Exam Manual

LearnSmart

Microsoft Windows 7

Enterprise Desktop Support (70-685)

Smarter Training

This LearnSmart exam manual empowers candidates who wish to pass the 70-685 Exam for Windows 7, Enterprise Desktop Support Technician. By presenting complex topics clearly and directly, the manual equips technicians and other IT professionals with the skills necessary to isolate, document and resolve problems on a Windows 7 desktop or laptop computer. Topics covered in this manual include:

- Desktop Application Issues
- Networking Issues
- Windows 7 Client
- Mobile User Support
- And more!

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

Windows 7 Enterprise Desktop Support Technician (70-685) LearnSmart Exam Manual

Product ID: 012382
Production Date: July 11, 2011

Warning and Disclaimer

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

Volume, Corporate, and Educational Sales

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

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

International Contact Information

International: +1 (813) 769-0920

United Kingdom: (0) 20 8816 8036

Table of Contents

Abstract

This manual is intended to help the technician prepare for the Windows 7 Enterprise Desktop Support Technician (70-685) Exam. It provides students with the knowledge and skills needed to quickly isolate, document and resolve problems on a Windows 7 desktop or laptop computer, especially as it pertains to an Enterprise environment. Typically, this includes the resolution of Tier 1 and 2 problems.

Microsoft suggests a minimum of three years of experience configuring and supporting desktop or laptop operating systems. It's also recommended to have at least six month's experience with Windows 7, as well. While Microsoft doesn't explicitly list a pre-requisite, it should be noted that the actual certification, Enterprise Desktop Support Technician on Windows 7 does require the 70-680 guide, which provides a much needed background to the higher-level concepts covered in this manual.

What to Know

When you pass Exam 70-685 for Windows 7, you will gain the following certification:

MCITP: Microsoft Certified Enterprise Desktop Support Technician 7

The 70-685 exam measures technician's ability to accomplish the tasks listed below. The percentages indicate the relative weight of each major topic area on the exam:

- Identifying and Resolving Desktop Application Issues (20 percent)
- Identifying the Cause of and Resolving Networking Issues (23 percent)
- Managing and Maintaining Systems That Run Windows 7 (21 percent)
- Supporting Mobile Users (18 percent)
- Identifying the Cause of and Resolving Security Issues (18 percent)

Tips

We recommend that you use at least one fully comprehensive source of information on Windows 7 and the exam, in general. This can include video training or a traditionally published book. As mentioned in the abstract, successful candidates will have had a few years professional experience as a PC tech and about six months experience with Windows 7.

Domain 1: Identifