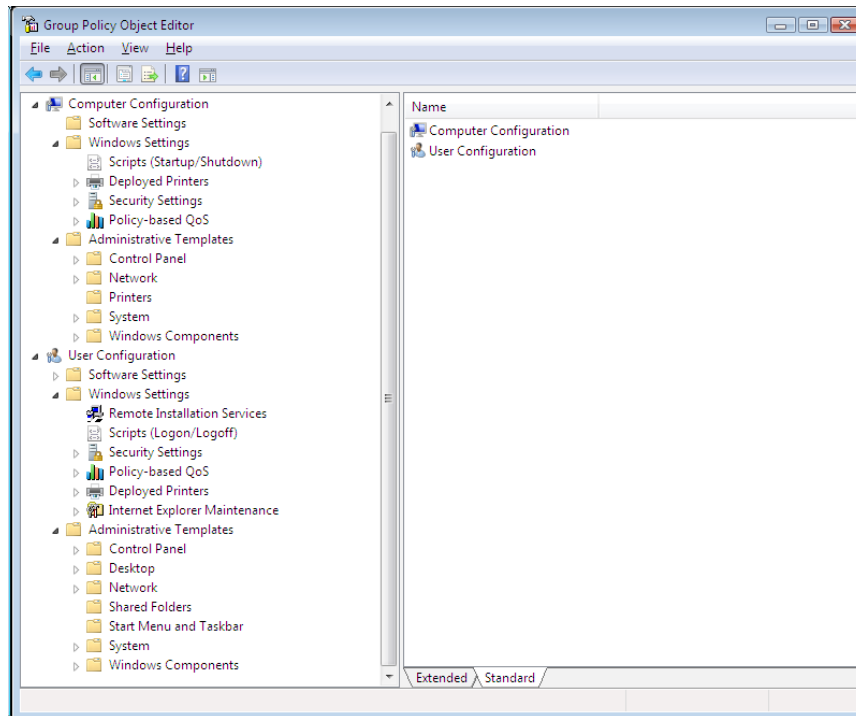
## Slow links

In systems prior to Windows Vista, Group Policy depended on ICMP to detect slow links. If a link was identified as "slow," then some parts of Group Policy (software installation, folder redirection, scripts) do not run. Unlike Windows 2000 and Windows XP, Windows Vista does not use ICMP to detect slow links.

## Local Group Policy

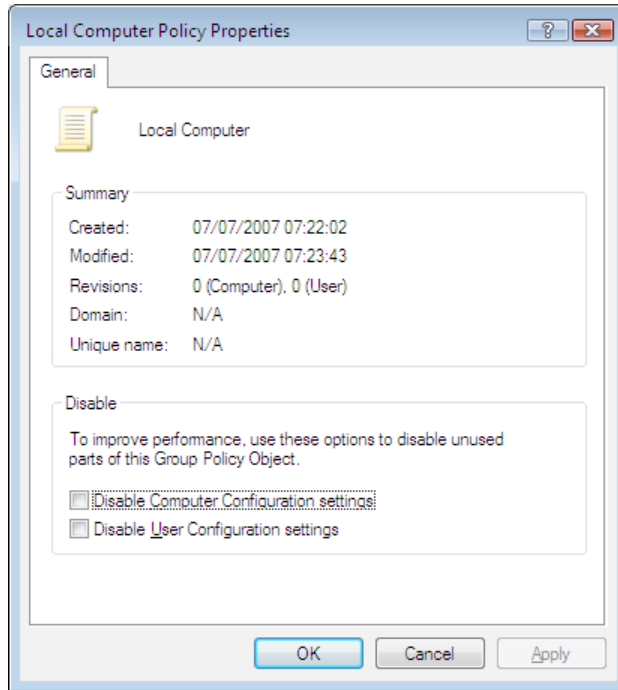
Each Windows Vista computer can have **one** local GPO. In a Workgroup, LGPs are the only option.

The LGP is opened/created using the Group Policy snap-in for the MMC, or by running the built in MMC (to invoke **GPEdit.MSC**):



## Vista group Policy

### Security Policy



**Security Policy** is the term Microsoft uses to describe all the configuration settings that can be used to protect each individual computer. Microsoft's definition of a Security Policy includes, but is not limited to:

- Password settings
- Registry settings
- Auditing
- User rights

A computer's Security Policy can be set at two points:

- Locally
- Via Active Directory

By default, Windows Vista will take Group Policies from the PDC emulator. It is possible to switch off either the computer or User half of a Local Group Policy (LGP).

## Main Security Policy Settings

In the past, Microsoft has shown great interest in the following LGP settings:

Computer Configuration   Windows Settings   Security Settings   Account Policies   Password Policy	
Entry	Default value
Enforce Password History	0 passwords remembered
Maximum password age	42 days
Minimum Password Age	0 days
Minimum password length	0 characters
Password must meet complexity requirements	Disabled
Store passwords using reversible encryption	Disabled

Computer Configuration   Windows Settings   Security Settings   Account Policies   Account Lockout Policy	
Entry	Default value
Account lockout duration	N/A
Account Lockout threshold	0 invalid logon attempts
Reset lockout counter	N/A

Make sure that you are familiar with each setting and how to combine them to meet a given password/lockout scenario. Also be aware that you can configure a logon message to appear before the logon screen. A new feature is the ability to deploy printers by the LGP.

# Vista Security

## Security background

Vista Security has been enhanced three ways:

First, Vista has a number of additional security features built into the OS itself; for example:

- Increased NTFS configuration of sensitive files and folders
- User Account Control (UAC)
- Integrity Control (IC)

Secondly, the Vista team has made strenuous efforts to prevent the core code of the OS from being tampered with, either maliciously (by a hacker) or deliberately, by add-on programs such as anti-virus detection utilities (Microsoft has always claimed that AV programs are one of the reasons why their products are so unstable).

Lastly, Microsoft has added additional security features, such as Windows Defender, and has made previous utilities (such as the Firewall) more effective.

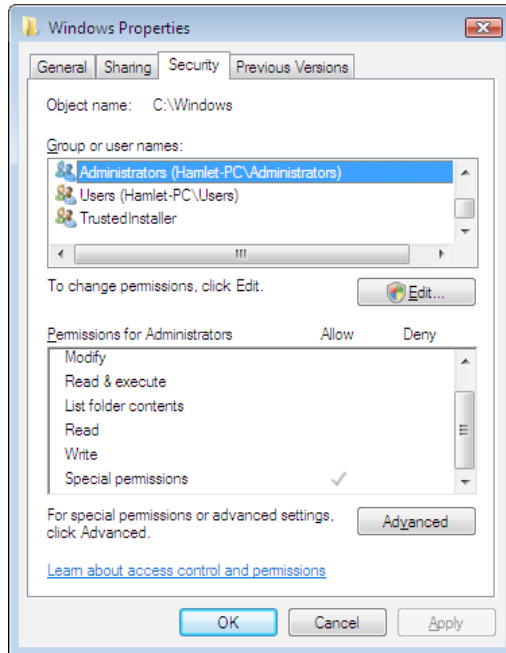
Additional or enhanced security utilities are:

Utility	Function	Where to use
<b>BitLocker</b>	Physical hard disk encryption at the sector level.	Mobile computers. Sensitive desktops.
<b>Windows Defender</b>	Detects the behaviour of malicious code.	Microsoft states that Windows Defender is not an anti-virus program, but that it can be used to detect all forms of malware.
<b>Windows Firewall</b>	Enhanced to two-way filtering in addition to being integrated with the OS.	Firewall protection.
<b>USB Group policy</b>	You can select which devices a user can plug in and use.	Highly secure environments where you do not want users installing programs from, or copying data files to, USB devices.

**Note:** *Firewalls and virus scanners provide protection for different areas on your computer - both are needed.*

## OS security enhancements

### NTFS settings



Prior to Windows, Vista Administrators have owned the %systemroot% folder, and have been allocated full control over both it and %systemroot%\System32 (In Vista, as in XP, %systemroot% defaults to C:\windows). In Vista, the owner is a system account **Trusted Installer**; Administrators lack the permission to:

- Take ownership
- Change permissions
- Delete files and folders

Also the folder is set to block permission inheritance, meaning that changes made to the root will not automatically affect %systemroot% and its subfolders. Similar adjustments have been made to System 32 and Drivers.

## User Account Control (UAC)

UAC works by limiting an Administrator's authority unless expressly instructed otherwise. It does this by changing the way that **access tokens** are used.

### Access Tokens

Anything that identifies a network member is known as a **Security Principle**; this includes users, computers, groups and domains. While humans see a friendly name (e.g., "USER1") Microsoft networks identify security principles by a unique 32 bit Hexadecimal number: the **Security Identifier**. You can change the friendly name but the SID is always the same. SIDs are never reused.

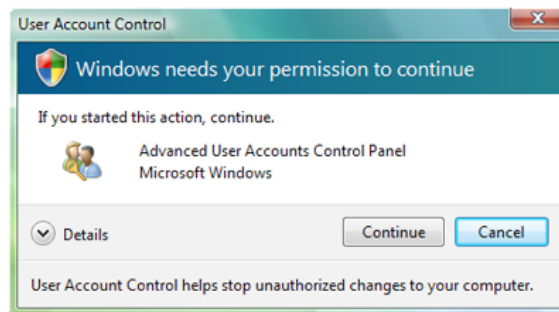
### Split tokens

The Access Token can be used in two ways:

- For access control
- To define the **system rights** an account has

When a user logs on with an Administrator account, Vista creates **two** tokens (previous versions just created one) — this is known as a **Split Token**. One token is a normal user token, while the other has full administrative rights. Microsoft refers to the normal user as a **Standard User**.

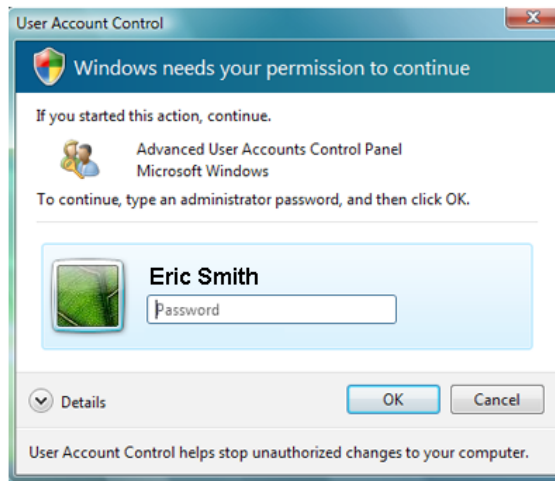
When a user starts up an application, the application uses the User's access token to authorise requests from the Operating System; the same happens if the user attempts to manipulate the User Interface. In each case, by default, Vista will supply the Standard User token, which limits the abilities of an application (such as malware) to create damage. This means that you can log on as an administrator and 90% of the time you are really acting as a **Standard User**.



When you need to use a tool that requires administrative privileges, Vista will try and guess that this is the case and do the following:

- Place the desktop into a secure mode, where only one Window can be active.
- Display an information box requesting you to confirm that you need to exercise administrative privileges.

If you affirm that you need to be an administrator, then that token is used rather than the Standard User.



Alternatively, in the case of a standard user account (who does not have a split token), Vista will ask for a second set of credentials that have the necessary rights.

#### Tasks which only require standard user privileges

The following tasks do not require administrative privileges (this is not an exhaustive list):

- Create a LAN connection
- Set up a Wireless connection
- Change the display settings
- Change the desktop background
- Play and burn CD/DVDs
- Change the time zone
- Change own password
- Set battery power options
- Set accessibility options
- Restore own files from backup
- Defrag hard disk (technically user's cannot do this but the service does under it's own privilege)
- Connect using Remote Desktop
- Synchronize with mobile device
- Set up BlueTooth connection

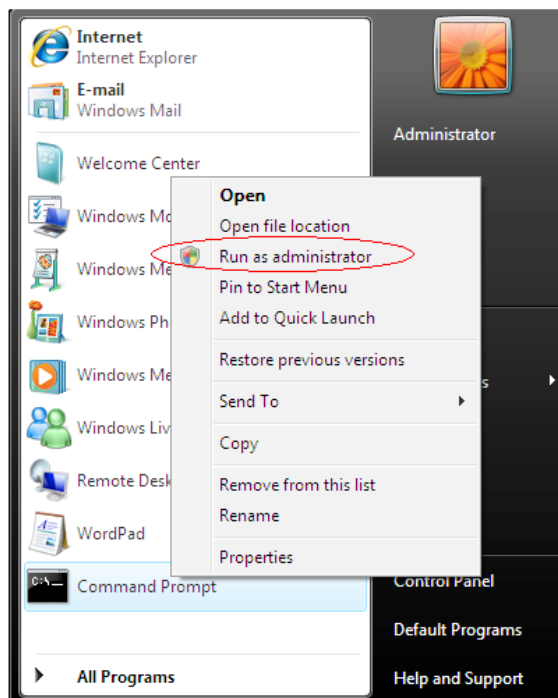


### Tasks which need administrative privileges to run

The following tasks **do** require administrative privileges (this is not an exhaustive list):

- Install/uninstall applications
- Install device drivers
- Install Windows updates
- Install ActiveX controls
- Configure Windows Family Safety
- Manage user accounts
- Change UAC settings
- Open the Windows Firewall Control Panel applet
- Configure Remote Access
- Schedule tasks
- Configure automatic updates
- Access other user's folders
- Make changes to the Program Files folder
- Make changes to the Windows folder
- Restore system files from a backup

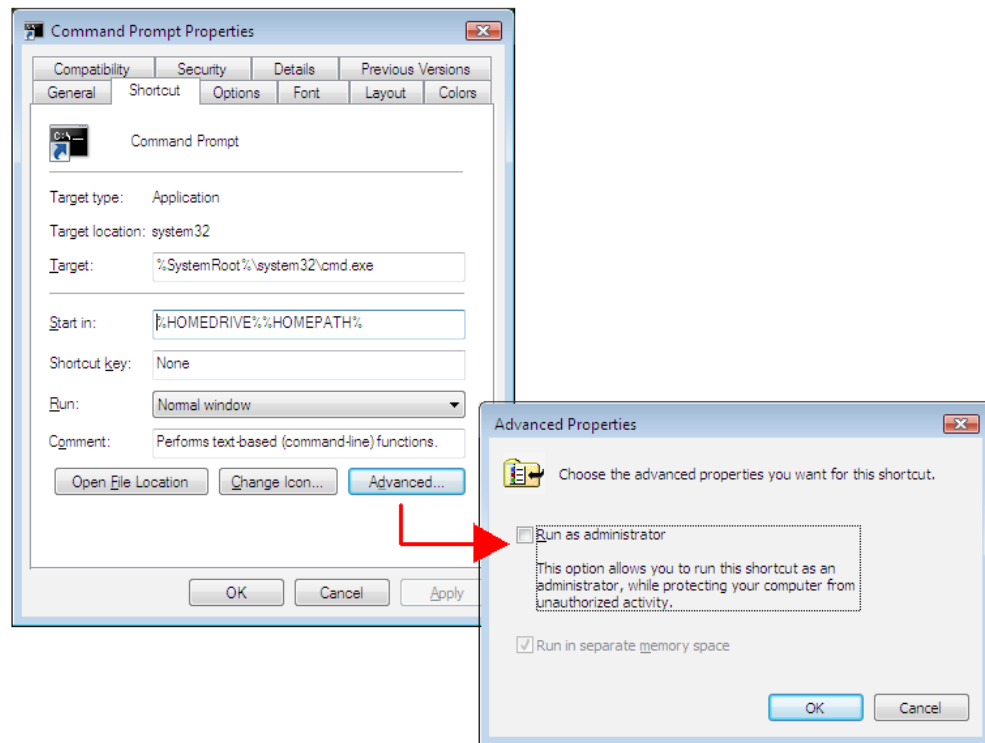
### Gaining administrative privileges



Vista cannot always guess that you will need the option of using the Administrator Token, in which case you will need to manually inform it.

There are several ways to do this. The two easiest are:

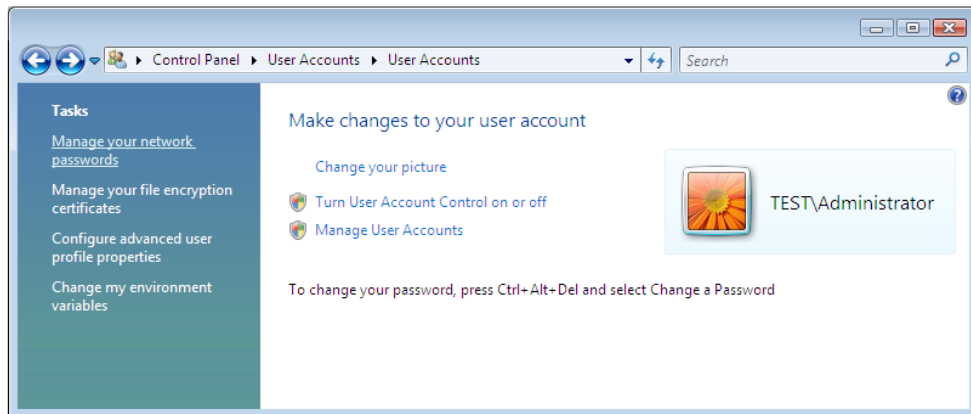
- Select **Run as Administrator** from the application's context menu.
- Configure a Shortcut.



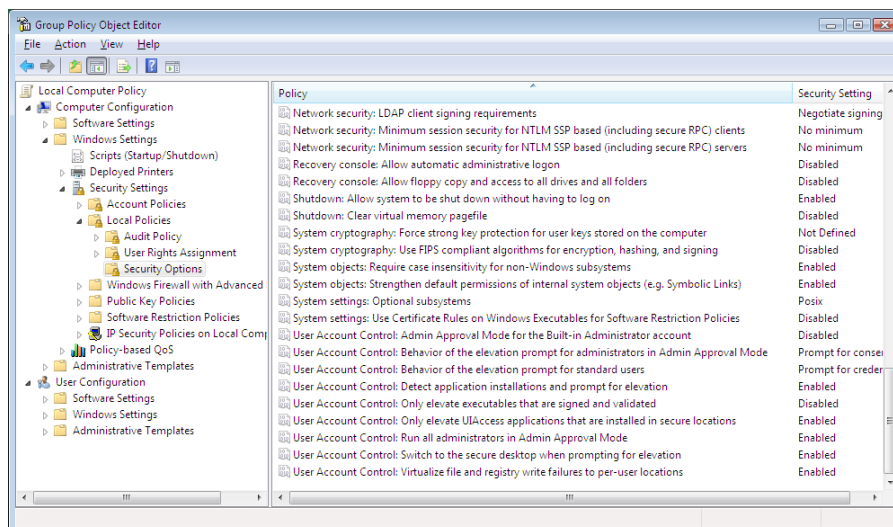
### Configuring a shortcut

## Controlling UAC

You can switch UAC on or off from **User Accounts** in **Control Panel**:



You can also control UAC's behavior by means of Group Policy. The policies for UAC are located in the **Security Settings** of the **Local Policies** in the **Computer Configuration** section of the Group Policy:



Look for entries that begin "User Account ..."

The following policies are available:

Policy	default	effect
<b>Approval Mode for the Built-In Administrator (BIA) account</b>	Disable*	Enabling provides BIA with a split token; disabling returns to the previous Windows mode.  *Default is different in an upgraded system where Built in Administrator is the only administrator account. In this case it is enabled.
<b>Behavior of the elevation prompt for administrators in Admin Approval Mode</b>	Prompt for consent	Controls how Vista behaves when it determines that administrative privileges are required and it is using the split token model. There are three choices:  <b>Prompt for consent:</b> An administrator will be asked to permit or deny. If they choose permit then the administrative token is used.  <b>Prompt for credentials:</b> The user is prompted for a set of administrative credentials instead of just permitting or denying.  <b>Elevate without prompting:</b> If the user has a split token, the system will simply use the administrator version without checking for a permit.
<b>Behavior of the elevation prompt for standard users</b>	Prompt for credentials	Users do not have split tokens so they will not be prompted for a permit/deny; the only two options are: <ul style="list-style-type: none"> <li>• Prompt for credentials</li> <li>• Automatically deny elevation requests</li> </ul>
<b>Detect application installations and prompt for elevation</b>	Enabled	Determines what happens when Vista detects an application installation that will require administrative rights. Can be enabled or disabled.
<b>Only elevate executables that are signed and validated</b>	Enabled	Options are enabled or disabled.

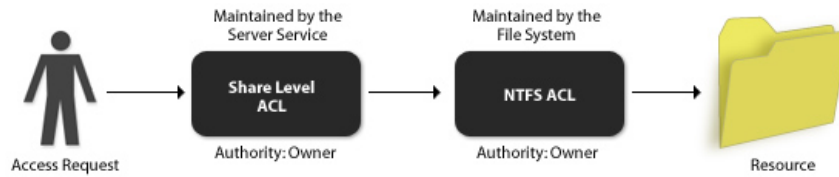
<b>Run all administrators in Admin Approval Mode</b>	Enabled	<p>This setting switches UAC on or off (it applies to all admin accounts, including BIA). There are two settings:</p> <p><b>Enabled:</b> Admin mode is switched on for all accounts (although it can be modified by the other policies mentioned here). This will require a re-boot.</p> <p><b>Disabled:</b> UAC is switched off and we return to a single token for administrators.</p>
<b>Switch to secure desktop when prompting for elevation</b>	Enabled	<p>This “isolates” the elevation prompt from the rest of the GUI. This prevents hackers attempting to modify the prompt so that you indicate yes allow when you mean deny. The options are enabled or disabled.</p>
<b>Virtulize the file and registry write failures to per-user locations</b>	Enabled	<p>Vista has tightened up on which locations in the registry can be written to. Legacy applications (and viruses) will be blocked from sensitive areas.</p> <p><b>Enabling</b> this option instructs Vista to maintain the data in a “mirrored” set of pseudo-keys held in the user’s profile. This is done invisibly to both the user and the application, so your old programs should continue to run.</p> <p><b>Disabling</b> this policy will cause the legacy applications to fail (it will not allow them to write to the actual registry keys).</p>

## Windows Integrity Control (WIC)

WIC establishes a security scheme based on **Mandatory Access Control** (MAC). There are a number of authentication systems in common use; however, most commercial Network Operating Systems have based their security model on **Discretionary Access Control** (DAC).

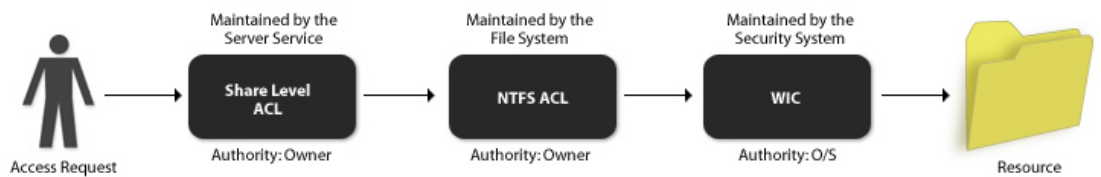
<b>Discretionary Access Control</b>	Every resource (e.g., a file, folder, or printer) has an <b>owner</b> who has complete control over it. The owner edits the resource’s access control list to specify who can have which type of access.
<b>Mandatory Access Control</b>	The owner is not the final authority. The System (or the system administrator, in some cases) defines what rights (if any) an owner can assign. MAC is much more secure than DAC; however, it is more complex to manage (which is why it is popular in secure military products).

With Vista, Microsoft inserted an additional test into the security system. You may recall that in previous versions of Windows a request from the network to access to a folder on a NTFS partition was tested twice:



Access control pre Windows Vista

Vista adds a third test which, like the other two, **must** be passed:



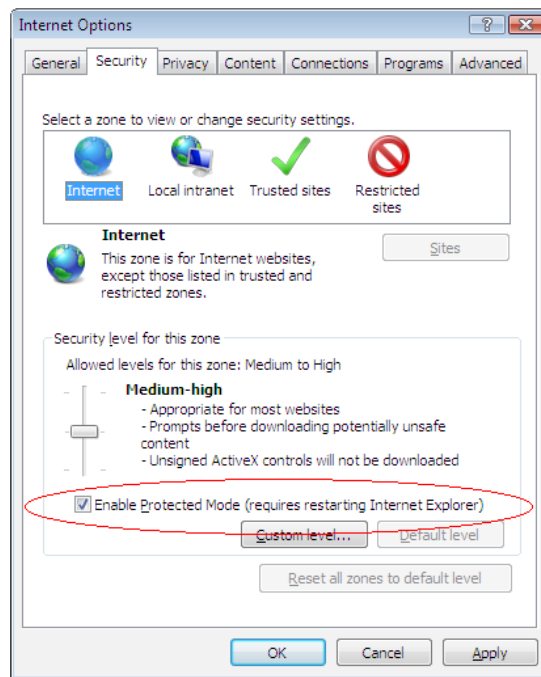
Access control in Vista

### Integrity levels

Vista assigns objects (such as users and files) to one of five **Integrity levels**. Each level has a place in the integrity hierarchy. The rule is that, by default, WIC will prevent a process from writing to one with a higher level.

The integrity levels are as follows:

Level	where it is used	typical assignments
<b>Untrusted</b>	Given to any process using anonymous credentials	N/A
<b>Low</b>	For download from the Internet	By default IE7 runs at this Level (see Protected Mode later)
<b>Medium</b>	The "default"	Any object not specifying another level Normal users are assigned this level when they log on
<b>High</b>	To allow accounts to control the OS	Assigned to administrators
<b>System</b>	OS components	Services Kernel mode components



### Internet Explorer 7 (IE7) Protected mode

By default, IE7 runs in **Protected Mode**, which uses the **Low** integrity level. As the OS and any data **not** acquired over the Internet runs at level 3, then this should prevent malicious code that has entered a computer via IE7 from attacking the OS and a user's files.

Vista sets the Low level on a few folders in the user's profile (such as Temporary Internet Files) and also does the same with some specific registry keys (the ones that are used to save a User's settings to).

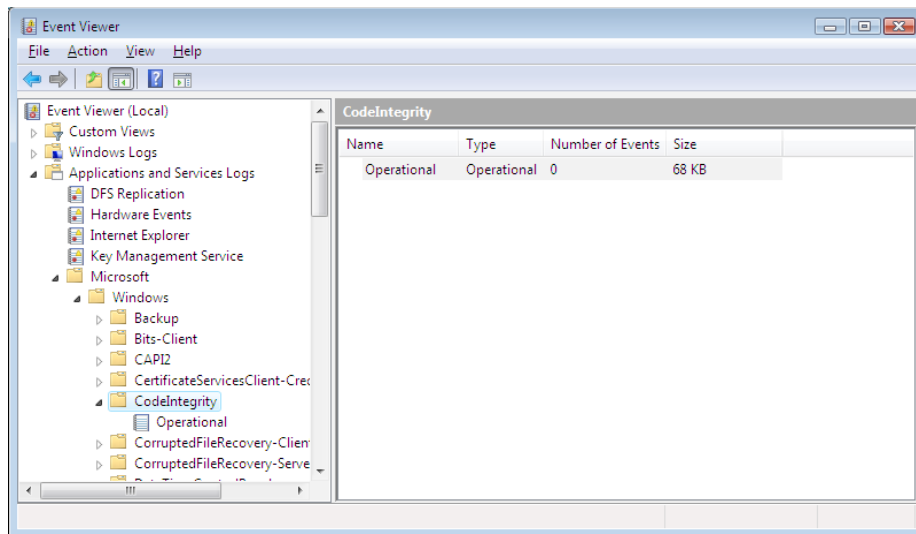
**Note: Trusted sites.** By default protected mode is switched off for this zone (it is on for all the others).

## Windows Resource Protection (WRP)

WRP is the successor to Windows File Protection used in XP. Its job is the same: to protect the files in %SystemRoot% and its sub-folders. WRP maintains “back-up” copies of these files; if they change, it is capable of replacing them.

**Note:** Unlike Windows XP however you have to run `sfc/scannow` to trigger the return.

The code integrity system also checks the kernel, HAL, and any initial drivers loaded when Vista boots. Details of code integrity problems may be recorded in the Event Viewer:



Code Integrity in Event Viewer

## Service management

In Windows, a **Service** is a background process which performs a specific tasks or maintenance functions. Some of the services included in Windows are:

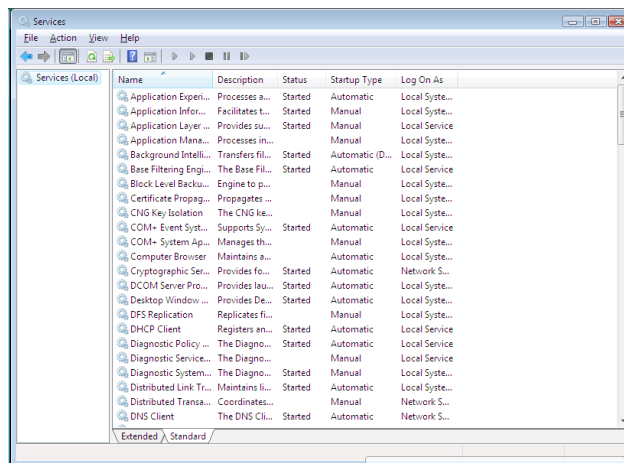
Service	Feature
Print Spooler	Manages the Print Spool (the storage system that accepts print jobs).
Server	“Listens” on the network and accepts connection requests from computers wishing to access shared resources such as printers and files.
Workstation	Transmits requests to another computer’s Server service.
Windows Update	Periodically checks and applies patches and service packs.
Windows Time	Synchronizes the computer’s clock with an external source.
DHCP Client	Allows Vista to make use of a DHCP server, if available.



A service is similar to an application; however, there are a number of major differences:

- They usually run all the time.
- They run in the background, so you may not be aware of them.
- They are assigned their own credentials to run under, and so will start working even if nobody is logged on.

Many server applications are implemented as a group of services, so as you install software, expect to see the number of services grow.



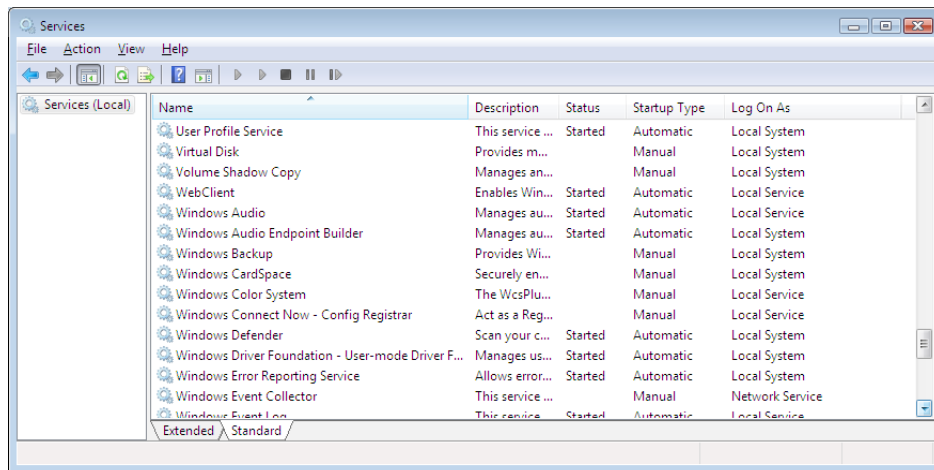
Vista Services

## Drivers

Drivers are also similar to services; however, drivers will interact directly with the system hardware, while services do not. From the control perspective, drivers are managed by **Device Manager**, while Services are managed by the **Service Control Manager** in Administrative Tools.

## Managing Services

There are a number of ways to manage services. The easiest way is to use the **Services** application (Service Control Manager) in administrative tools:



**Vista Service Control Manager**

**Tip:** You can start up Service Control Manager from the command line. Type: **Services.msc**. To see a list of all services running use the **Net Start** command without any switches.

Using Service Control Manager, you can see which services are running and change each one's configuration.

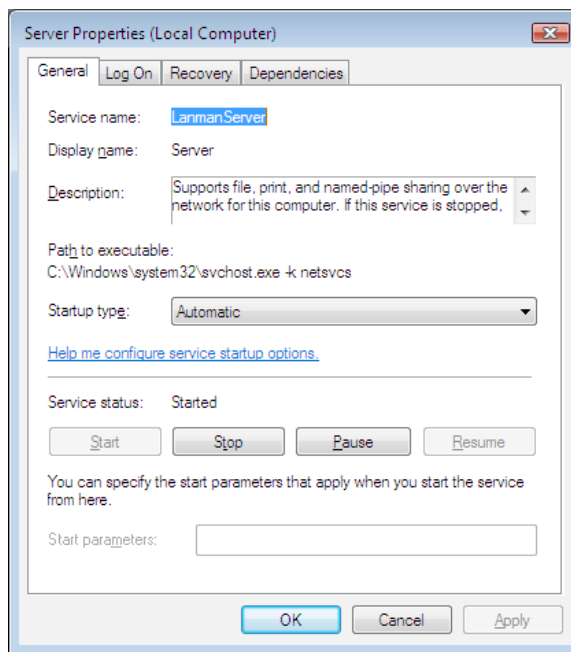
**Note:** If a service is not listed as **Started**, then it is not running.

Services can also be managed:

- using the **SC.Exe** command line tool.
- using the **Net** commands (Net Start, Net Stop etc).

**Alt-clicking** on a service allows you to view its configuration pages.

## General tab



Provides information on the state of the service and allows you to modify the following:

Startup state:

<b>Disabled</b>	Service cannot and will not start
<b>Automatic</b>	Service starts when Windows boots
<b>Manual</b>	Service does not start when Windows boots however it starts if another service needs it (or if it is started manually)

### Service Status:

Defines the state of the service

<b>Start/Stop</b>	If a service is stopped then it shuts down, any process using that service is cut off
<b>Pause/Resume</b>	If a service is paused then it <b>usually</b> remains running however it will not accept any new connections from processes

### Log On tab

This tab allows you to configure the security credentials that the service will use. As services perform “behind” the user interface, they need elevated privileges. You can choose to create a User Account with the correct rights for the service, or select one of the “generic” service accounts provided by Microsoft. If you have a password expiration set in your password policy, make sure that the password is configured to never expire; otherwise, your service will fail when the password becomes out of date.

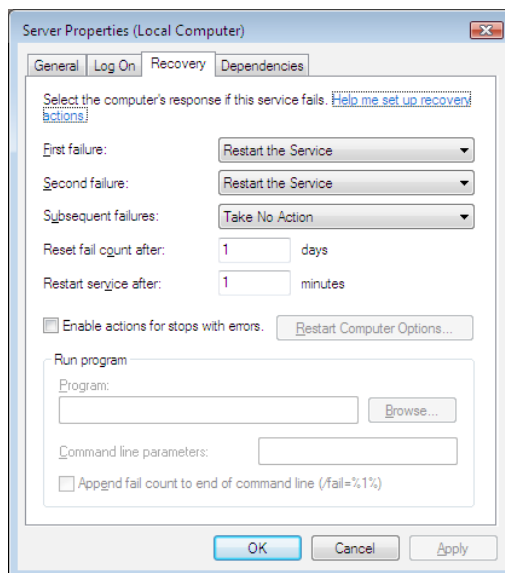
Windows Vista provides three types of generic service accounts:

Account	Features
<b>Local System</b>	Local System has full administrative rights to a computer (or a Domain, if on a Domain Controller). In previous versions, it was the account that all Windows services used, by default (called <b>System</b> ).
<b>Local Service</b>	Similar to a standard user, this account has the same level of access to resources and objects as members of the Users group.
<b>Network Service</b>	Similar to the <b>Local Service</b> account; however, it can access networked resources.

**Warning:** Changing a Services credentials can cause it to fail.

Prior to Vista, just about every service used the Local System account by default. Vista has started using the lesser accounts, which means that the capability of a hacker to hijack a service then use it to create havoc has been reduced.

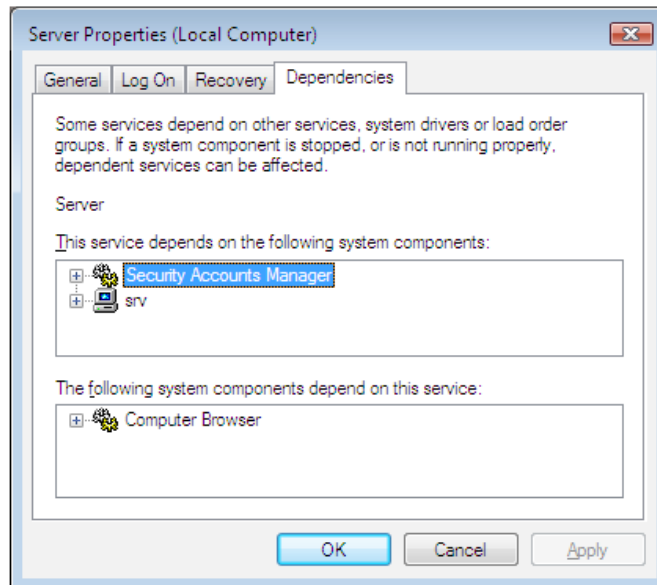
### Recovery tab



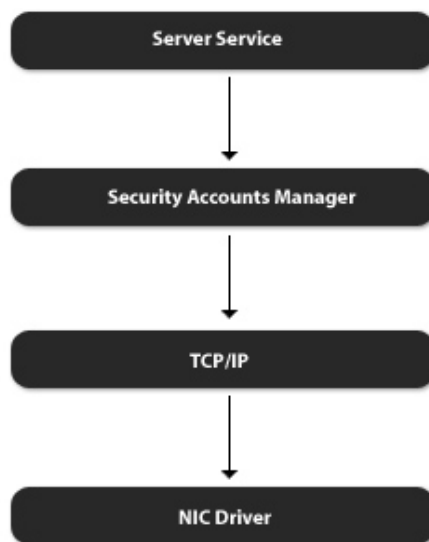
Allows you to specify what actions Windows should take if the service fails.

**Dependencies tab**

Visually shows you the other services a service needs to run, and which services need that service:



Services make use of each other, as the graphic example below demonstrates:



Service and Driver Dependencies

If a service or driver further “down” the chain fails, then none of the services which depend on it will start. This is often indicated with a “**Service or Dependency failed to start...**” message when the system boots.

**Tip:** *The event logs track service failure.*

### Vista service security enhancements

Microsoft modified the service environment to make Vista more secure than previous versions of Windows. Some of the modifications made include:

- Using a less authoritative set of service credentials
- Session separation
- Service isolation
- Restricting

### Using a less authoritative set of service credentials

As discussed previously, Microsoft is making much more use of the “lesser” service accounts. Where necessary, Vista services have been modified to work using these accounts instead of needing the Local System account.

**Note:** *An administrator could use SC.Exe to reduce service privileges.*

### Session separation

Vista, like XP before it, runs as a series of **sessions**. A session can be loosely defined as **a common group of applications accessed through a desktop**.

Sessions are created for such events as:

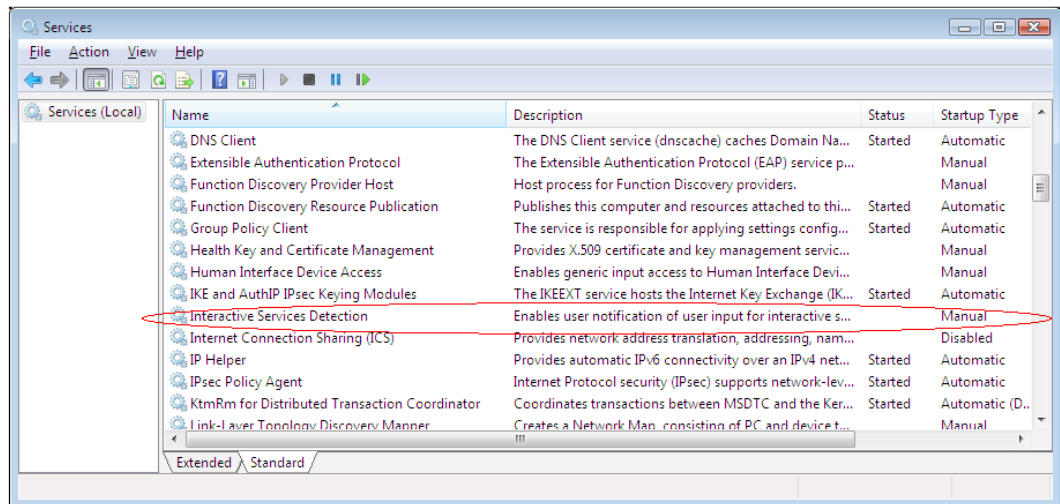
- User switching
- Terminal Server
- Remote Desktop/Remote assistance

Vista uses sessions to help secure services. Vista now runs all services in their own session (Session 0 — the first session). Microsoft has modified the abilities of Session 0 in the following ways:

- No User Interface supported
- Cannot communicate with the video hardware
- Can only communicate with other sessions via RCP (Remote Procedure Call)

This isolation helps secure Vista by helping to prevent the authority of a service from abusing the system; however, it can create problems if a service needs to alert you about something.

Vista has a helper application that reduces the service-to-desktop communications restrictions, allowing service pop up boxes to inform you, for example, that “the printer is out of paper”. This is another service called the **Interactive Services Detection Service**.



By default, the startup type for this service is **manual**, so it should start when needed. If you do not need the communication feature, you may wish to disable this service.

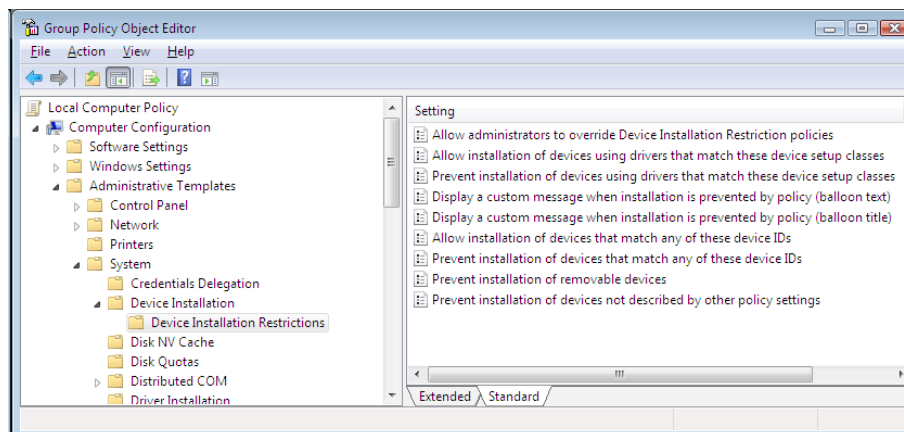
**Note:** Microsoft see the **Interactive Services Detection Service** as a temporary fix and intend to remove it as soon as feasible.

### Service Isolation

It is possible to **isolate a service**; that is, to prevent the service from modifying any file without explicit permission by the administrator. Microsoft changed services in Vista giving each an **SID** (Security ID) just like a user account. If you set up service isolation then you need to configure the ACL on every file and registry key that you wish the service to change and grant it **write** access. Administrators use **sc.exe** to configure Service Isolation.

### USB management

You can use Group policy to control how users work with USB devices.



Group Policies can be found in Computer Configuration \Administrative Templates \System \Device Installation \Device Installation Restrictions.

Using Group Policy, you can:

- Prevent users from installing all devices.
- Specify an "Allow List" including the only devices Users are permitted to install.
- Specify a "Deny List". Users can install any devices not on this list.
- Deny Read or Write access to removable media devices.

USB devices identify themselves by means of **Identifiers**. You can query a USB device for its identifier by using the **DevCon** tool. This is a command line tool and can be downloaded from the Microsoft Website.

## File Security

Files are secured by **Access Control Lists (ACLs)**; these are lists of Users and Groups linked to the type of access they are permitted.

A Windows Vista system can draw on the following for a list of Users or Groups:

Situation	Can use ...
<b>Vista in a Workgroup</b>	Local Groups and Local User Accounts
<b>Vista in a Domain</b>	Domain User Accounts and Groups Local User Accounts and Local Groups

If a file resides on an NTFS partition, then there are two security systems which maintain ACLs on the folder and/or files:

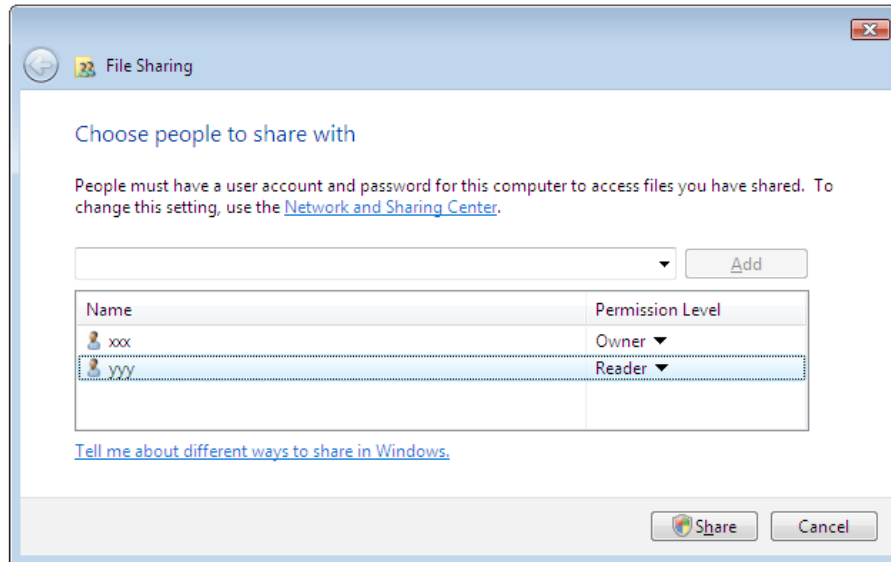
- Server Service maintains Share level Security
- NTFS maintains Local Security

To successfully access a resource you will need to pass both security systems if accessing from the network, and only Local Security if you are logged onto the system itself (logged on **Interactively**).



## Simple File Sharing

In a Workgroup environment, Windows Vista uses Simple File Sharing as the default method.



In Simple File Sharing, share level and local security is configured at the same time. Users require a password, and may be assigned one of the following permissions:

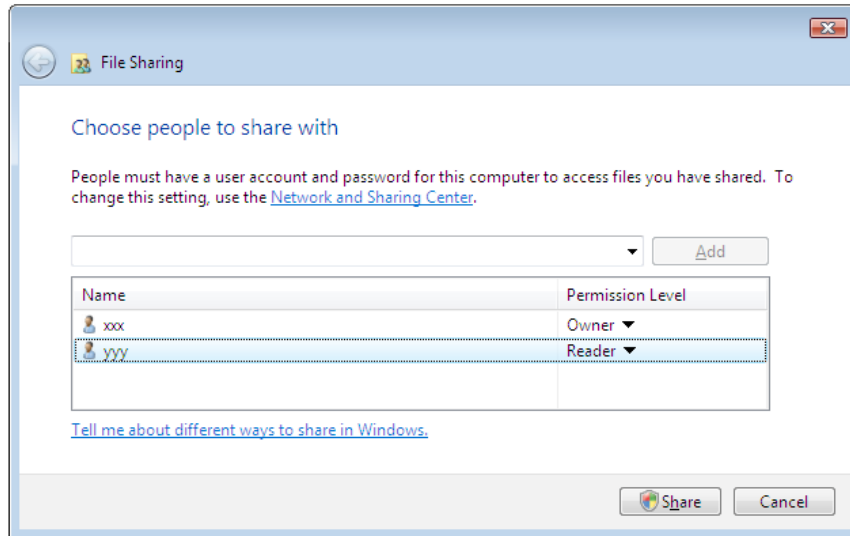
<b>Owner</b>	The creator of the folder that has full control over access and the contents inside.
<b>Co-owner</b>	Allows the person or group to view, change, add, and delete files in the shared folder.
<b>Contributor</b>	Can view all files, add files, and change or delete the files that they add.
<b>Reader</b>	Can view files in the shared folder.

## Public folder

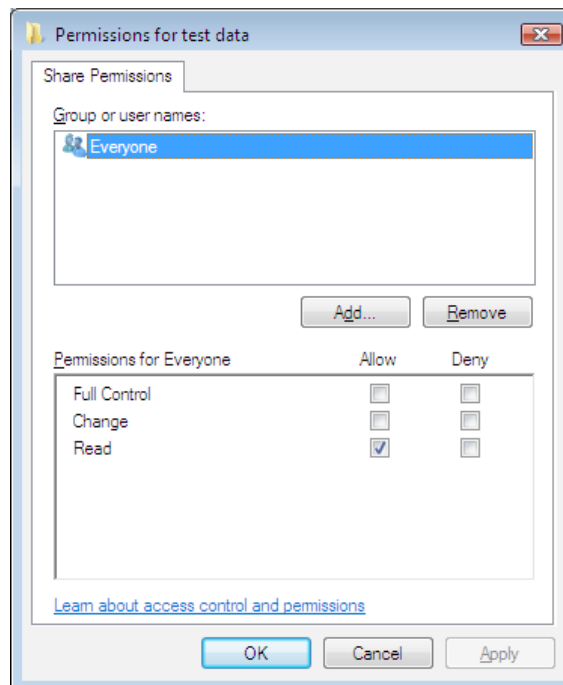
A simpler method of sharing files is to use the **Public Folder** included on the Start Menu. This is accessible by all users of the computer and it can be shared to provide access across the network.

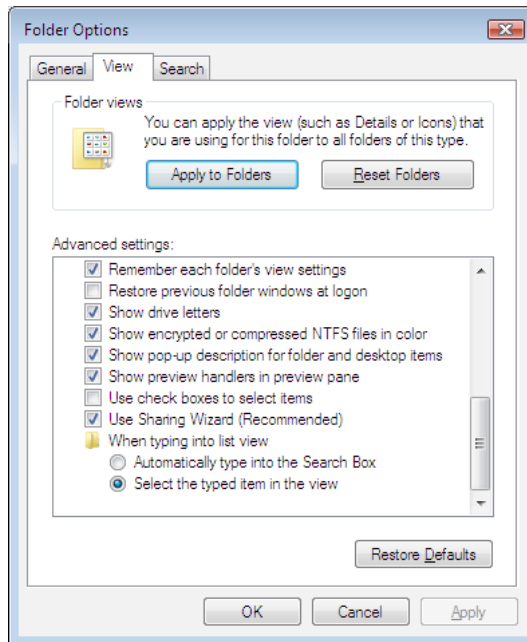
## Traditional Access Model

Simple File sharing is switched off when Vista receives Domain membership; it is also possible to switch sharing models from the **View** menu in the **File Options** settings pages.



The traditional model, which has separate tabs on a folder's properties settings for both security systems:





Traditional control tabs detailing default Vista settings

### Share level permissions

Access Level	Feature
<b>Full Control</b>	<p>Allows user to take ownership of files and folders.</p> <p>Is assigned to the Everyone group by default.</p> <p>Users can change file access rights.</p> <p>Grants user all permissions assigned by the Change and Read levels.</p>
<b>Change</b>	<p>User can add and create files.</p> <p>Grants ability to modify files.</p> <p>User can change the attributes of the file.</p> <p>User can delete files.</p> <p>Grants user all permissions assigned by the Read level.</p>
<b>Read</b>	<p>User can display and open files.</p> <p>User can display the attributes of the file.</p> <p>User can execute program files.</p>

## NTFS permissions

Permission	Allows the user to
<b>Read</b>	View files and subfolders in the folder and view folder attributes, ownership, and permissions.
<b>Write</b>	Create new files and subfolders within the folder, change folder attributes, and view folder ownership and permissions.
<b>List Folder Contents</b>	View the names of files and subfolders in the folder.  <b>Note:</b> <i>Only available on the folder, not the file.</i>
<b>Read and Execute</b>	Traverse folders and perform actions permitted by the Read permission and the List Folder Contents permission.
<b>Modify</b>	Delete the folder and perform actions permitted by the Write permission and the Read and Execute permission.
<b>Full Control</b>	Change permissions, take ownership, delete subfolders and files, and perform actions permitted by all other NTFS folder permissions.

## Rules

You must satisfy both security systems when connecting across the network. This means you must be allowed the appropriate access in either your own account or by group membership.

- A **deny** always overrides an allow.
- NTFS files moved or copied into another folder inherit their folder's permissions.
- NTFS files and folders **inherit** their permissions from their parent folders unless permission inheritance is switched off on the file or folder (share level security does not use the concept of inheritance in this way).
- Only NTFS allows files to be compressed, or encrypted by the Operating System.

## Contrasting permissions

Share permissions are set at the folder only Local Security and can be set at the folder or the file level. In Local Security, files pick up the settings of the folder they are in but can then be modified. In share level, you are evaluated when you connect to a computer. In NTFS, your permissions are re-assessed as you attempt to access each new sub-folder or file.

## Disks and File Systems

Although not explicitly mentioned in the exam syllabus, the examiners will expect you to be aware of disks, file systems and file system capabilities, and may quiz on the security capabilities of each. Here is an overview of the major points.

### Dynamic and Basic Disks

Basic disks are the traditional means of partitioning a hard disk. The disk can be split into **four** partitions, one of which could be an **extended partition**. Extended partitions can hold multiple file systems (FAT 16/32 or NTFS), each of which can be assigned a capital letter as an identifier. The other partition types can only hold one file system. Windows Vista, like other workstation products, can use **Primary Partitions** (which can be made **active** so the BIOS will use them to boot from), **Stripe Sets** (up to 32 areas spread over up to 32 drives, with one area per drive) or **volume sets** (32 areas combined on one or more drives).

Dynamic Disks introduced in Windows 2000 present to the hardware as a single traditional partition (which can be active). Internally, they can be divided into **volumes** (instead of partitions) which can be **simple** (one area on one disk), **stripped** (32 areas on 32 disks) or **spanned** (32 areas on one to 32 disks). Stripping delivers the fastest speed but cannot be used to host the system boot files.

There is no fault tolerance built into Windows Vista (you require a server product for that).

### File Systems

A file system is used by an OS to store and retrieve files. There are three main file systems that Vista supports:

- FAT16 (often referred to as just FAT)
- FAT32
- NTFS

Microsoft recommends NTFS, as it can support the following:

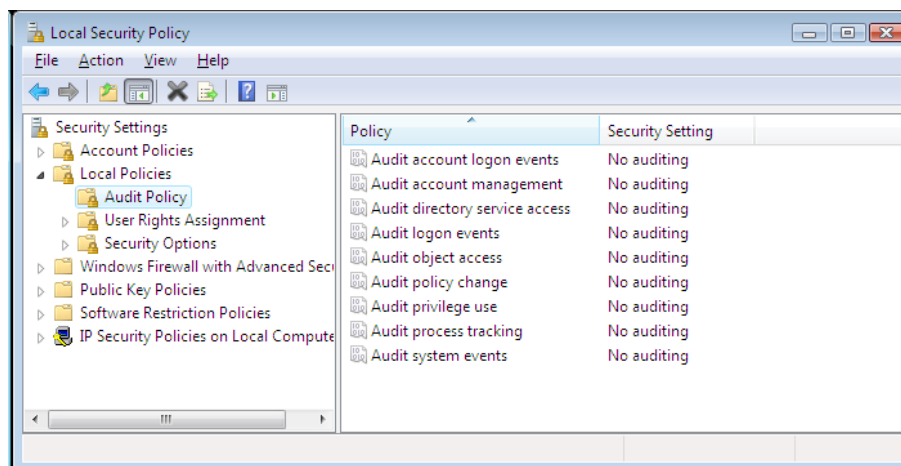
Feature	Provides
<b>Disk Quotas</b>	Allocation of disk space on a per user/per volume basis.
<b>Local Security</b>	Access control to the users' files.
<b>Compression</b>	Compression to files in order to save space.
<b>Encrypted File System</b>	Transparent encryption of files on a per User basis.

A comparison of the file systems supported by Windows Vista is as follows:

Feature	NTFS	FAT16	FAT32
<b>Volume size</b>	10MB (recommended minimum) - Practical Max 2TB	Volumes up to 4 GB	Volumes from 512 MB to 2 terabytes  Vista, you can format a FAT32 volume only up to 32 GB
<b>File size</b>	Maximum file size 16 terabytes minus 64 KB	4GB	4GB
<b>Files per volume</b>	4,294,967,295	65,536	4,177,920

## Auditing

Auditing allows you to monitor users' activities on the network. You can choose to audit the success or failure of several types of network usage, such as logging on, printing activities, and attempting (or succeeding) to access NTFS files or Folders. Auditing is set up in the **Local Security Policy**; individual audit lists are then created on folders and files.



The results are recorded in the **Security Event Log**:

Audit	Covers
<b>account logon events</b>	This is used by Domain Controllers to record logons, which they have validated for remote systems. An example would be someone logging onto a Vista system that is a domain member.
<b>logon events</b>	Logging on locally. This will record interactive logons by local accounts on workstations and domain accounts on Domain Controllers.
<b>account management</b>	Changes to User accounts and groups such as: <ul style="list-style-type: none"> <li>• Renaming</li> <li>• Deleting</li> <li>• Enabled/Disabled</li> <li>• Password changed</li> </ul>
<b>directory service access</b>	Records access to Active Directory objects.
<b>Object Access</b>	Sets up recording to (NTFS) files and folders, printers, registry keys etc. Unlike the other settings, each object must then be individually configured with the type of auditing required (Group/User and access type).
<b>policy change</b>	Records modifications of User rights, audit policies and trust policies.
<b>privilege use</b>	Records the use of a User right.
<b>process tracking</b>	Records processes — this is used by programmers when troubleshooting code.
<b>system events</b>	Records shutting down the system or events which impact the computer's security or event log.

## Windows Firewall

The firewall in Vista has been modified two ways:

- Functionality vastly enhanced
  - Two way filtering
  - More flexible rules
  - Incorporates IPSec policies
- Integrated into the networking sub-system
  - Network profile

### Rules

Rules can be based on the following:

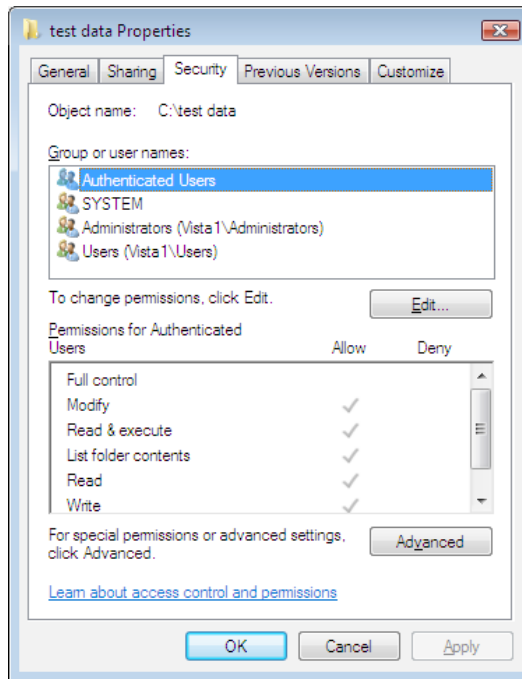
- Domain Users and Groups
- Type of network interface (WLANS, LANs, WANs etc)
- IP protocol number
- Services
- IP protocol number
- Source/Destination IP address
- Source/Destination Port number
- Multiple ports
- ICMP types (ICMP 4 and 6)



## Firewall Management tools

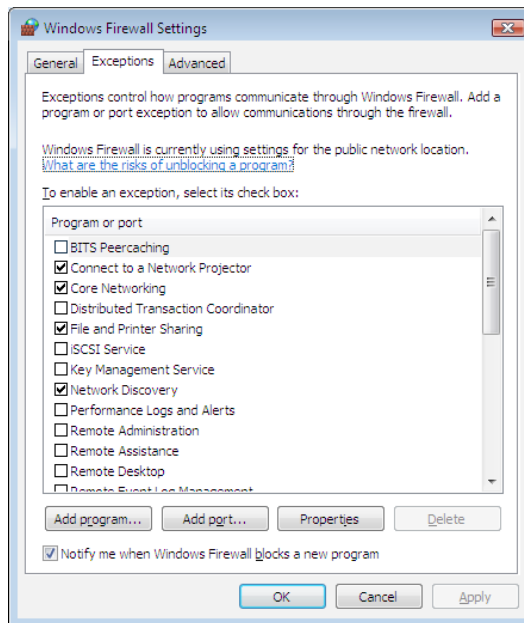
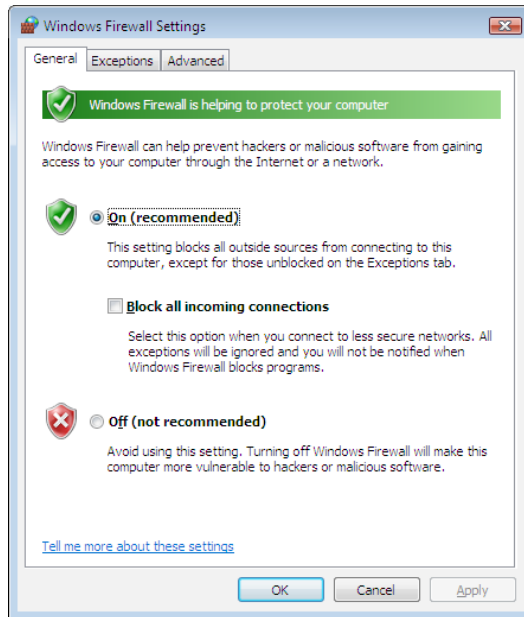
The Vista firewall has two management tools

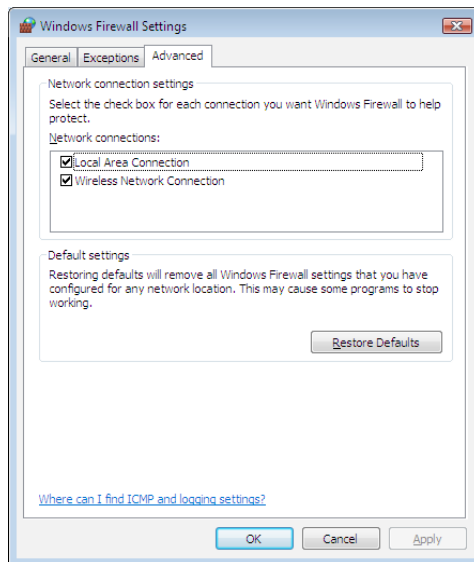
### Windows Firewall in Control Panel



The screenshot below represents a less complex interface with a lot of the more detailed settings not available. Using this interface, you can perform the following tasks:

- Turn the firewall On or Off
- Configure the firewall to admit an external application (perhaps to connect to a web server)
- Block all incoming connects
- Select which network connections the firewall will protect

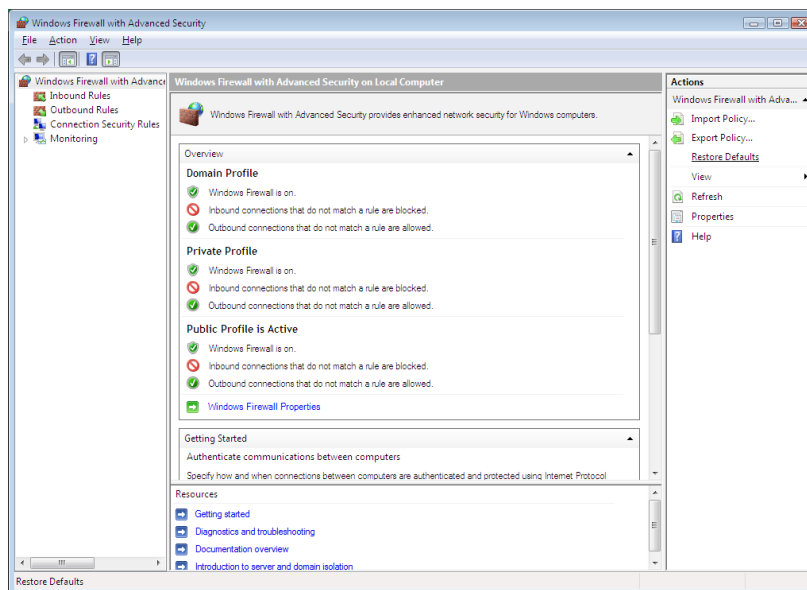




Windows Firewall Tabs

## Windows Firewall with Advanced Security

The screenshot below represents the more complex management tool. It can be accessed from **Control Panel Administrative Tools** or by creating a custom MMC snap-in.



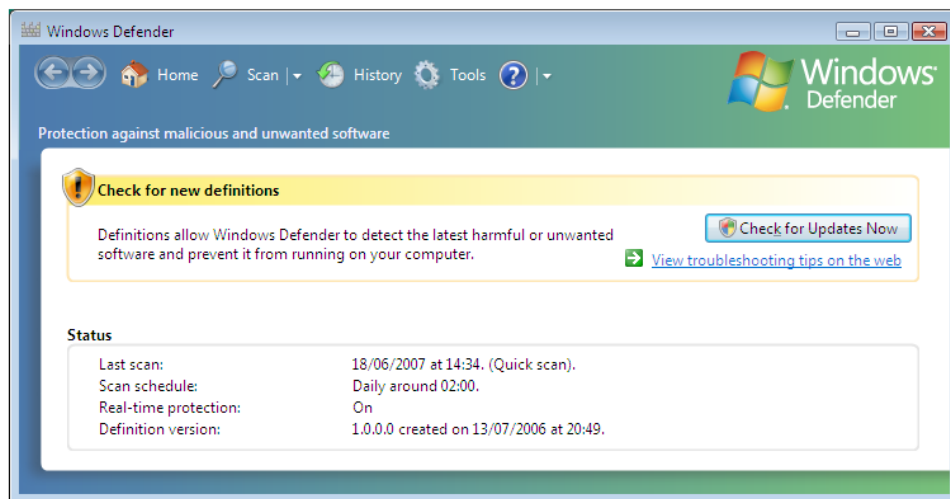
The extra configuration settings available in this console are:

- Import/Export a policy
- Configure the network profiles
- Configure Outbound/Inbound rules
- Configure connection security rules
- View current settings and activities

**Tip:** Firewall settings can be configured by group policy and by the **netsh adv firewall** command.

## Windows Defender

This is Windows Vista's real-time, anti-malware protection system:



Windows defender has a number of agents which monitor parts the system for potentially dangerous activity.

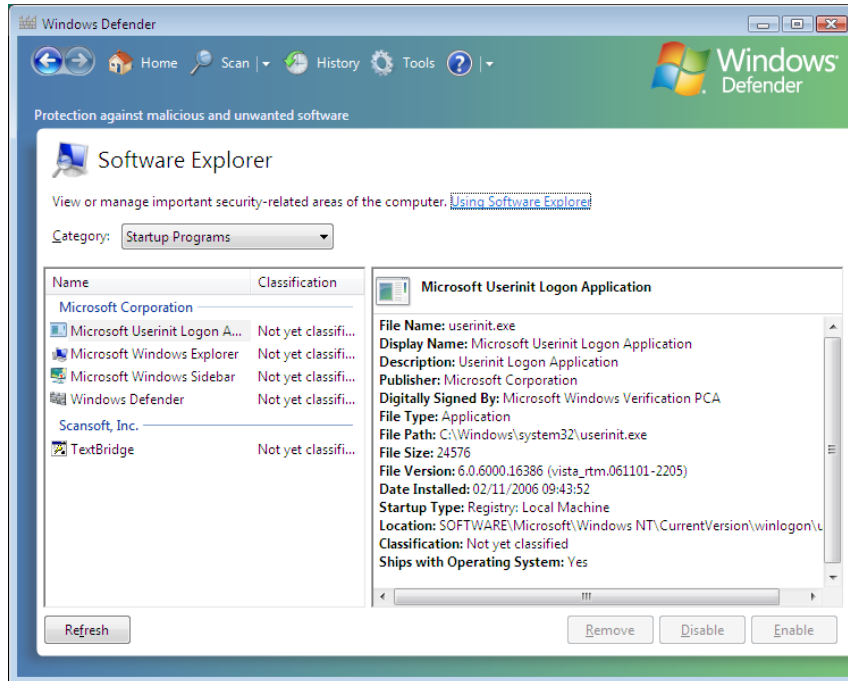
The agents included with Defender are:

Agent	Area Monitored
Auto Start	Programs which start up when Vista boots (can distinguish between the startup folder and registry).
System Configuration	Monitors application attempts to change the configuration of the OS.
Internet Explorer	Defender has three separate agents: <ul style="list-style-type: none"><li>• Add-ons</li><li>• IE configuration</li><li>• Downloads</li></ul>
Services and Drivers	Software that mimics driver or service behavior.
Applications	Two agents: <ul style="list-style-type: none"><li>• Application Registration.</li><li>• Application Execution.</li></ul>
Windows Add-ons	Tools and add-ons.

Windows Defender can be configured to define what actions it takes when an agent detects something suspicious.

## Software Explorer

Found in the **Tools** section of Windows Defender, Software Explorer allows you to examine programs installed on your system.



Software Explorer is capable of reporting on the following:

- Startup programs
- Programs running
- Network-connected programs
- Winsock service provider

Some of the information returned is:

- Auto start
- Startup type
- Shipped with the OS
- Classification (security hazard)
- Digitally signed by

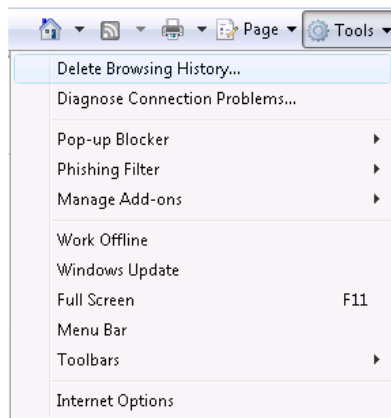
## Internet Explorer (IE)

IE is Microsoft's proprietary web browser and is bundled on just about every version of Windows. The most current version is IE7; however, IE6 is still popular and in use. The last few versions of IE have many features in common. IE7 has made quite a few changes including:

- Tabbed pages
- Pop-up blocker
- Phishing Filter
- Zone setting made more stringent
- "Safe mode" IE can be configured to start without running add-ons or Active-X controls
- RSS Feeds

### Tools menu

As the name implies, this menu provides access to the major configuration tools within IE. There are many more additional tools in IE7:



### Pop-ups

Browser windows that open then you access a web page are called **pop-ups**. They are often attempting to sell you something. Not all pop-ups are stopped by default. For example, if you initiate a pop-up by clicking on a button, then IE7 will allow it.

### Phishing

Extracting confidential information from people is known as **phishing**. One common method is to lure victims to a dummy website which purports to be a legitimate site (such as a bank). Once there, the victims are conned into entering their account details and passwords (usually on the premise of a security breach). The phishing filter in IE7 allows you to perform the following acts:

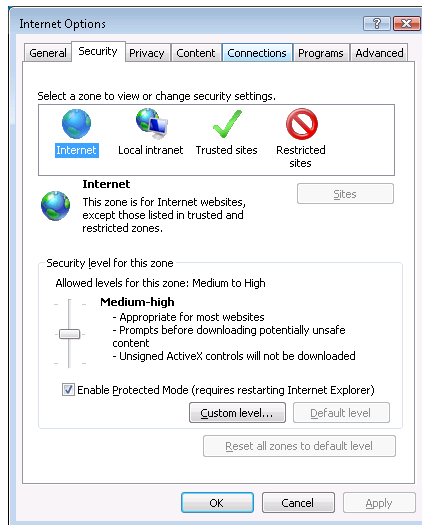
- Ensure the validity of the website
- Turn on/off automatic website checking
- Report this website
- Configure phishing filter settings (which takes you to the **Advanced** tab in **Internet Options**)

## Internet Options

For the purpose of the exam, this section contains most of network configuration that you need to know. Internet options can be accessed two ways:

- From Control Panel
- From the **Tools** menu within IE

Internet Options contain a number of tabs each one with multiple settings ...



### Security tab

The security tab allows you to specify how IE interacts with websites. IE assigns each site to a zone. Each zone has customizable settings which specify what is allowed from websites. For example, you may be happy to run Java from some websites (that you trust) but not from others. You configure your zones with the required behavior then place the sites into the appropriate zone.



Sites are added to a zone as follows:

Zone	Who should go in it	How membership is created
Internet	This is the catch-all zone — any site not located in the other three zones ends up here.	You cannot add sites to the Internet zone. IE assumes every site belongs there if they have not been already allocated to another zone.
Local intranet	Websites on your own internal network	Although you can (on advanced settings), you should not specify this for the site, rather you should specify this zone for the circumstances. For example, in IE7 you can select the following situations: <ul style="list-style-type: none"> <li>• Include all local intranet sites not placed manually in another zone</li> <li>• Include all sites that bypass the proxy server</li> <li>• Include all network paths (UNCs)</li> </ul> The IP address of the site identifies whether it is on the intranet or not. Any site meeting the above requirements is then included in the Local intranet site.
Trusted sites	Sites that you are sure are harmless	You add these manually.
Restricted sites	Sites that you are certain are dangerous	You add these manually.

**Exam Tip:** You add sites to Trusted and Restricted zones **not** the Internet zone.

To make it simpler, Microsoft provides you with a slider for each zone that pre-sets the configuration. The default settings for the zones changed between IE6 and IE7:

Zone	IE7 Setting
Internet	Medium-high
Local intranet	Medium-low
Trusted sites	Medium
Restricted sites	High

**Exam tip:** In IE7 the **Internet zone** will only slide to **Medium** the **Restricted Sites** zone can only be set to **High**.

**Exam tip:** Java and ActiveX are competing technologies which can be used to “push” applications from the website to the local machine via the Web Browser. These applications are then run locally.

ActiveX is Microsoft’s product and only works on Internet Explorer. Java is owned by Sun Microsystems. Many authorities agree that Java is slower than ActiveX, but much more secure: Java runs in an abstracted Java Virtual Machine (JVM) while ActiveX runs directly on the host Operating System (which is why it can be used only on Windows platforms).

Microsoft is attempting to increase popularity for ActiveX and considers that accompanying an ActiveX control with a **digital certificate** provides robust security. Wherever possible in any exam Microsoft will try and sneak in a mention of ActiveX and probably certificates. You add sites to Trusted and Restricted zones **not** the Internet zone.

### Privacy options

Privacy options allow you to configure how IE responds to cookies. Cookies are small text files inserted by a web server onto the browser’s hard disk. They are often used to store membership details and other semi-confidential information.

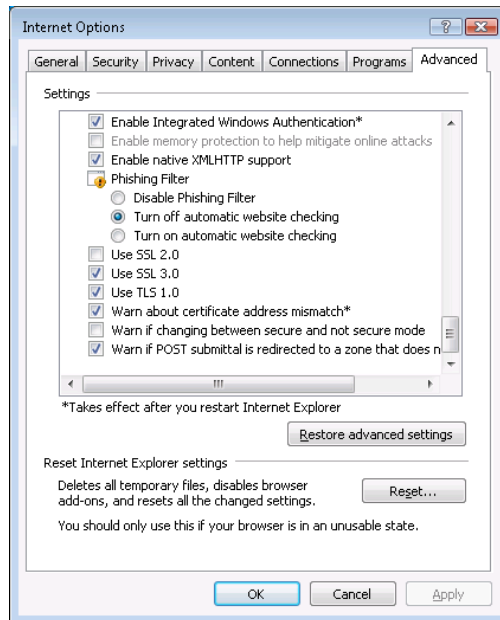
There are several types of cookie:

Cookie	Features
First Party Cookies	Remain on the system but can only be accessed by the application that created them.
Third Party Cookies	Remain on the system but can be accessed by other applications.
Session cookies	Are used only while the session is active, and are then are removed.

You can configure Privacy Options to control how Internet Explorer deals with cookies:

Setting	Action
Block all cookies	No cookies allowed.
High	Blocks all cookies do not have a compact privacy policy. Blocks all cookies that use personally identifiable information without the User’s permission.
Medium high	Blocks all third party cookies that do not have a compact privacy policy. Blocks all cookies that use personally identifiable information without the User’s permission.
Medium	Blocks all third party cookies that do not have a compact privacy policy. Blocks all third party cookies that use personally identifiable information the User’s permission. Restricts First party cookies that use personally identifiable information without the User’s permission.

Low	Restricts all third party cookies that do not have a compact privacy policy. Restricts all third party cookies that use personally identifiable information the User's permission.
Accept all cookies	All cookies allowed.



### The Advanced tab

The **Advanced** tab contains configuration settings that a typical User would not normally need to use. It contains a **Security** section which, among other settings, allows you to configure how IE manages a secure link.

### SSL and TLS

Secure Sockets Layer (SSL) is the most common method of securing communications between a Browser and a Web server. SSL has two current versions: SSL2 and SSL3. On IE6, both are switched in, while IE7 has SSL2 (just about obsolete) switched out.

Transport Layer Security (TLS) is an alternative to SSL which is sometimes used in E-Mail communications. By default IE6 has TLS switched off (while IE7 has is switched on).

## Monitoring Windows Vista

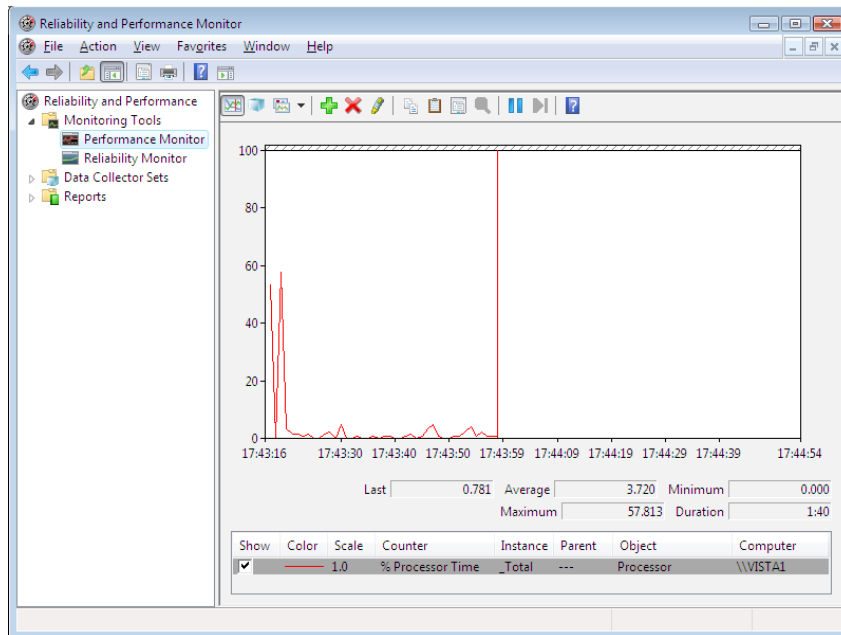
There are a number of tools used to monitor the behavior of Windows Vista:

<b>Tool</b>	<b>Features</b>
<b>Device Manager</b>	Displays driver settings and allows you to resolve driver and driver configuration problems.
<b>Event Viewer</b>	Provides access to, and management of, the Vista event logs.
<b>Performance</b>	Allows you to monitor specific areas of a Vista system.
<b>Task Manager</b>	Displays applications and OS components and allows you to stop them. Displays real time performance indicators based round memory, CPU, and Network activity. In a Workgroup also lists User's logged on.
<b>System Information</b>	Displays configuration settings of Vista and some applications.
<b>Reliability Monitor</b>	Allows you to asses the stability of a Vista system and investigate the causes of instability.
<b>System Properties General Tab</b>	Displays the CPU type, the system memory, and the Service Pack level.

## Reliability and Performance Monitor

Performance monitor has been around since the early days of Windows. Reliability Monitor is new to Windows Vista. Microsoft has installed the pair into one console along with some associated utilities.

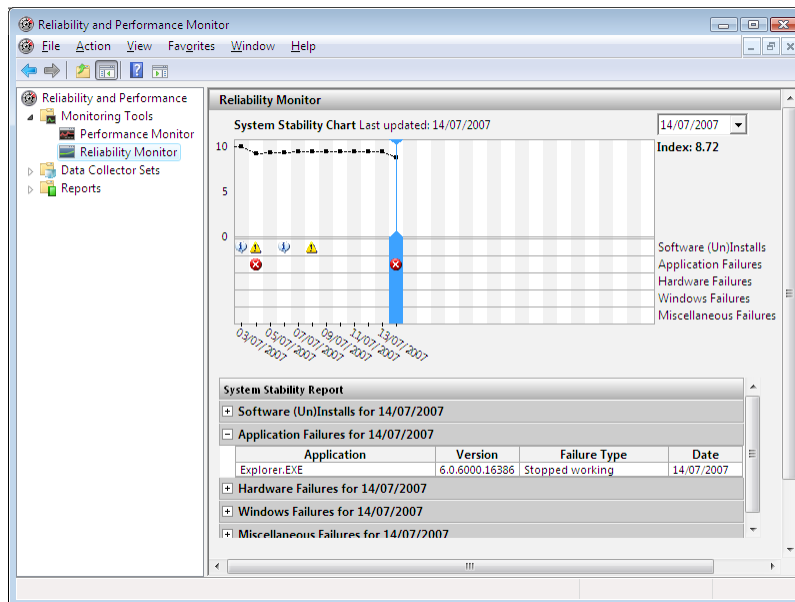
### Performance Monitor



The performance monitor allows you to view the major components (hardware and software) of a Vista system and to monitor how it is working. The performance monitor can monitor in real time or save its output to a file for review later. Performance monitor hinges on **counters** (a facet of the system such as CPU, Hard Disk, TCP etc) and **instances** (if there is more than one).

## Reliability Monitor

This monitor provides an overview of system stability. The reliability monitor will display information about events which it considers may have affected the stability of Windows Vista. From the information gathered, the reliability monitor will work out a **Stability Index** which is displayed on the **System Stability Chart**.



Reliability Monitor uses the following:

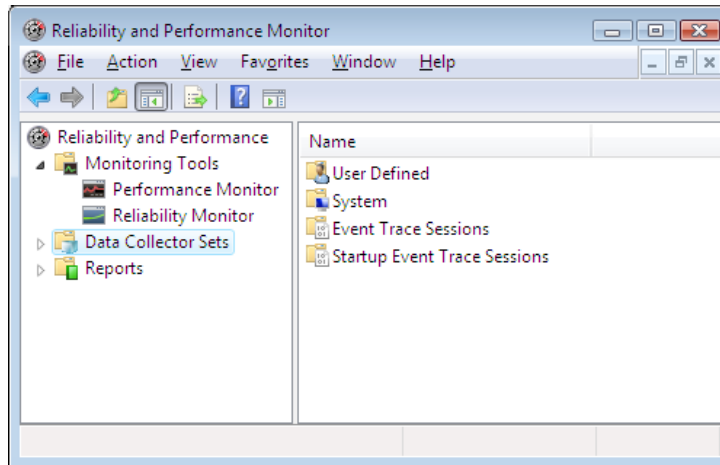
<b>Performance Counters</b>	As used by Performance Monitor.
<b>Event Trace Data</b>	Many parts of the Vista OS include <b>Trace Providers</b> which report system behavior. The reliability monitor can tap these and combine them into a <b>Trace Session</b> if required.
<b>Configuration information</b>	These are registry key settings. The reliability monitor can monitor changes to these keys.

The reliability monitor can only be used with **local data**; in other words, you cannot use it on remote systems. In such a case, you would need to either log onto the remote system directly or use the **Remote Desktop** or **Remote Assistance** features built into Windows Vista.

## Data collector sets

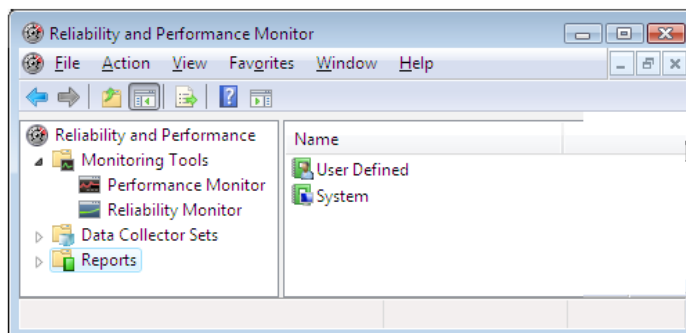
A data collector set is the fundamental monitoring block used in Windows Vista. A data collector set may consist of a combination of any of the following:

- Event trace data
- Performance counters
- System configuration settings such as registry key settings



Data collector sets can be viewed with the performance monitor and/or used to trigger alerts. Microsoft assumes that 3<sup>rd</sup> Party programs will be written to make use of the information provided by Data Collector Sets. Data collection can also be scheduled so that reading takes place at an appropriate time. The configuration for a Data Collector Sets can be held in a **template**, which, like most files in Windows Vista, uses an XML format (Office 2007 uses the DOCX format for XML). Templates can be imported and exported between systems. Vista provides some templates ready for use.

## Reports



The reports feature of the Reliability and Performance Monitor provide you with feedback.

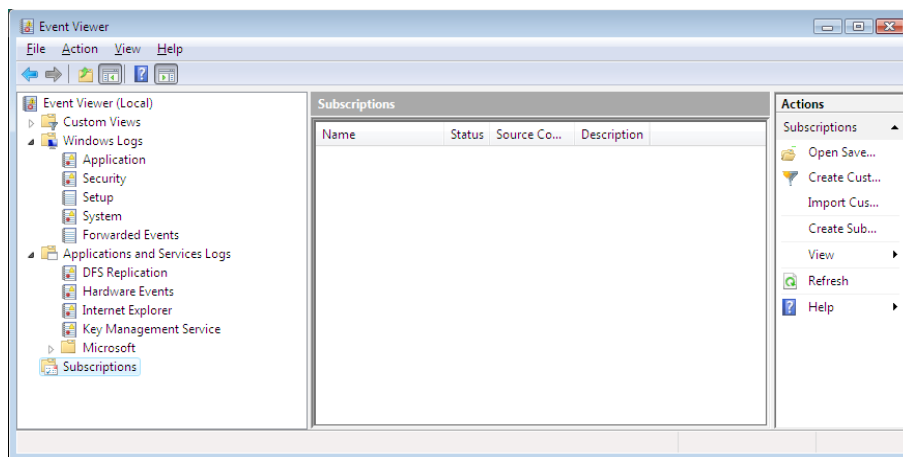
The following are the pre-configured system reports:

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

You may also create your own.

## Event Logs

Event Logs record information about **events** (activities and actions) which occur in the Operating System and the applications running on it. Event logs can be viewed and managed using the **Event Viewer** utility. Drastic changes have been made to the event log system in Windows Vista.



There are now more log types plus the ability to record events directly from multiple computers (**subscriptions**). Event viewer allows you to create re-useable custom views displaying filtered information. Event Viewer can be used in combination with the Windows Task Scheduler so that you can configure the system to run a specific task when an event occurs (**alt-click** on the event to configure this).



## Types of Event Logs

Event logs are divided into two sections:

- Windows Logs
- Applications and Services Logs

### Windows Logs

<b>Application</b>	Applications and programs including some Windows events (such as group policy).
<b>Security</b>	Audited events set with the Local Group Policy.
<b>Setup</b>	Application installation.
<b>System</b>	OS events such as service or driver failure.
<b>Forwarded Events</b>	Events forwarded from other computers (see Event Forwarding).

### Applications and Services Logs

These are new to Windows Vista and have been included to provide a more detailed reporting system to aid in trouble-shooting. The default logs are:

<b>DFS Encryption</b>	<b>Key Management Service</b>
<b>Encrypting File System</b>	<b>Microsoft</b>
<b>Function Discovery Provider Host Service</b>	<b>Microsoft Windows Performance Diagnostic Provider</b>
<b>Hardware events</b>	<b>Microsoft Windows Services Svchost Performance diagnostic Provider</b>

Each of these logs can contain up to four categories:

<b>Admin</b>	Contain proved solutions to a problem
<b>Operational</b>	Can be used in trouble-shooting
<b>Analytic</b>	Issues with cannot be solved by the user
<b>Debug</b>	Debug data for programmers

## Managing Event logs

You can:

- Filter (select which events to display)
- Set the log size
- Backup and/or clear the log
- Set a Retention Policy
- View saved logs
- Forward events

Management is performed by **Event Viewer** from the GUI or the **wevtutil.exe** command line tool.

### Exam Tip: Saving Event Logs.

*Logs can be saved in several formats:*

- ▶ *.evtx (replaces the previous .evt now in xml format)*
- ▶ *.xml (XML file)*
- ▶ *.txt (Tab delimited text)*
- ▶ *.csv (Comma delimited text)*

*You cannot save directly to a database but you can use .csv to transfer.*

*.txt and .csv do not save the hexadecimal event data.*

### Retention Policy

The retention policy defines what happens when a log file becomes full:

Policy	description
Overwrite events as needed	A new event will overwrite the oldest event held in the log.
Archive the log when full, do not overwrite events	The log is automatically archived. No events are lost.
Do not overwrite events. (Clear logs manually)	New events are not recorded until the log is manually cleared.

## Event Subscriptions

Event viewer can work with the event logs of other computers. You can connect to a second computer directly, or arrange for the logs to be forwarded, in which case it is possible to collate events from several computers simultaneously. Event forwarding relies on two services which must both be running on all computers involved in the process:

- Windows Remote Management (WinRM) service.
- Windows Event Collector (Wecsvc) service.

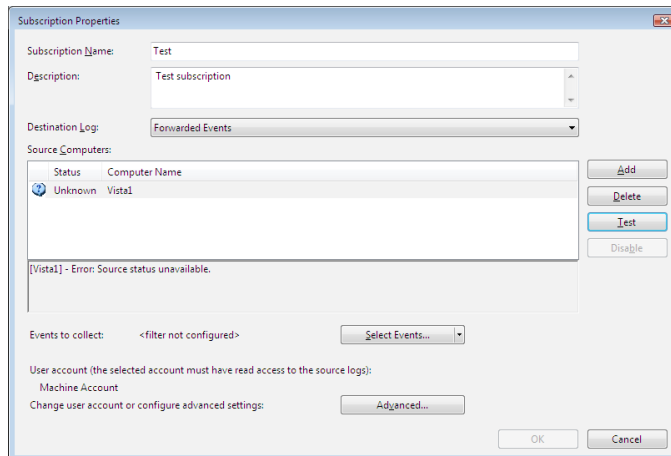
Event Forwarding uses **subscriptions** to configure the process, a number of **source** computers which forward events, and a **collector** computer to hold them. Needless to say, administrator privileges are required on all participating computers.

### To configure computers for Event Forwarding

- Add the collector computer's account into the Local Admins group of each source computer.
- On each source computer run **winrm quickconfig**.
- On each source computer run **wecutil qc**.

### To configure subscriptions

- On the **collector** click **Subscriptions** in Event Viewer.
- On the **Actions** menu select **Add Subscription**.

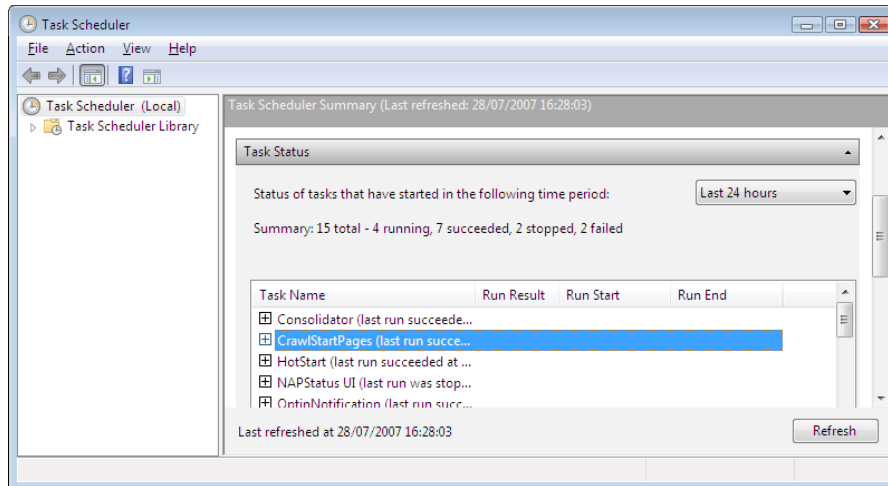


- Fill in the settings box, providing collection system details and the events required.

**Note:** It is not possible to create a subscription while Event viewer is connected to a remote computer.

## Task Scheduler

The Task Scheduler allows you to create pre-configured **Tasks** (a string of instructions or applications) which Windows Vista will run at a pre-determined time.



Tasks can be created on your own or another networked Vista system.

A Task consists of the following:

Triggers	<p>Start the task. Triggers can be:</p> <ul style="list-style-type: none"> <li>• A schedule</li> <li>• At startup or Logon</li> <li>• At connection/disconnection of a user session</li> <li>• Workstation Lock/Unlock</li> <li>• When the computer is idle</li> <li>• When an event is logged</li> <li>• At task creation/Modification</li> </ul>
Actions	<p>The “payload” for the task. There are three categories:</p> <ul style="list-style-type: none"> <li>• Start a program (an EXE file for example)</li> <li>• Send an E-Mail</li> <li>• Display a message</li> </ul>

Conditions	<p>Modify the trigger. Some examples include:</p> <ul style="list-style-type: none"> <li>• Only allows the task to start or continue to run if it is idle (which can be specified)</li> <li>• Only run if powered on AC (Mains)</li> <li>• Only run a task if there is a network connection</li> <li>• Bring the system out of standby to run the task</li> </ul>
Settings	<p>Provides additional controls:</p> <ul style="list-style-type: none"> <li>• Allow the task to run on demand</li> <li>• If a schedule is missed run the task asap</li> <li>• Stop the task if it runs longer than a specified period</li> <li>• Restart the task a number of times if it fails</li> </ul>

## Schedules

Tasks can be set to run:

- Daily
- Every n days
- Weekly
- Monthly
- Once only
- At logon
- At start up
- When a specific event is logged

Repeating jobs can have start and end dates configured and the time to start.

## BitLocker

**BitLocker** is a low-level disk encryption system which works at the sector level. Once started, BitLocker acts invisibly to the User, so there is no need to set individual encryption, as in EFS; for example:

- BitLocker works at a low level in the kernel so it is transparent to most applications (however, Microsoft has written hooks so that other applications can make use of the service).
- BitLocker uses a secured hardware module to hold the primary encryption keys (there are several types of keys).

The module can be one of the following:

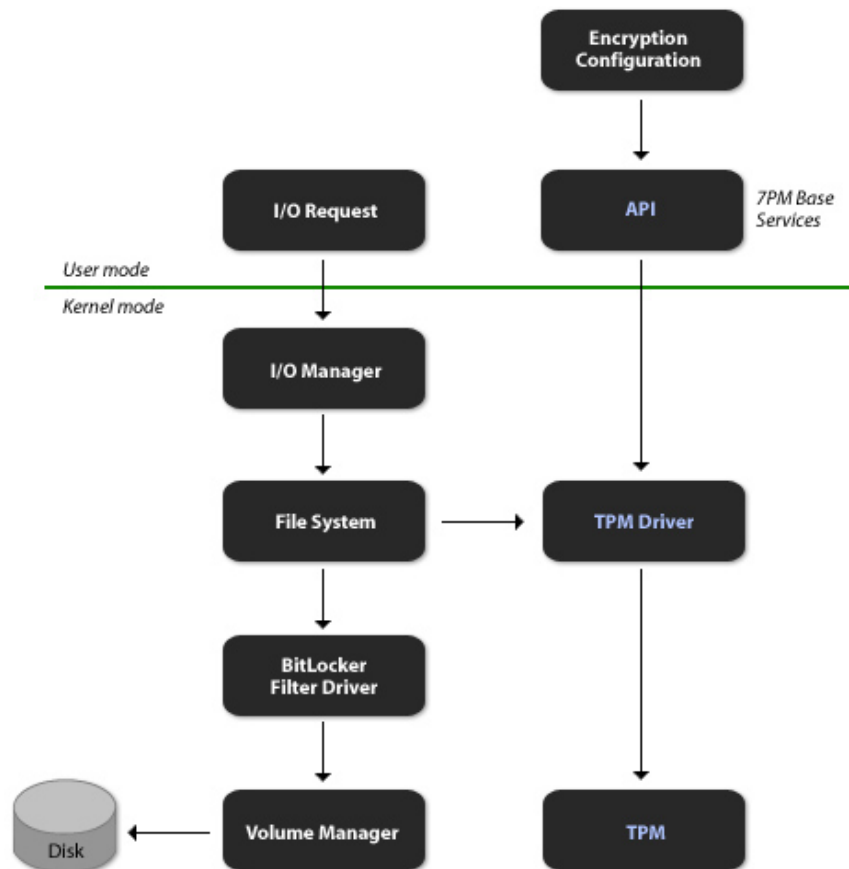
Technology	Details
Trusted Platform Module (TPM)	<p>A TPM is a dedicated security module integrated onto the motherboard. Vista is compatible with TPM version 1.2 or later. The TPM handles a number of security features notably:</p> <ul style="list-style-type: none"><li>• Key generation</li><li>• Secure key storage</li></ul>
USB memory pen	<p>In practice, BitLocker's key system works differently by using a USB pen. For one thing, the keys are generated from within Vista. The USB pen must be inserted before Vista starts and the PC Hardware must have the capability to access it without the aid of an OS.</p>

**Exam Tip:** *BitLocker only encrypt the partition containing the OS other partitions should be formatted with NTFS and secured with EFS.*

#### **Additional security**

It is possible to configure BitLocker to require a PIN number before commencing booting or to require a key protector held on a USB memory device. Both of these methods represent additional security preventing unauthorized access. If using USB, then care must be taken not to leave the USB device with the computer.

The BitLocker system can be represented as follows:



BitLocker block diagram

### Encryption system

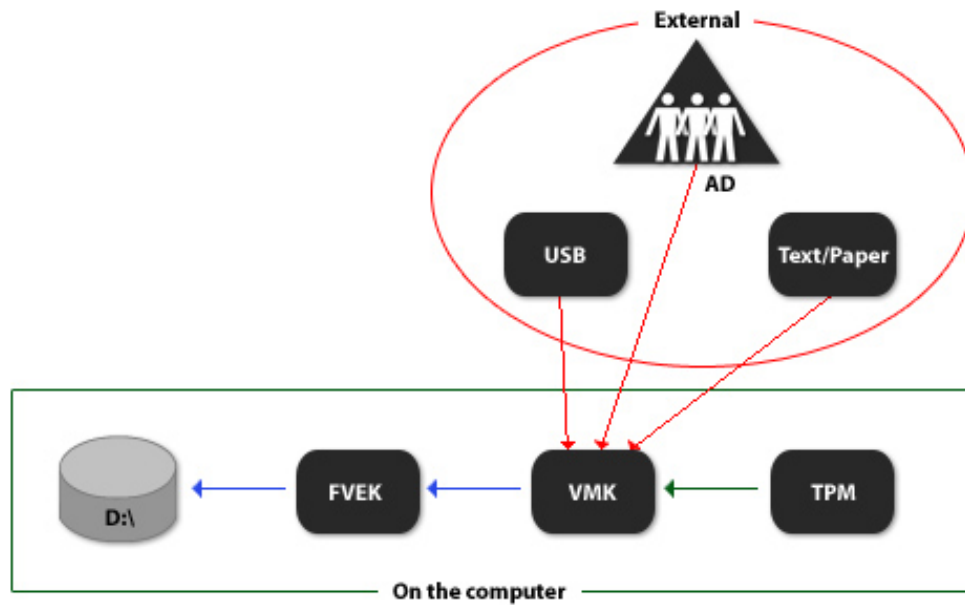
BitLocker works at the drive level and at the first release of Vista will only encrypt the **Windows OS Volume** (the new term for the Boot Partition). BitLocker encrypts each sector independently using an encryption mechanism based on the **Advanced Encryption Standard (AES)** with a 512 bit key length.

Each sector on the drive is partially encrypted using the **Full Volume Encryption Key (FVEK)**. Ultimately, to regain the data, you need to be able to read the FVEK which will allow you to read any sector on that drive (permissions willing). The FVEK is held on the disk itself. To protect the FVEK it is encrypted with a second key known as the **Volume Master Key (VMK)**.

The VMK is also held on the disk and again is encrypted (known as **Key Protectors**); however, in this case, the VMK can be encrypted several times with different algorithms. If you can access just one of these algorithms, then you can decode the VMK. This, in turn, will allow you to decode the FVEK, which will let BitLocker decrypt the data on the disk.

Key protectors can be held in different locations:

- The TPM
- A USP Memory pen
- Active Directory
- Text file
- Paper (ie write it down and lock it away)



**How disks are encrypted using BitLocker**

The advantages of this arrangement are as follows:

- Vista can use the key protector in the TPM to automatically “unlock the disk”.
- If the computer’s motherboard fails, then the encrypted disk can be connected to a replacement; however, the TPM key protector will be missing. In this case, one of the external key protectors are applied and then the VMK is encrypted using the new TPM, so that the system runs automatically in the future.
- If a key protector becomes compromised, all the data is at risk; however, in this case, all that is needed is to generate a new VMK, encrypt the FVEK with this, create new key protectors then delete the old VMK. The drive is once more secure. This is less time consuming than re-encrypting each sector.



To decrypt the VMK you need a functioning TPM or a USB alternative on the computer. If the system cannot decrypt the VMK, then you will need to **recover** it manually. The recovery system circumvents the TPM/USB with an external alternative such as Active Directory, paper, file, or another USB device. Circumstances when this may be necessary are:

- You have re-housed a BitLocker encrypted drive to another Vista system.
- The TPM is faulty or has been replaced (typically by replacing the motherboard it is soldered on to).
- The TPM has been cleared or re-set.
- You have configured to use a start-up PIN with BitLocker and have forgotten it.
- You are using a USB memory pen which you have lost or has become faulty.
- You have changed critical hardware or modified boot components which has caused the “fingerprinting” system to fail (this system is described later in this section).

If BitLocker cannot access the VMK, then it will start up the **Disaster Recovery Console**, which allows you to supply the recovery key. If entering the data manually, then you will use the function keys on the keyboard. F1-F9 represents the number 1 to 9 and F10 represents 0.

### Active Directory and BitLocker

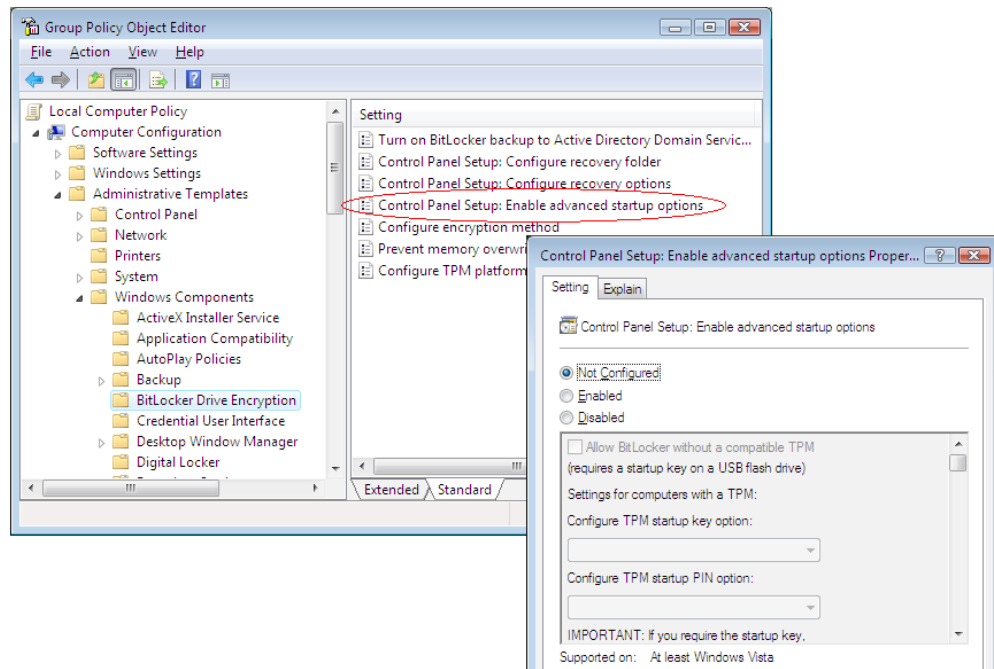
Group Policy can be used to control the recovery methods available to Users. You can also use the **Require BitLocker Backup to AD DS** Group Policy setting. This policy does not allow BitLocker encryption to be configured unless a system is in contact with Active Directory. The recovery keys are then automatically stored in the AD database. Unfortunately, to recover them, you will need to resort to LDAP commands as the GUI has no method of accessing them at present. You also need to extend the AD schema. As an alternative, you may also create a Policy to set the default save location for recovery keys to a shared folder.

### Supporting BitLocker on systems without a TPM

Vista will work on computers without a compatible TPM. In this case, an external recovery key on a USB pen will be necessary. As this is accessed before Vista starts, it will be necessary to configure the BIOS to work with USB memory devices.

By default, the option to use BitLocker is not made available if a TPM is not present.

This feature may be activated by changing a local policy setting:



To set this open the group policy, navigate to **Local Computer Policy > Administrative Templates > Windows Components > BitLocker Drive Encryption > Control Panel Setup: Enable Advanced Setup Options**. Set the **Setup Wizard Configure** startup option for TPM computers to **Enabled** and **Allow BitLocker without a compatible TPM**.

## Boot Process Integrity Check

Vista splits the files needed to start it up into two portions:

- Files the BIOS uses to select a version of Windows including Vista (the **Start-up** files)
- The actual files to start up that version of Windows (the **Boot** files)

The drive holding each of the groups is given a special name by Microsoft: **Active Partition** (for the start-up files) and **Windows OS Partition** (for Vista's files proper). Usually, Windows Vista will install to a single partition with both sets of files on the C:\ drive; however, this situation is not acceptable when implementing BitLocker. This is because BitLocker runs from within Vista proper: the start-up process cannot handle the encrypted sectors. So, to implement BitLocker, you need to separate the two groups of files onto two partitions.

For example:

C:\ is active and holds the **start-up** files and is not encrypted by BitLocker.

D:\ holds the Vista boot files and is encrypted by BitLocker.

If using a TPM, BitLocker can provide some protection to the start-up files. The TPM specification provides for 24 **platform control registers** (PCRs) although only 11 are in current use. Each PCR can be used to hold a “fingerprint” of a critical part of the OS. The fingerprint is created by the TPM firmware. The PCRs are used as follows:

PCR	Fingerprints
0.	BIOS and BIOS extensions
1.	Platform and Motherboard configuration and data
2.	Option ROM code
3.	Option ROM Configuration and Data
4.	Master Boot Record (Disk) code
5.	Partition Table (Disk)
6.	State Transition and Wake events
7.	Computer Manufacturer Specific
8.	NTFS Boot Sector
9.	NTFS Boot Block
10.	Boot Manager
11.	BitLocker Access Control

Each time the computer boots, the TPM recalculates each fingerprint and compares it with the stored value. The default setting of BitLocker checks for changes on PCR 0, 2, 4, and 8-11; however, this can be modified.

This allows BitLocker to monitor the start-up files and what Microsoft refers to as the “pre-boot environment”; making it possible to detect malicious code which runs “under” the OS proper (such as a Root Toolkit). Unfortunately, some hardware and configuration changes may also amend the fingerprint.

## Implementing BitLocker

### Hardware requirements

#### Key storage

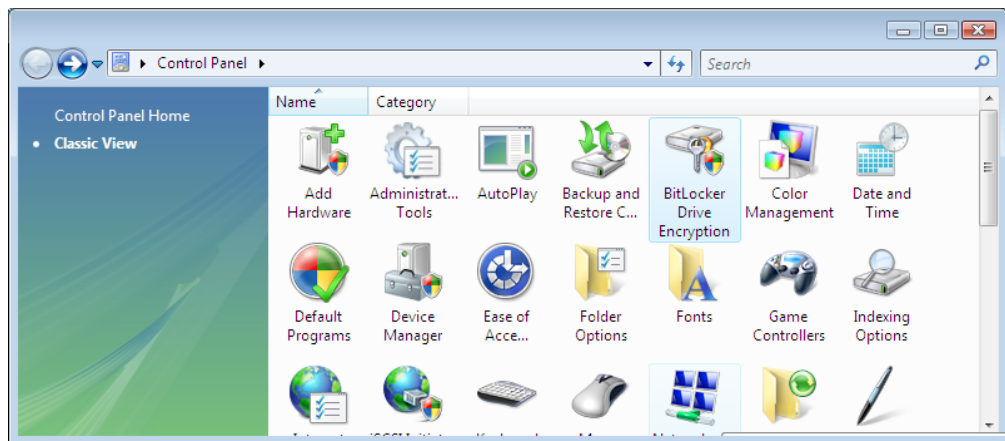
The computer must have Trusted Platform Module (TPM), version 1.2 or higher, or a removable USB memory device, such as a USB memory pen. The BIOS must be capable of supporting the TPM device if you use it or supports USB devices during computer startup.

#### Disk configuration

You will need to place the Active and the Windows OS Partitions on separate drives, each formatted with NTFS. The Active Partition will remain un-encrypted while the Windows OS Partition will be managed by BitLocker.

### Managing

BitLocker is managed from Control Panel | BitLocker:



**BitLocker controls**

From here you can:

- Create new Key protectors
- Turn off/Turn on BitLocker
- Disable/Enable BitLocker

<b>Turning off</b>	All sectors are decrypted (time consuming).
<b>Disabling</b>	The VMK is stored on the disk in plaintext. As it is not encrypted, the TPM and/or key protector are not required. Disabling is a quick process that should be performed before working on the installation (such as changing the Motherboard or working on the Vista files on the Active Partition or modifying the BIOS).

## Vista Networking

### GUI enhancements

- My Network Places has been replaced by the Network Sharing Center
- Improved diagnostic tools
  - Network Diagnostic Framework
  - Network Map
- Network Profiles (security settings)
- Network Explorer

### Network Protocols added

- TCP/IP stack re-written and self tuning
- Native support for IPv6 (as well as IPv4)
- Link Layer Topology Discovery (LLTD) allows devices to discover each other on the network
- L2TP (Layer 2 Transport Protocol) additions
  - AES encryption supported with 128/192/256 bit keys
  - IKE (Internet Key Exchange) strengthened including support for Diffie-Hellman 256/348 bit keys
  - NAT (Network Address Translation) traversal for both IP4 and IP6

## Network Protocols removed

- NetBEUI
- Services for Mac
- IPX (InterPacket Exchange)/NWLink
- SLIP (Serial Line Interface Protocol)
- BAP (Bandwidth Allocation Protocol)
- PPTP (Point to Point Tunnelling Protocol) changes
  - MS-CHAP v1 not supported
  - RC4 40 and 56 bit no longer supported
- L2TP/IPSec (IP Security) changes
  - DES (Data Encryption System)/MD5 (Message Digest 5) no longer supported

## Other features

- Improved Firewall
- Improved support for Wireless networks

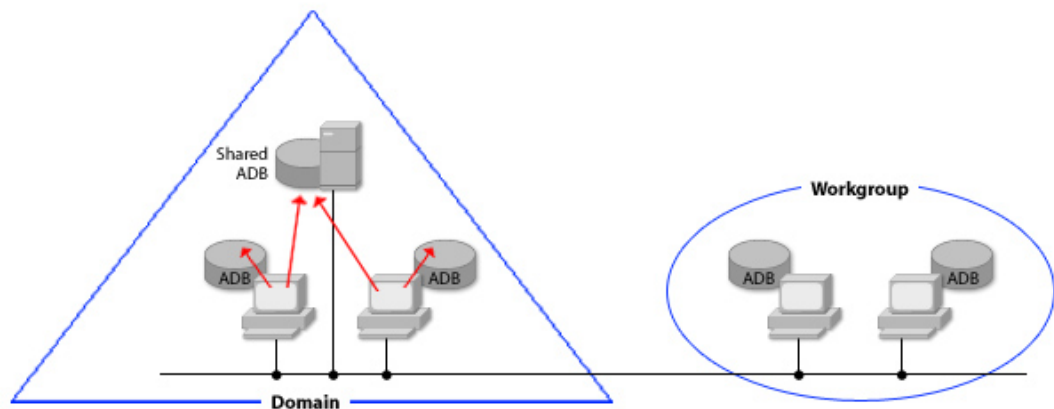
## Workgroups and Domains

Microsoft uses two security models:

- Workgroup
- Domain

It is important to understand that both Workgroups and Domains are security structures which are superimposed on the network itself. In the following diagram, all the computers are members of the same network and each can see every other computer; however, the computers have been logically divided into the two security groups.

One is a domain while the other is a Workgroup.



**A Domain and a Workgroup sharing a single LAN**

For the exam, the main differences to consider between the Domain and Workgroup models are where accounts can be obtained for ACLs, who has Administrative authority over a system, and where Group Policies can be applied:

Workgroup features	<ul style="list-style-type: none"> <li>• Each system uses its own accounts database exclusively.</li> <li>• The only group policy which can be applied is the Local Group Policy.</li> <li>• Members of the Local Administrators Group (a Local Group) have full control over their system.</li> </ul>
Domain Features	<ul style="list-style-type: none"> <li>• Each Vista system can use its own Local Account Database or the shared domain accounts database.</li> <li>• Group Policies can be “pushed down” from the Domain, OU, or site.</li> <li>• Domain Administrators are made members of the Local Administrators group on every domain member computer.</li> </ul>

## Authentication problems

If a domain user has trouble logging onto a system, then check that they are selecting the domain database to be validated against.

In Active Directory domains, DNS is used by domain computers to locate the Domain Controllers (the Servers which host the shared domain accounts database). Each member of the Domain needs to be configured with the IP address of their DNS Server. This can be either from DHCP (Dynamic Host Configuration Protocol — a method of providing IP configuration automatically to IP based systems) or by manual configuration.

## Basic TCP/IP

To be connected using TCP/IP, a computer needs:

- An IP address
- A subnet mask

To allow routing to the Internet, or to a different subnet, a system will also require the default gateway setting to be configured.

## IP Version 6

Windows Vista supports a native IPv6 protocol stack.

IPv6 is a 128 bit addressing scheme with the address configured in hex mode. A typical IPv6 address looks like this:

```
4DFE:897A:0000:3BC4:3458:D98E:00B9:1DA3
```

Leading zeros can be omitted, as well:

```
4DFE:897A:0:3BC4:3458:D98E:B9:1DA3
```

Windows Vista can use **IP Tunneling** allowing IPv6 to traverse IPv4 networks.

## Network Services

### DNS

The Domain Name Service is a system which converts a URL, such as `www.Myco.com` into an IP address, such as `160.40.199.120`

### WINS

The Windows Internet Name Service converts NetBIOS names to IP addresses. NetBIOS is an old naming scheme used in previous versions of Windows and maintained for backward compatibility. Microsoft suggests that NetBIOS and WINS are not needed with networks composed solely of Windows 2000 systems and above.

### DHCP

Dynamic Host Configuration Protocol is a method of automatically assigning IP configuration settings to clients that need them. By default, Windows Vista is configured to run as a DHCP client. If no DHCP server is available, then Vista will make up its own IP address, which will begin with `169.254` and have a subnet mask of `255.255.0.0` and no Default Gateway. This system, known as APIPA (Automatic Private IP Addressing) is important to know for the exam.

Vista allows you to create a “fallback” set of IP configuration data which it will use if it is configured as a DHCP client, but there is no DHCP server available. This is known as an “Alternative IP Address” and is used **instead** of the APIPA auto-generated one.

The DHCP client is managed by a dedicated Windows Vista service.



**NAT**

Network Address Translation is used to convert private IP addresses used on an Internal LAN into an address that can traverse the Internet. NAT is normally performed at your Firewall/Router.

The private ranges for IPv4 are:

Class	Reserved Network Address	Mask
A	10.0.0.0 to 10.255.255.255	255.0.0.0 (/8)
B	172.16.0.0 to 172.31.255.255	255.255.0.0 (/16)
C	192.168.0.0 to 192.168.255.255	255.255.255.0 (/24)

In IPv6, anything starting with FE80 is regarded as a private address.

**Proxying**

Proxying is normally used with web browsers such as Internet Explorer 7. A proxy obtains data on behalf of a client, instead of the client going to the server directly.

**Firewall**

A router with built in intelligence which examines packets flowing through it stopping ones that do not meet its rules.

**Testing and Troubleshooting IP****IPCONFIG**

Provides a configuration report on how IP is configured on that system:

```

C:\Windows\system32\cmd.exe
C:\Users\test>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::8541:5473:cb2:6538%8
    IPv4 Address. . . . . : 192.168.0.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Tunnel adapter Local Area Connection* 6:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::5efe:192.168.0.1%9
    Default Gateway . . . . . : 

Tunnel adapter Local Area Connection* 7:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\Users\test>

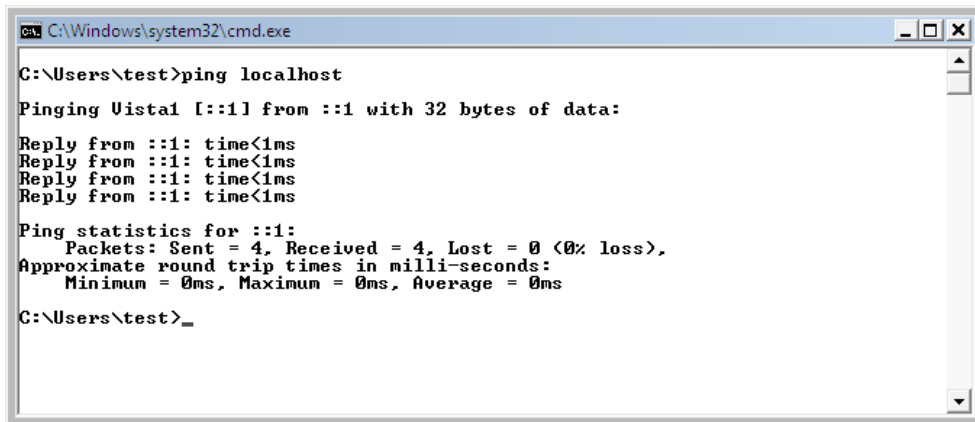
```

A number of switches can be used with IPConfig:

Command	Provides
<b>IPCONFIG</b>	Displays basic settings.
<b>IPCONFIG /ALL</b>	A more detailed listing, including DNS server and the MAC address; however, there is a quirk in IPCONFIG /ALL such that if a WINS server is <b>not</b> configured, then it does not include a WINS entry at all.
<b>IPCONFIG /Release</b>	Instructs IP to drop a DHCP lease.
<b>IPCONFIG /Renew</b>	Instructs IP to attempt to obtain a new DHCP lease.
<b>IPCONFIG /RegisterDNS</b>	Instructs IP to attempt to register the computer's DNS name with its configured DNS Server.
<b>IPCONFIG /FlushDNS</b>	Empties the local DNS cache (including negative registrations).

### Ping

Ping is a simple test that “bounces” a packet off another host - you can specify the destination by IP address or Hostname.



```
C:\Windows\system32\cmd.exe

C:\Users\test>ping localhost

Pinging Uistal [::1] from ::1 with 32 bytes of data:

Reply from ::1: time<1ms
Reply from ::1: time<1ms
Reply from ::1: time<1ms
Reply from ::1: time<1ms

Ping statistics for ::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\test>
```

### To test a TCP/IP configuration by using the ping command

- At the command prompt, ping the loopback address by typing 127.0.0.1.
- If the ping command fails, verify that the computer was restarted after TCP/IP was installed and configured.
- Ping the IP address (eg "PING 200.200.200.200").
- If the ping command fails, verify that the computer was restarted after TCP/IP was installed and configured.
- Ping the IP address of the default gateway.
- If the ping command fails, verify that the default gateway IP address is correct and that the gateway (router) is operational.
- Ping the IP address of any remote host (a host that is on a different subnet).
- If the ping command fails, verify that the remote host IP address is correct, that the remote host is operational, and that all the gateways (routers) between this computer and the remote host are operational. (Note: The Default Gateway address must be on the same subnet as the Host computer.)
- Ping the IP address of the DNS server.
- If the ping command fails, verify that the DNS server IP address is correct, that the DNS server is operational, and that all the gateways (routers) between this computer and the DNS server are operational.
- Ping the FQDN of the DNS server (FQDN= Fully Qualified Domain Name eg Server.myco.local).
- If the ping command fails then suspect a DNS resolution failure - check that a record exists on the DNS server and that requests can be properly referred.

### Tracert

Traces the route between two systems identifying the router passed at each stage.

### PathPing

A combination of Tracert and Ping.

### NetStat

Network statistics allows you to see which ports are active. Ports identify actual applications on a computer, while the IP address identifies the computer itself. When a service (such as a web server) starts up, it requests to use a **Well Known Port**. Client software expects to find the server on this port meaning the user just has to identify the computer by either DNS name or IP address. As an example, the Well Known Port for HTTP (used in the Web) is port 80. When you start up your web browser and tell it to connect to [www.microsoft.com](http://www.microsoft.com) this DNS name is first resolved into an IP address. Your client then connects to that address and sends a request to the application using Port 80.

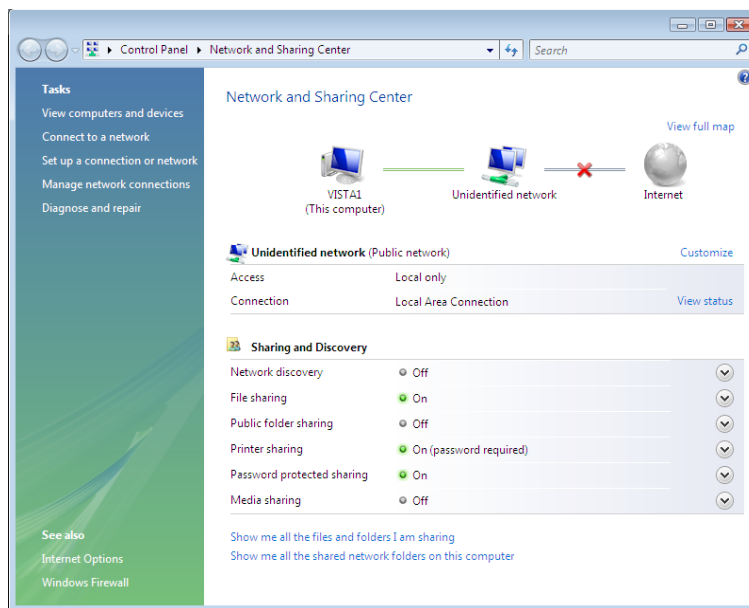
Some well known ports you should be aware of for the exam are:

Application	port
FTP (File Transfer Protocol)	20/21
SMTP (Simple Mail Transport Protocol)	25
HTTP (Hyper Text Transport Protocol)	80

### NBTStat

NBT statistics lets you investigate NetBIOS resolution on a system. You may use NBTStat -RR to register with a WINS Server and NBTStat -c to view the NetBIOS cache.

## Network and Sharing Center



The **Network Sharing Center** is the replacement for **My Network Places** and is the main network management interface within the Vista GUI. Just about everything you need is here.

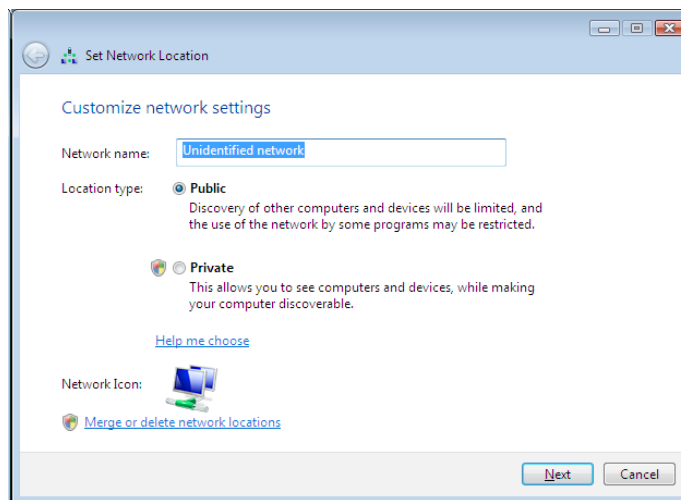
The right hand pane displays a stylized legend of how your system is connected, as well as the state of major networking features (such as **Network Discovery** and **File Sharing**).

## Network Profile

The features are set by the **Network Profile** in use. A profile consists on a set of Windows Firewall rules which allow or deny certain network features. The less features allowed, the more secure the computer is from attack; however, the more restrictions in place reduces the effective use of the profile. Home users require a different restriction set when compared to business users on a domain.

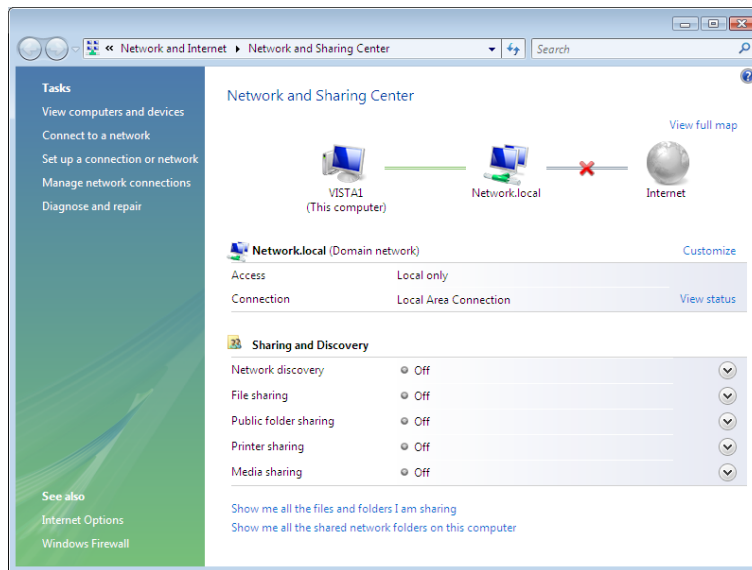
Vista attempts to automatically optimize the allowed feature set by means of three profiles:

Profile	Details
<b>Public</b>	The most restrictive setting (and the one selected by Vista "if in doubt"). Basically, simple Internet connectivity is allowed (HTTP, SMTP, DNS, POP3, and RDP). All sharing and discovery is disabled.
<b>Private</b>	An Administrator has to manually change the Public to Private use this if on a secure network only.
<b>Domain</b>	If Vista is a member of a Domain then it will select this profile automatically. Network components needed to communicate in a commercial environment will be enabled.



Changing between Public and Private Network Profiles

You have some control over the options within the Network Sharing Center:



**Network Sharing Center on a Domain Member**

For other options, you need to adjust the Windows Firewall.

### Options available on each profile

Profile	Network Discovery	File Sharing	Public Folder Sharing	Printer Sharing	Password protected sharing	Media sharing
<b>Public</b>	Off	On	Off	Off	On	Off
<b>Private</b>	Off	On	Off	Off	On	Off
<b>Domain</b>	Off	Off	Off	Off	N/A	Off

### Profile selection

An administrator can switch between the public and the private profile. If Vista selects the domain profile, however, that cannot be changed.

Only one profile can be selected at any given time. Vista attempts to automatically assign a profile based on the network characteristics. If in doubt, it uses the public profile, which is the most stringent (therefore, the most secure).

According to Microsoft, the algorithm works this way:

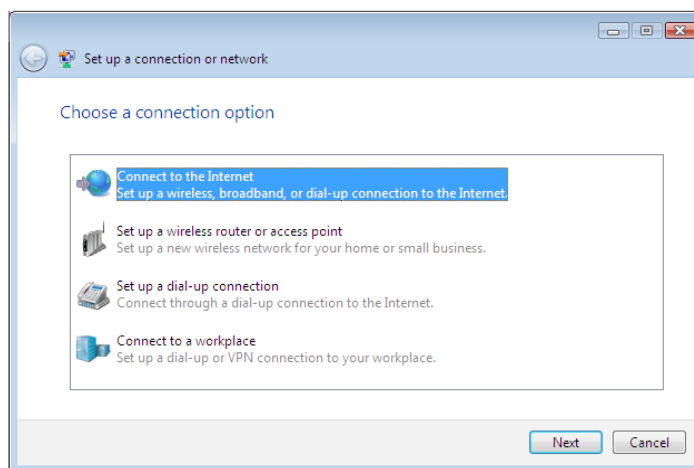
- If any network interface is evaluated as a public network use the public network profile
- If all available networks are evaluated as being private use the private network profile
- If all available networks are evaluated as being domain use the domain network profile

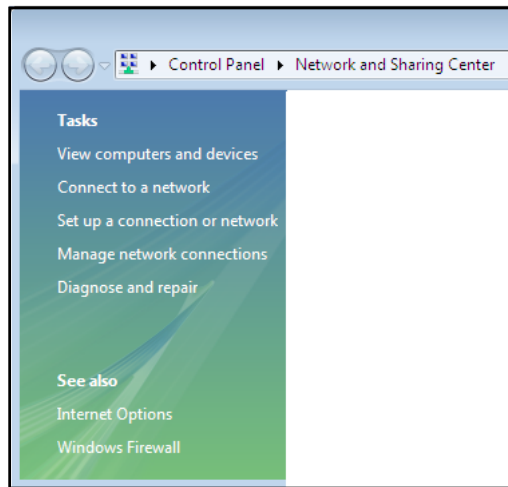
## Network Awareness

This is a set of APIs that allow programs to become network aware. For example, suppose that you are having trouble saving a file to a network share. The application you are using could discover this and perhaps start up Vista's **Network Diagnostic Framework** in an attempt to fix the problem. Also, your application could behave differently depending on whether it was connected to a network or not.

## Network Setup Wizard

The Network Setup Wizard is designed to make setting up a network easy. Once you have configured your network settings, you can export the relevant data to a USB pen. This can be used by other Vista machines to incorporate them onto the network.





To access the network setup wizard, select **Setup a connection or network** in the Network and Sharing Center.

### Network Diagnostic Framework (NDF)

The NDF is a group of technologies acting together to “automate” connectivity diagnosis and repair. Some of the problems that NDF can repair are:

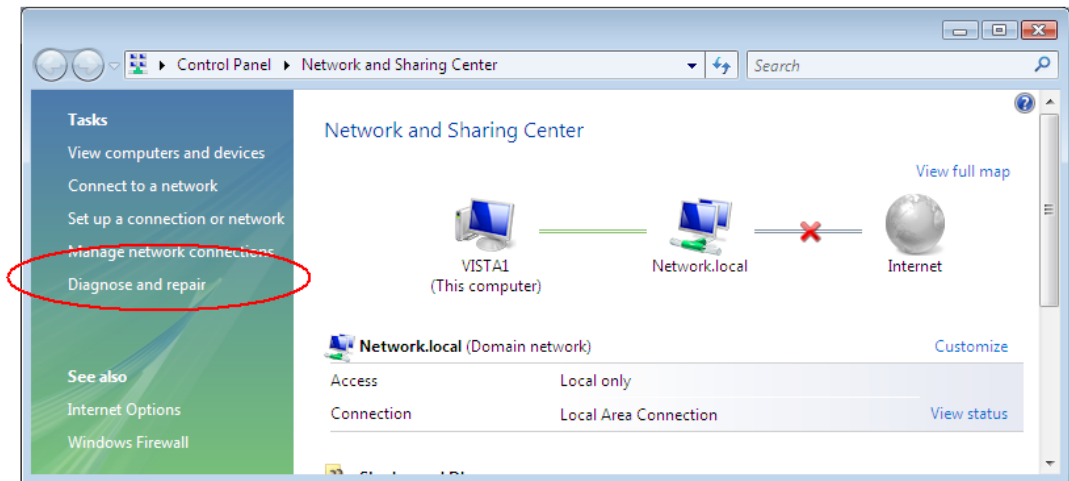
- IP configuration
- Workgroup settings
- Firewall settings
- Network hardware configuration

NDF works with wired and wireless LANs. Additionally, it can be called from within a Network Aware application, if necessary (as well as from the GUI). NDF’s **Network Diagnostics Engine** will use its agents (called **Helper Classes**) to investigate your network and devise solutions. If only one solution is found, NDF will attempt to use it. If more than one exists, then NDF solicits the user for which solution to implement — after the implementation, NDF will check to determine whether or not the problem has been resolved. If the problem has not been rectified, it will give the user the option to try a different method.

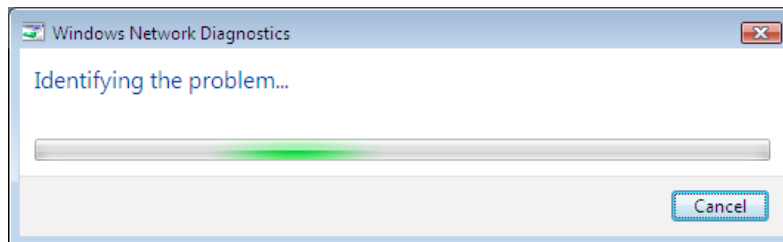


### Manually running NDF

In **Network and Sharing Center** select the **Diagnose and repair** option (left hand column).



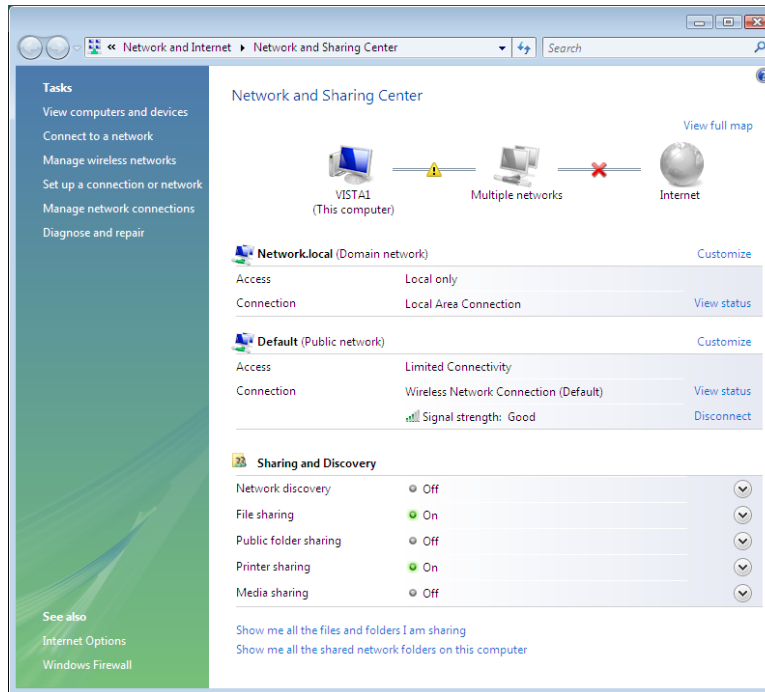
NDF starts up and investigates the network (Vista considers that the test network used to research these notes is faulty because it is not connected to the Internet — that is the significance of the red “X” on the network diagrams in these illustrations).



NDF attempts a fix, offers multiple potential solutions, and allows you to select one.

## Network Map

This is a graphical view of how your computer is connected into the network. The visual style is designed to be clear and easy to understand. Wired and wireless networks are clearly differentiated.



## Network Explorer

Displays all devices connected to the network and provides limited administration for computers.

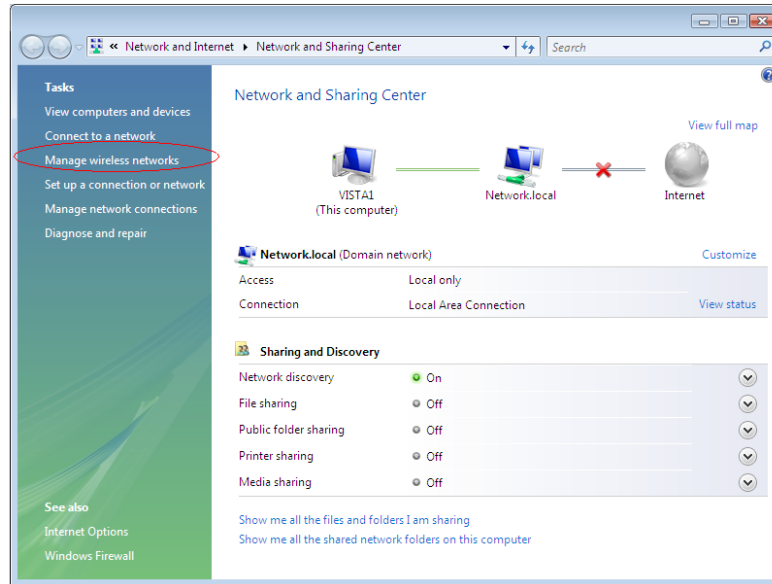
## Wireless Networking

### Wireless terminology

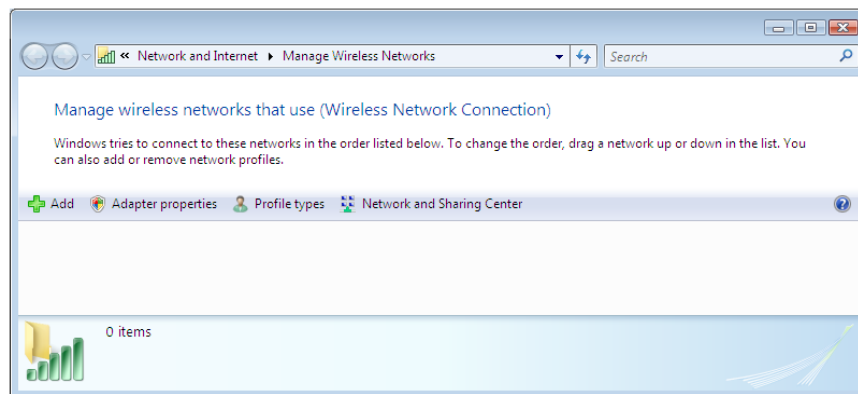
Term	meaning/functionality
<b>Wireless Networking</b>	Literally, "networking without wires"; however, this is usually taken as connecting computers using radio frequencies and protocols conforming to IEEE 802.11 a, b, g, or n standards.
<b>Access Point</b> <b>AP or WAP</b>	It is often convenient to think of an AP as a switch which connects its member stations wirelessly. AP can perform simple switching functions, or include more sophisticated capabilities such as a firewall, DHCP, etc.
<b>SSID</b> <b>Service Set Identifier</b>	Unlike a wired switch, you have no physical connection method. Instead, you specify the name of the AP with the SSID. By default, most APs broadcast their SSIDs so Vista can automatically detect them. As a security measure, this can be disabled, meaning that the SSID must be entered manually on the computer to enable connection.
<b>Ad Hoc network</b>	A group of computers communicating wirelessly, but without the aid of an AP. Microsoft considers Ad Hoc networks as incapable of encryption or authentication.
<b>MAC address lists</b>	A security feature in an AP in which an administrator configures a list of MAC addresses from which connection requests are accepted. Each Network Interface Card (NIC) holds a unique numerical number that identifies it out of all the NICs ever built. This is known as the NICs Media Access Control (MAC) address and is included on all transmissions from the card.
<b>Encryption</b>	Obscure data so that hackers cannot read it. The two methods currently in use are WEP (poor) and WPA/WPA2 (much better).
<b>RADIUS</b>	An external authentication system used to centralize authentication for multiple APs. RADIUS can also be used to gather statistics. Microsoft Windows 2003 Server contains IAS (Internet Authentication Server), which is a crude RADIUS server.

### Configuring wireless connections




If your Vista computer is Wireless-enabled then you will find an extra option in Network and Sharing Center — **Managing wireless networks**.



Selecting this leads to the following screen:



Here you can:

	"recognize" wireless networks within range
 Add	Check and/or modify the wireless adapter settings
 Adapter properties	Set up who can use the connection (everyone or just the user who set it up)
 Profile types	

### Adding a wireless network

To connect to a Wireless network you need to be able to configure the following:

component	details
<b>Service Set Identifier</b>	The SSID identifies the wireless network allowing you to choose it to connect to it. Usually, a Wireless Access Point (commonly called a WAP or just AP) broadcasts its SSID so that you can select it from within Vista. Some APs do not broadcast their SSID (as a security feature), in which case you need to know it in advance.
<b>Authentication</b>	Authentication identifies something. In wireless networking, you can identify either the User or the computer attempting to connect to the network. User identification is considered the most robust system and Wireless networks often use a RADIUS server to handle the user database.
<b>Encryption</b>	Manipulates the data by means of a mathematical key so that only authorized recipients can decode it. There are several encryption schemes in common use with varying bit lengths.

Windows Vista can provide encryption and authentication by using either WEP (Wired Equivalent Privacy) or WPA2 (WiFi Protected Access); WPA2 is the most secure. Varying encryption algorithms and bit lengths can be used for encryption. Certificates, RADIUS or pass phrases can be used for authentication. You will also need to be in range of the AP and to have TCP/IP configured correctly (typically this is performed by DHCP).

## Remote Access

Remote Access is generally used two ways:

- To provide access to your business LAN
- To provide connections off your LAN (typically the Internet)

## Creating connections

A connection allows you to configure the **Network Interface**; i.e., how data is transferred across a network

link. Typical settings configured at a connection are:





- IP settings
- Encryption type
- Authentication type

Every NIC which is recognized is automatically allocated a connection by Windows Vista; other links, such as dial-up, will need to be configured manually.

**Tip: Broadband**

*Some broadband connections use a NIC so gain an automatic connection, others use a USB Modem and may need to be configured automatically.*

Windows Vista allows you to create the following additional connections:

Icon	Connection type	Features ...
	<b>Connect to the Internet</b>	Assumes a broadband connection TCP/IP ( DHCP client) ISP details File and Printer sharing and Client for Microsoft networks unbound
	<b>Set up a wireless router or access point</b>	Configures the AP by IP Requires Admin privilege Asks to turn on Network Discovery
	<b>Set up a dial-up connection</b>	Assumes connection to Internet TCP/IP (As DHCP Client) Modem Setup ISP Details SMB not bound
	<b>Connect to a workplace</b>	Configures a VPN (Tunnel) to connect across the Internet SMB bound

**Note:** Internet connections will allow you to select a dial-up connection (if a one is configured) as the connection to the ISP.

## Authentication protocols

Authentication is the process of an RAS (Remote Access Service) Client identifying the User to the RAS Server.

Protocol	Level	Description	Use
<b>PAP</b>	Low	Password Authentication Protocol  Industry standard passwords sent as clear text	when nothing else will work
<b>CHAP</b>	High	Challenge Handshake Access Protocol  Industry standard	Between Microsoft and non-Microsoft systems
<b>MS-CHAP v2</b>	High	Upgraded version  The Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) version 2 significantly strengthens the security for the passing of security credentials and the generation of encryption keys during the negotiation of a remote access connection. MS-CHAP version 2 was specifically designed for authenticating virtual private network connections.	Microsoft systems only  Windows 98 and NT4 have limited functionality  Windows 95 cannot use MS-CHAPv2
<b>EAP</b>	High	Extensible Authentication Protocol  Allows extensions to the built-in authentication systems	Mutual Authentication  Security hardware e.g., smartcards, etc.

Client and Server negotiate the strongest authentication protocol that both have in common. The User's credentials are transmitted to the RAS server using this protocol. If the client does not share a common authentication protocol with the server, then the link cannot be established.

Increasingly, more secure systems are being developed. Examples of this are smart-cards using disposable, use-once, passwords. To provide support for advanced authentication methods, Windows Vista has EAP, which allows programmers to design their own high-security authentication systems and integrate them into the OS.

If the User's credentials are accepted, then the Server checks its RAS Policies to make sure that the conditions of the call are acceptable. If they are, the link is accepted.

### Exam Tip: **Smart Cards**

*Smart Card authentication requires a certificate and the use of EAP.*

## VPN protocols supported by Windows Vista

Authentication protocols only protect a User's logon credentials - they do **not** protect any data. To protect both data and credentials you need to create a "Tunnel" using a VPN.

A **virtual private network** (VPN) is an authenticated and encrypted communication link which is used to securely send packets across some form of public network, such as the Internet. Since the public network is considered to be insecure, encryption and authentication are used to protect the data while it is in transit. Windows Vista supports two VPN systems: PPTP (Point to Point Tunneling Protocol) and L2TP (Layer 2 Tunneling Protocol) – each has slightly different features:

Feature	PPTP	L2TP
<b>Network Type</b>	IP only	Anything: <ul style="list-style-type: none"> <li>• IP</li> <li>• Frame Relay</li> <li>• X25</li> <li>• ATM</li> </ul>
<b>Header Compression</b>	No	Yes
<b>Tunnel Authentication</b>	No	Yes
<b>Encryption</b>	MPPE	IPSec (most secure)

Windows 2000 and above support the above features (limited support is available on Windows 98 and NT4; there is no support for these features on Windows 95).

## Internet Connection Sharing (ICS)

Windows Vista allows you to make an external connection available to other Workgroup members. In this way, it is possible to provide access to the Internet for multiple computers, but through only one dial-up connection.

When ICS is installed (by selecting the **Allow other network users to connect through this computer's internet connection** tick box on the **Sharing** tab of the connections properties settings), some fundamental changes are made:

- The ICS system adopts the IP address of 192.168.0.1.
- It acts as a DHCP server offering IP addresses in the 192.168.0.0 range.
- It offers the DHCP options of 192.168.0.1 as the Default Gateway and the DNS server.
- It provides NAT and DNS forwarding.

The idea is that in a Workgroup, all clients are running APIPA until ICS is activated. The network then changes to the 192.168.0.0/24 network, and all clients receive a router and DNS server; this is the ICS system. Requests are passed to the ICS system and relayed to the ISP. You can allow other systems to dial out, if required, and change ICS configuration. You can also allow Internet users access to internal services such as Web, Mail and FTP servers.

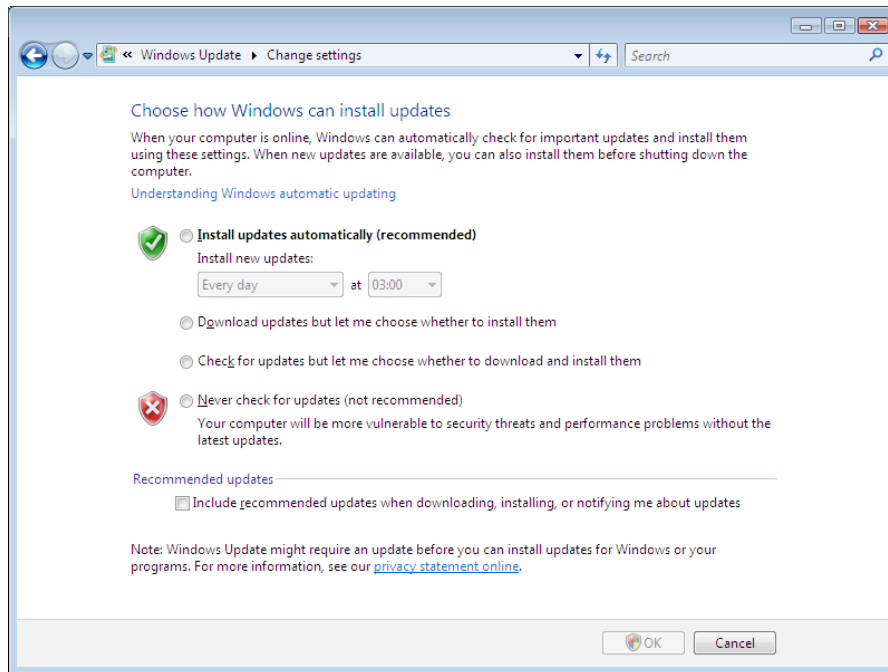


## Windows Update

Windows Update allows your computer to periodically connect to Microsoft's website, where it is scanned so that needed software updates can be identified.

You have the choice of how Updates are applied:

Setting	Ramifications
<b>Install updates automatically (recommended)</b>	The system contacts Microsoft automatically (by default, daily at 3pm).
<b>Download updates but let me choose whether to install them</b>	All updates are downloaded to the computer, then you select the updates to install.
<b>Check for updates but let me choose whether to install them</b>	No updates are downloaded until you specify them.
<b>Never check for updates (not recommended)</b>	No automatic update — you will need to manually update.
<b>Recommended update</b>	Microsoft groups its updates into two classes: <b>Important</b> and <b>Recommended</b> . Important updates cover security and stability, while recommended updates cover what Microsoft terms "Operating System Enhancements". You can elect to skip the recommend class and only download Important updates.



Windows will inform you if the system is missing critical updates. All updates downloaded and marked for installation install when the system closes down (in some instances a re-boot will be required).

## Troubleshooting

If you are using a Proxy Server, then the automatic system may not be able to connect and will display a Windows Update 8024410B error message. Downloads may fail because of a lack of disk space, you did not accept license terms, the Internet link dropped, or the processes were cancelled. In such instances, you can attempt to download again. If you do not accept a download, then Windows Update will hide it. If you change your mind, then you can use the **Restore** option in Windows Update. If hardware or applications fail after updating you may need to restore the previous drivers. Updates may need the **Windows Installer Service** running.

# Practice Questions

## Chapter 1 Deploying Windows Vista

1. You are a desktop support professional for your company. You need to capture an image of a reference Windows Vista installation in order to deploy the image to 200 other computers in your organization. What should you do?  
Choose the best TWO answers.
  - A. Boot the reference computer by using the Windows Vista product DVD and holding down the F8 key during startup.
  - B. Boot the reference computer by using a Windows PE CD-ROM.
  - C. Run Setup Manager on the reference computer to capture the operating system image.
  - D. Run ImageX on the reference computer to capture the operating system image.
  
2. You are a computer desktop support professional for your organization. You plan to upgrade 25 computers in your Accounting department from Windows XP SP2 to Windows Vista Business. You also need to employ the USMT tools to save and restore user state data. On the first user's computer you issue the following command:  
`scanstate \svr01\migration\mystore /v:13 /i:miguser.xml /i:migapp.xml /efs:abort`  
You find that the user state backup fails. What is the most likely cause of the problem?  
Choose the best answer.
  - A. The user's computer contains encrypted files.
  - B. The Miguser and Migapp configuration files should have the .inf extension.
  - C. The LoadState command needs to be run before the ScanState command on the user's computer.
  - D. User state data compression is disabled on the user's computer.
  
3. You are a desktop support professional for your organization. You plan to install Microsoft Windows Vista Business on 100 desktop computers in your company. However, the installation process fails on a test computer. All 100 computers possess the following hardware profile:  
  
1 GHz 32-bit processor  
768 MB RAM  
40-GB hard drive  
128-MB video card (DirectX 10 supported)  
  
What action should you take?  
Choose the best answer.
  - A. Replace the video card.
  - B. Upgrade the processor.
  - C. Replace the hard drive with a larger-capacity model.
  - D. Upgrade the RAM.

## Chapter 2 Managing Windows Vista Security

1. You are a computer desktop support professional for your organization. All servers in your single Active Directory domain run Windows Server 2003 R2 with SP2, and all desktop computers run Windows Vista Business. You discover that users are unable to add new Authenticode publisher digital certificates from trusted business partners to their Personal certificate store by using Internet Explorer 7. You need to allow users to add these digital certificates to their Personal certificate store. What should you do?

Choose the best answer.

  - A. Use Group Policy to edit the security zone and privacy settings for the relevant users' Internet Explorer 7 browsers.
  - B. Use Group Policy to customize the Content Ratings on all relevant users' Web browsers.
  - C. Use Group Policy to disable trusted publisher lockdown for the relevant users.
  - D. Disable Automatic Browser Configuration on the relevant users' computers.
  
2. You are a computer desktop support representative for your organization. Your network is organized into a single Active Directory domain. All desktop computers run Windows Vista Business. The manager of the Marketing department asks you to set up a shared folder for departmental use. The manager wants to be able to make changes to the access control list (ACL) of the shared folder. What action should you take?

Choose the best answer.

  - A. Grant the department manager the Allow -Write permission on the shared folder.
  - B. Grant the department manager the Allow -Read & Execute permission on the shared folder.
  - C. Grant the department manager the Allow -Modify permission on the shared folder.
  - D. Grant the department manager the Allow -Full Control permission on the shared folder.
  
3. You are a computer desktop support professional for your organization. Your network is organized as a single Active Directory domain in which all desktop computers run Windows Vista Ultimate. You need to ensure that all network traffic passing between the company's CFO and CEO is encrypted with IPSec. Your solution must involve the least amount of administrative effort. What action should you take?

Choose the best answer.

  - A. Associate the users' corporate wireless network connection type with the Domain location.
  - B. Associate the users' corporate wireless network connection type with the Public location.
  - C. Associate the users' corporate wireless network connection type with the Private location.
  - D. Configure the Group Policy setting Windows Firewall: Protect all network connections to Not Configured on all the users' laptop computers.

4. You are a desktop support professional for your organization. Your network is organized as a single Active Directory domain. All domain controllers run Windows Server 2003. Half of the company's desktop workstations run Windows XP Professional SP2, and the other half run Windows Vista Business. You configure Windows Firewall through Group Policy to disable inbound and outbound ICMP Echo Request traffic on all workstations. However, you discover that some of the workstation computers no longer effectively process Group Policy. What should you do?

Choose the best answer.

- A. Enable the Network Location Awareness service on the Windows XP workstations.
- B. Enable Slow Link Detection on the Windows XP workstations.
- C. Enable ICMP Echo Request in Group Policy for the Windows XP workstations.
- D. Enable ICMP Echo Request in Group Policy for the Windows Vista workstations.

5. You are a computer desktop support professional for your organization. Your network is organized as a single Active Directory domain. All of the users in the Sales department use company-issued laptop computers that run Windows Vista Business. Several of these users complain that their corporate-mandated Windows Firewall policies adversely affect their user experience when they are at home. You need to resolve this situation by exerting the least amount of administrative effort. What action should you take?

Choose the best answer.

- A. Use domain-level Group Policy to relax the settings of the Domain profile for Windows Firewall.
- B. Use domain-level Group Policy to relax the settings of the Private profile for Windows Firewall.
- C. Use the Windows Firewall with Advanced Security console on each computer to relax the settings of the Public profile for Windows Firewall.
- D. Use the Services console on each computer to set the startup type for Windows Firewall to Manual.

6. You are a desktop support technician for your organization. Your network is organized as a single Active Directory domain in which all servers run Windows Server 2003 and all desktop computers run Windows Vista Business. A network user named Paul belongs to the Marketing domain global group. You need to configure security on a shared folder named POLICIES such that the Marketing department can access its contents, but Paul cannot. You have granted the Marketing group the Allow > Change permission on the folder. What should you do?

Choose the best answer.

- A. Remove Paul from the Marketing global group.
- B. Grant Paul's user account the Deny > Read permission on the POLICIES folder.
- C. Add Paul's user account to the Guests local group on the computer that hosts the POLICIES folder.
- D. Grant special permissions on the POLICIES folder to the Marketing group.

## Chapter 3 Managing and Maintaining Systems that Run Windows Vista

1. You are a desktop support professional for your company. Your network is organized as a single Active Directory domain in which all servers run Windows Server 2003 R2 SP2. You need to configure 50 Windows Vista notebook computers to print to the appropriate network print devices regardless of which physical site in your organization the computers are used. The printer configuration needs to meet the following requirements:

The same printer connections apply to all users who log on to that notebook computer. The solution must involve the least amount of administrative effort.

What action should you take?

Choose the best answer.

- A. Deploy the appropriate printer connections by using User Configuration in Group Policy.
  - B. Deploy the appropriate printer connections by using Computer Configuration in Group Policy.
  - C. Deploy the appropriate printer connections by using a VBScript-based startup script in Group Policy.
  - D. Deploy the appropriate printer connections by using a VBScript-based user logon script in Group Policy.
2. You are a desktop support technician for your organization. All computers in the company run Windows Vista. The network is currently configured as a workgroup. A user informs you that he is unable to use his USB-based hard drive with his computer. He mentions that in the past, a contract systems administrator had established a device installation restriction policy on the computer. You need to resolve this matter as efficiently as possible. What action should you take? Choose the best answer.
- A. Enable the Removable Disks: Deny read access policy in Group Policy.
  - B. Disable the Prevent installation of removable devices policy in local Group Policy.
  - C. Use Device Manager to update the driver software for all USB controllers on the local system.
  - D. Relax the driver signing options on the local system.
3. You are a desktop support technician for your organization. Your network consists of a single Active Directory domain. All client computers run Windows Vista. You are troubleshooting network access for one of your users. In particular, you need to view the current user and computer Group Policy settings that are affecting the individual's user account and computer account. What should you do?

Choose the best TWO answers. Each answer represents a complete solution.

- A. Run the Gpupdate command from an administrative command prompt.
- B. Open the Resultant Set of Policy MMC console.
- C. Open the Group Policy Management MMC console.
- D. Run the Gpresult command from an administrative command prompt.

4. You are a desktop support professional for your organization. You use a third-party disk imaging tool to deploy Windows Vista to all desktop computers in your organization. You have staged several out-of-box device driver packages on the hard drive of your Windows Vista master image. You deploy the image to a reference computer and you need to verify that the out-of-box device driver packages exist in the Windows Driver Store. What action should you take?  
Choose the best TWO answers. Each choice represents a complete solution.
- A. Open Device Manager and issue the Show hidden devices command.
  - B. Use the command pnputil.
  - C. Use the command ImageX.
  - D. Analyze the contents of the %SystemRoot%\Inf folder.
5. You are a desktop support engineer for your company. Your network is organized as a single Active Directory domain in which all servers run Windows Server 2008 and all client computers run Windows Vista. You use Systems Management Server (SMS) 2003 to centrally manage software installations in your enterprise. You need to configure your client computers such that software installations can be undertaken without escalation of account privileges. Standard users must also be prevented from installing software themselves. What action should you take?  
Choose the best answer.
- A. Configure the setting User Account Control: Run all administrators in Admin Approval Mode to Enabled in domain Group Policy.
  - B. Configure the setting User Account Control: Detect Application Installations and Prompt for Elevation to Disabled in domain Group Policy.
  - C. Configure the setting User Account Control: Behavior of the elevation prompt for administrators to Prompt for consent in domain Group Policy.
  - D. Configure the setting User Account Control: Behavior of the elevation prompt for standard users to No prompt in domain Group Policy.
6. You are a computer desktop support technician for your company. Your network is organized as a single Active Directory domain in which all servers run Windows Server 2003 R2 SP2 and all client computers run Windows Vista. Because of the security policies enforced in your organization, all users are required to use smart cards in order to log on to the domain. However, a user reports that he is unable to log on to the domain when using his smart card. You verify the integrity of the smart card and the user's domain user account. What action should you take?  
Select the best TWO answers.
- A. Run Gpresult on the user's computer to verify that the host computer is being affected by the Smart Card Removal Policy setting in Group Policy.
  - B. Run Gpresult on the user's computer to verify that the host computer is being affected by the Require Smart Card setting in Group Policy.
  - C. Enable the Smart Card service on the user's computer.
  - D. Disable the Secondary Logon service on the user's computer.

7. You are a support engineer for your company. Your network is organized as a single Active Directory domain in which all servers run Windows Server 2008. You have Group Policy-based folder redirection enabled on the network. You plan to upgrade half of the client computers in your company from Windows XP Professional to Windows Vista. You need to ensure that Folder Redirection policy remains operational for all users after the upgrade. What action should you take? Choose the best answer.
- A. Configure the downlevel client computers to use the Windows Vista user profile namespace.
  - B. Configure all domain user accounts to use mandatory user profiles.
  - C. Ensure that Folder Redirection Group Policy is configured to redirect the Documents folder back to the local user profile location when policy is removed.
  - D. Ensure that Folder Redirection Group Policy is configured to apply settings to downlevel operating systems.

## Chapter 4 Configuring and Troubleshooting Networking

1. You are a desktop support technician for your organization. Your network is organized as a single Active Directory domain in which all servers run Windows Server 2003 and client computers run either Windows Vista Business or Windows XP Professional. You want to use the Network Map feature on your Windows Vista administrative workstation to diagnose a network connectivity issue. You have installed the LLTD Responder on all Windows XP Professional computers. However, the Windows XP computers fail to appear on the Network Map. What should you do? Choose the best answer.
- A. Enable the File and Printer Sharing exception in Windows Firewall on all Windows XP computers.
  - B. Install the Network and Sharing Center on all Windows XP computers.
  - C. Disable File and Printer Sharing on your administrative workstation.
  - D. Enable QoS on the local area network.
2. You are a desktop support engineer for your company. Your network is organized as a single Active Directory domain in which all servers run Windows Server 2003 R2 SP2 and all client computers run Windows Vista Business. Due to a hardware failure, you replaced the network interface card (NIC) in a shared workgroup print device in your organization and recreated the DHCP reservation for the device in DHCP, specifying a different IP address. However, users complain that they are no longer able to print to the print device. What action should you take? Choose the best answer.
- A. Instruct the users to run the command `ipconfig /registerdns` on their computers.
  - B. Instruct the users to run the command `ipconfig /flushdns` on their computers.
  - C. Instruct the users to run the command `dnscmd /clearcache` on their computers.
  - D. Restart the network print device.



3. You are a computer desktop support technician for your organization. You are preparing a reference WIM disk image of a Windows Vista Business installation for mass deployment by using Systems Management Server (SMS) 2003 and Windows Preinstallation Environment (PE). You need to ensure that Remote Assistance is functional on the reference disk image. What action should you take?

Choose the best TWO answers. Each choice represents a part of a single solution.

- A. Ensure that the Terminal Services service is started.
- B. Ensure that the Server service is started.
- C. Enable Remote Assistance in the System Control Panel.
- D. Enable Remote Assistance in the Security Center Control Panel.

4. You are a desktop support professional for your company. Your corporate network is organized as a workgroup with 25 computers that all run Windows Vista. You need to provide employees with a secure method for sharing local file and print resources with selected colleagues. Your solution must be cost-effective as well as involve least administrative effort. What action should you perform?

Choose the best TWO answers. Each correct choice represents a part of a single solution.

- A. Enable IPv6 on the LAN.
- B. Instruct users to place shared resources in their Public folders on their computers.
- C. Enable Password Protected File Sharing on all computers.
- D. Configure a domain controller to host shared resources.

5. You are a computer desktop support technician for your organization. You support a mixture of desktop and laptop computers running Windows Vista. The Research and Development department asked you to install a wireless access point so laptop computer users can work in a more mobile fashion. You have secured the wireless access point by disabling SSID broadcasts and by using WPA Personal/AES encryption. You need to configure the laptop computers to connect to the WLAN. What action should you take?

Choose the best answer.

- A. Specify the Manually connect to a wireless network option in the Connect to a network dialog box on each laptop computer.
- B. Specify the Set up a wireless router or access point option in the Connect to a network dialog box on each laptop computer.
- C. Enable RADIUS authentication on the wireless access point.
- D. Run the Windows Network Diagnostics utility on each laptop computer.

## Chapter 5 Supporting and Maintaining Desktop Applications

1. You are a desktop support professional for your organization. Your network is organized as a single Active Directory domain in which all servers run Windows Server 2003 and all client workstation computers run Windows Vista. You create a Software Restriction Policy in Group Policy and apply the policy to a reference workstation. You discover that the Software Restriction Policy locks down the computer to the point where the computer is unusable. You need to gain access to the workstation in order to reset the local resultant Group Policy. What action should you take?

Choose the best answer.

- A. Reboot the computer into the Windows Recovery Environment and log in as an administrator.
  - B. Reboot the computer into the Windows Recovery Environment and log in as a standard user.
  - C. Reboot the computer into Safe Mode and log in as an administrator.
  - D. Reboot the computer into Safe Mode and log in as a standard user.
2. You are a desktop support analyst for your company. Your network is organized as a single Active Directory domain in which servers run Windows Server 2003 and Windows 2000 Server and client computers run either Windows Vista or Windows XP Professional. The members of the Research and Development use Virtual PC software installed with Windows 95 to perform backward-compatibility testing. These team members need to configure a legacy command-line application to print to a network workgroup printer from their virtual machines. What action should you take?

Choose the best answer.

- A. Run the command `net use lpt1 \\server01\laser1 /persistent:yes` from the MS-DOS prompt in the virtual machine.
  - B. Run the command `print /d:\server01\laser1` from the MS-DOS prompt in the virtual machine.
  - C. Install the printer in Windows 95 and print to the device by using the path command from the MS-DOS prompt.
  - D. Enable the LPT port in the virtual machine.
3. You are a desktop support analyst for your company. Your network is organized as a single Active Directory domain in which all servers run Windows Server 2003 and all client computers run Windows Vista. You publish several shared folders in Active Directory for employees in the Marketing department. Amanda, a member of the Marketing department, complains that she is unable to access one particular folder. Other members of the Marketing team can access all folders. What actions should you take?

Choose the best TWO answers. Each answer represents part of the solution.

- A. Run the Resultant Set of Policy (RSOP) tool on Amanda's workstation.
- B. Check the NTFS permissions on the shared folder.
- C. Verify that Amanda is logged on to the domain.
- D. Check the Shared Folder permissions on the shared folder.

4. You are a desktop support professional for your organization. Your network is organized as a single Active Directory domain in which all servers run Windows Server 2003 and all client workstations run Windows Vista. You have deployed an IPsec security policy named SecureIP by using Active Directory Group Policy. The SecureIP GPO is linked to an organizational unit (OU) named HiSecure. Computer accounts from the Accounting department are contained in the HiSecure OU. You learn all but two workstations in the department receive the policy. You need to determine why the two computers are not being affected by the Group Policy settings. What action should you take first? Choose the best answer.
- A. Verify that the GPO is properly linked to the HiSecure OU.
  - B. Verify that the two computer accounts exist in the HiSecure OU.
  - C. Verify that the Accounting department computers have the Read permission to the GPO.
  - D. Verify that the two computers in question have UAC enabled.

## Answers and Explanations

### Chapter 1

#### 1. Answers: B, D

**Explanation A.** Incorrect. In order to capture a Windows Vista operating system image, you need to create a Windows PE boot CD. This CD can be created by using free utilities available from Microsoft. Pressing the F8 key during a product DVD-based system startup has no effect.

**Explanation B.** Correct. You can use freely available Windows deployment tools to create a Windows Pre-installation Environment (PE) CD, which can be used to capture or apply WIM-format operating system images.

**Explanation C.** Incorrect. Setup Manager is a Windows XP tool used to create unattended setup answer files.

**Explanation D.** Correct. You can use the ImageX utility to capture and apply (that is to say, upload and download) operating system images from a Windows PE boot environment.

#### 2. Answer: A

**Explanation A.** Correct. You need to use the `/efs:skip` parameter of the `ScanState` command in order to back up files that have been encrypted with Encrypting File System (EFS). The default option, `/efs:abort`, causes `ScanState` to fail if an encrypted file is detected on the user's system.

**Explanation B.** Incorrect. The configuration files in USMT 2.6 used the `.inf` extension. The USMT 3.0 toolkit now stores all configuration data in Extensible Markup Language (XML) format.

**Explanation C.** Incorrect. The `ScanState` component of the USMT backs up user state data to an external drive or network share location. The `LoadState` program restores the backed-up user state data.

**Explanation D.** Incorrect. Unless you use the `/nocompress` option with `ScanState`, all user state data is compressed in order to conserve disk space.

### 3. Answer: D

Explanation A. Incorrect. Windows Vista supports video cards with at least 128-MB of onboard RAM, DirectX 9 or later and hardware-based support for Microsoft Pixel Shader 2.0.

Explanation B. Incorrect. The minimum processor specification for Windows Vista is a 1-GHz x86 or x64 CPU.

Explanation C. Incorrect. The minimum system requirement for Windows Vista is a 40-GB hard drive with at least 15 GB of available space.

**Explanation D.** Correct. These computers require at least 1 GB of system RAM in order to support an upgrade to Windows Vista.

## Chapter 2

### 1. Answer: C

Explanation A. Incorrect. Windows Vista Group Policy does contain a policy entitled Security Zones and Content Ratings. However, these settings do not affect a user's ability to add trusted publisher digital certificates to their Personal certificate stores.

Explanation B. Incorrect. The Security Zones and Content Ratings policy allows an administrator to customize the behavior of the Internet Explorer 7 Content Advisor tool. However, this policy has nothing to do with the challenges inherent in this scenario.

**Explanation C.** Correct. The trusted publisher lockdown feature in Windows Vista Group Policy allows an administrator to prevent users from adding new trusted publishers by using Internet Explorer 7. By relaxing this policy, the users can then add the digital certificates from the trusted software publishers to their certificate stores.

Explanation D. Incorrect. The Automatic Browser Configuration Group Policy has nothing (directly) to do with digital certificate installation and management. Instead, this policy allows an administrator to auto-configure an installation of Internet Explorer from settings defined in an Internet Explorer Administration Kit (IEAK) script file.

### 2. Answer: D

Explanation A. Incorrect. First of all, granting the Write permission without at least the Read permission is worthless. Second of all, the marketing manager needs to adjust the access list to the resource: Allow -Full Control is the only feasible permission in this case.

Explanation B. Incorrect. The Read & Execute permission allows a user to read files and run programs from a particular secured folder. This permission level does not grant the user the ability to add or subtract users from the access control list of the resource.

Explanation C. Incorrect. The Modify folder permission allows the user to edit the content or files and to run executable program files in a folder. The Full Control permission is required in order to edit the ACL for the resource.

**Explanation D.** Correct. The Allow -Full Control permission would give the manager ultimate control over the shared resource, which is required in this scenario.

### 3. Answer: C

Explanation A. Incorrect. The Domain Windows Firewall profile is optimized for networks that rely upon Microsoft Windows Active Directory domain security. The scenario explicitly states that Active Directory is not in use on this network.

Explanation B. Incorrect. By associating a network connection with the Public Windows Firewall location type, you are enabling high security, which will, in this scenario, result in reduced functionality and connectivity options for this user.

**Explanation C.** Correct. You should associate your network connection with the built-in Private Windows Firewall location if the security requirements on the network aren't as stringent (for example, an enterprise firewall protects the internal network from the Internet).

Explanation D. Incorrect. We do not want to compromise the security of the users' laptop computers. Therefore, we do not want to use Group Policy to globally disable the Windows Firewall feature on those computers.

### 4. Answer: C

Explanation A. Incorrect. Network Location Awareness (NLA) is a network link-state protocol used with Windows Vista to more effectively tune its relationship with other computers on a LAN. The analog to NLA in Windows XP is "slow link detection." Slow link detection requires Internet Control Message Protocol (ICMP) to be enabled on all participating computers. Moreover, NLA in Windows XP pertains to Internet Connection Sharing.

Explanation B. Incorrect. The Slow Link Detection feature determines the relative link speed in use and is used to tune Group Policy processing in Windows XP. Number one, the service is enabled by default. Number two, the fact that we disabled ICMP effectively disables Slow Link Detection. Windows Vista uses NLA for link management and is therefore 'free' of the ICMP requirement.

**Explanation C.** Correct. You will need to enable ICMP Echo Request (ping) traffic on the Windows XP computers for them to process Group Policy, in particular by using the Slow Link Detection feature, effectively.

Explanation D. Incorrect. Windows Vista is free from the ICMP requirement. Network Location Awareness detects whether the link on which the computer resides is high speed or low-speed; this has a positive impact on Group Policy processing.

### 5. Answer: B

Explanation A. Incorrect. We don't want to alter the Windows Firewall settings as they pertain to the corporate LAN. Rather, we want to relax the Windows Firewall settings for the users' Private profile; in other words, their home network environment.

**Explanation B.** Correct. The users' home networking connections are doubtless associated with the Private profile in Windows Firewall. By relaxing these settings in domain-level Group Policy, users can enjoy two separate Windows Firewall environments, each customized to a particular networking environment.

Explanation C. Incorrect. First off, 'least administrative effort' does not equate to making computer-by-computer modifications. Second, the Public profile is a higher-security location intended for unsecure network environments, such as a public Wi-Fi hotspot. In this scenario, the users want freedom with regard to their Private profile in Windows Firewall.

Explanation D. Incorrect. We need to exert least administrative effort in this case; making changes to each computer separately fails to meet this requirement. Moreover, globally stopping or suspending the Windows Firewall service reduces overall system security, and is never advisable on general principle.

## 6. Answer: B

Explanation A. Incorrect. If we remove Paul from the Marketing global group, then Paul will instantly be stripped of any other network or local privileges and permissions that the Marketing group has already been granted.

**Explanation B.** Correct. The way shared folder permissions work is that they are cumulative, with the exception that an explicit Deny permission always overrides a corresponding Allow permission. In this case Paul's effective permission on the POLICIES folder denies him the ability to read files in the folder.

Explanation C. Incorrect. Unless the Guests group appears on the access control list of the POLICIES folder, making this change will not alter Paul's effective permissions to resources residing in the POLICIES folder at all.

Explanation D. Incorrect. Any permissions changes you make on the Marketing group will affect all users in this group, including Paul. This scenario calls for editing Paul's own permissions on the POLICIES folder without affecting any other Marketing person's access.

## Chapter 3

### 1. Answer: B

Explanation A. Incorrect. We should use the Deployed Printers policy in Computer Configuration in domain Group Policy to handle this situation. Any Group Policy settings under Computer Configuration will apply to any user who logs on to an affected computer.

**Explanation B.** Correct. Windows Server 2003 R2 supports Group Policy-based printer deployments. So long as we deploy the network printer connections through the Computer Configuration node, instead of the User Configuration node, the printer connections will be available to all domain notebook computer users.

Explanation C. Incorrect. Startup scripts run during machine startup, so these settings would indeed apply to all users of the affected computer. However, this solution fails to meet the requirement for least administrative effort. After all, how many full-time systems engineers are also programmers?

Explanation D. Incorrect. A logon script affects only specific users, not all users of a particular computer globally. Also, we have the requirement in the scenario calling for least administrative effort to consider.

### 2. Answer: B

Explanation A. Incorrect. Enabling this policy prevents the user from using removable disks on his local system.

**Explanation B.** Correct. This policy is a sort of global on/off switch with regard to removable device usage. By lifting this policy, the user will thereafter be permitted to plug in his USB hard drive on the local computer.

Explanation C. Incorrect. This choice is a classic 'red herring.' That is, no evidence exists in this scenario to lead us to believe that there is something wrong in hardware or software on the removable storage ports themselves. This is a local Group Policy issue, pure and simple.

Explanation D. Incorrect. The System Control Panel item includes options for handling device drivers and driver signing. While it is remotely feasible to think that a driver signing issue might be the culprit behind the user not being able to plug in his USB drive, the scenario stated explicitly that a former administrator enabled device restriction policies on the local computer. Don't read too much into certification exam items!

### 3. Answers: B, D

Explanation A. Incorrect. The Gpupdate utility is used to reprocess local and/or Active Directory-based Group Policy.

**Explanation B.** Correct. The Resultant Set of Policy Microsoft Management Console (MMC) is a graphical tool for analyzing Group Policy Object (GPO) settings. The console can also perform "what if?" scenarios and generate reports.

Explanation C. Incorrect. The Group Policy Management Console (GPMC) is an administrative tool that is used to create, edit, and analyze GPOs for a local computer or in Active Directory. While GPMC can be used to perform RSoP modeling, you would get much better 'bang for your buck' by using the RSoP console.

**Explanation D.** Correct. The Gpresult utility is a command-line interface for the RSoP console.

### 4. Answers: B, D

Explanation A. Incorrect. The Show hidden devices command in Device Manager is used to display non-Plug and Play (PnP) devices in the hardware tree.

**Explanation B.** Correct. The pnputil command is used to add driver installation packages to a Windows Vista computer. You can also run pnputil -e to display the current contents of the Windows Driver Store. Driver staging is useful in cases where you want to use a custom out-of-box device driver rather than the 'generic' or absent one in the default Plug and Play driver library.

Explanation C. Incorrect. ImageX is a separate (but free) utility available from Microsoft that allows administrators to manage Windows Image Format (WIM) operating system image files. The ImageX tool cannot be used alone to view the Windows Driver Store on a target Windows Vista computer.

**Explanation D.** Correct. The Windows Driver Store in Windows Vista is located in (if your system drive is drive C:) C:\Windows\Inf.

### 5. Answer: B

Explanation A. Incorrect. The UAC Admin Approval mode forces administrator interactivity with sensitive system processes, either through consent or through prompting for credentials. In this case, we want automatic software installations to proceed independently of UAC and without administrator intervention.

**Explanation B.** Correct. This particular policy is useful in environments where software is deployed centrally and we want the installation to 'silently succeed' without stopping and prompting the user for administrative credentials.

Explanation C. Incorrect. The requirements for the scenario state that we need for the software deployments to proceed without pausing for the input of administrator credentials. By enabling this Group Policy, we have effectively defeated our purpose.

Explanation D. Incorrect. It should be noted that when the Group Policy setting User Account Control: Detect Application Installations and Prompt for Elevation is disabled, standard users still have no user right to install software on the computer. Therefore, the User Account Control: Behavior of the elevation prompt for standard users policy has no net effect to what we are trying to accomplish here.

## 6. Answers: B, C

Explanation A. Incorrect. The Smart Card Removal Policy Group Policy setting simply forces a workstation to lock whenever the smart card is removed from the reader.

**Explanation B.** Correct. The command-line Gpresult tool allows you to view precisely which user and/or computer Group Policy Objects (GPOs) are affecting the current user and computer.

**Explanation C.** Correct. If you plan to use smart cards to provide for secure authentication to Active Directory, then you need to make sure that the Smart Card service is enabled and running on all relevant Windows Vista client computers.

Explanation D. Incorrect. The Secondary Logon service allows you to impersonate the security credentials of another user on an ad-hoc basis. The Secondary Logon service is not relevant in this scenario.

## 7. Answer: D

Explanation A. Incorrect. Windows XP uses the namespace %SystemRoot%\Documents and Settings. Windows Vista uses the namespace %SystemRoot%\Users. There is no functional or reasonable method for 'converting' the Windows XP user profile path to that of Windows Vista.

Explanation B. Incorrect. Mandatory user profiles are shared, read-only user profiles. This action would prevent users from maintaining their own personal roaming user profiles, and is therefore not applicable in this scenario.

Explanation C. Incorrect. This particular Group Policy setting can be helpful when troubleshooting malfunctioning roaming user profiles after an upgrade from Windows 2000/XP to Windows Vista. After all, the default user profile store location has changed in between the operating system versions.

**Explanation D.** Correct. The User Configuration/Windows Settings/Folder Redirection/Documents Group Policy contains a setting that makes folder redirection compatible with Windows 2000, Windows XP, and Windows Server 2003. This setting is crucial if your client computers run Windows Vista in addition to downlevel OS versions.



## Chapter 4

### 1. Answer: A

**Explanation A.** Correct. In order for Windows XP computers to appear on a Windows Vista-generated Network Map, both the Link-Layer Topology Discovery (LLTP) Responder component as well as the appropriate protocol exception in Windows Firewall need to be configured on all Windows XP computers in the network.

Explanation B. Incorrect. The Network and Sharing Center is actually not an installable component. Instead, this is the built-in module in Windows Vista that allows you to generate a Network Map diagram.

Explanation C. Incorrect. All Windows hosts to be included on a Network Map diagram require the LLDP Responder as well as an exception in Windows Firewall for File and Printer Sharing.

Explanation D. Incorrect. Quality of Service (QoS) refers to a network traffic-shaping technology. We don't have any sort of dependency on this service for Network Maps in Windows Vista. Think LLDP Responder instead, at least for Windows XP client computers.

### 2. Answer: B

Explanation A. Incorrect. This command re-registers the local computer's host name and IP address with its configured primary Domain Name System (DNS) server computer.

**Explanation B.** Correct. Issuing this command purges the DNS resolve cache on the target computer. The problem here is that the users are resolving the printer's old IP address from local cache instead of querying their DNS server for the updated IP address.

Explanation C. Incorrect. This command is used on Windows Server 2003-based DNS servers to purge the host name resolver cache on the server.

Explanation D. Incorrect. Because the scenario states that we are centrally managing the IP configuration for the print device in DHCP, there is no need to restart the print device again.

### 3. Answers: A, C

**Explanation A.** Correct. The Remote Desktop and Remote Assistance technologies in Windows Vista have a dependency upon the Terminal Services service.

Explanation B. Incorrect. The Server service allows a Windows computer to host incoming network and remote management requests. However, this service relies upon a different protocol than does Remote Assistance.

**Explanation C.** Correct. We should make sure that the option Allow Remote Assistance connections to this computer is enabled on the Remote tab of the System Control Panel item.

Explanation D. Incorrect. The Security Center Control Panel is nothing more than a notification mechanism regarding the current run status of Windows Update, Windows Firewall, Windows Defender, and Internet Explorer 7.0 security settings.

#### 4. Answers: B, C

Explanation A. Incorrect. File-sharing services have nothing whatsoever to do with the IP version in use on the LAN.

**Explanation B.** Correct. The Password Protected File Sharing feature of Windows Vista automatically creates a default shared folder. This feature saves the administrative effort of teaching the users to manually create and share file-system folders.

**Explanation C.** Correct. The Password Protected File Sharing feature in Windows Vista is intended to make it as easy as possible for users to share resources with other users on their local area network (LAN).

Explanation D. Incorrect. Although creating an Active Directory domain is, in theory, the best approach (after all, we would have centralized security and network administration), the scenario states that we need to avoid extra administrative effort and be aware of monetary expenses.

#### 5. Answer: A

**Explanation A.** Correct. This option allows you to specify the service set identifier (SSID) and encryption protocols, such as Wi-Fi Protected Access (WPA) Personal and Advanced Encryption Standard (AES), in use on the WLAN.

Explanation B. Incorrect. This particular option is what you need if you want to configure a wireless router or access point device, not to create a dedicated connection profile to such a device.

Explanation C. Incorrect. The scenario states that we are using WPA Personal encryption, which does not require a dedicated RADIUS server. Moreover, there is much more work to do than enable RADIUS on the WAP if we want to use, say, WPA Enterprise authentication and encryption.

Explanation D. Incorrect. In this case we have no need for running diagnostics. In fact, all we need is the SSID of the WLAN along with the preshared encryption key and compatible protocols and we are 'all set.'

## Chapter 5

### 1. Answer: C

Explanation A. Incorrect. The Windows Recovery Environment (RE) is a replacement for the Recovery Console that we used in Windows XP and Windows 2000. The Windows RE is not a graphical user interface, so Group Policy is not only not applied here but is not relevant in this case at all.

Explanation B. Incorrect. You must log into a Windows Vista installation via the Windows Recovery Environment as a member of the local Administrators group on the local computer, not as a standard user.

**Explanation C.** Correct. If you reboot a Windows XP or Windows Vista client computer into Safe Mode and log on to the local machine as a member of the Administrators group, then Software Restriction Policies are not applied to the user or to the computer. You can then begin troubleshooting.

Explanation D. Incorrect. Software Restriction Policy applies to standard users regardless of whether the users logs on to their Windows Vista computer in normal mode or in Safe mode.

## 2. Answer: A

**Explanation A.** Correct. The net use command is used in a command-line environment to map a shared file or print resource to either a local drive letter or to a local printer port.

Explanation B. Incorrect. The DOS print command is used to submit a print job to a print device that has already been mapped to a local port by using the net use command.

Explanation C. Incorrect. Number one, the path command is used for nothing more than specifying the search path for executable program files in MS-DOS. Number two, we won't be able to print to a Windows printer connection from within our MS-DOS application, period!

Explanation D. Incorrect. First, the Line Print Terminal (LPT) port in Windows 95, assuming that there is one present, will be enabled by default. Second, the existence of an LPT port is wholly insignificant unless and until we can map that physical interface port with a local or remote print device.

## 3. Answers: B, D

Explanation A. Incorrect. The command-line utility Gpresult.exe is great for reporting to you what Group Policy Objects (GPOs) are affecting the currently logged on user. However, this problem centers on file and folder permissions, not Group Policy.

**Explanation B.** Correct. Publishing a shared folder in Active Directory makes that file or print resource more easily 'findable' by your users. The AD publishing in itself doesn't handle security. Instead, you must verify that correct NTFS permissions are configured on shared file and print resources.

Explanation C. Incorrect. In this scenario, Amanda is able to connect to other shared folders, implying that she is correctly logged on to the Active Directory domain.

**Explanation D.** Correct. Remember that NTFS permissions and Shared Folder permissions combine to form a user's effective permissions. Therefore, when checking access to a shared folder you must examine both types of permissions.

## 4. Answer: B

Explanation A. Incorrect. If the SecureIP GPO were not properly linked to the HiSecure OU, then none of the Accounting department computers would receive the policy settings.

**Explanation B.** Correct. The best explanation for why the two 'rogue' computers are not receiving Group Policy settings is that their respective computer accounts reside, for whatever reason, outside of the HiSecure OU. Moving the computer accounts to the correct OU should solve this problem nicely.

Explanation C. Incorrect. In order for user accounts or computer accounts to be affected by Group Policy settings, these accounts must be granted the Apply Group Policy permission to the GPO, not simply the Read permission.

Explanation D. Incorrect. User Account Control (UAC) technology plays no part in the problem that is outlined in this scenario.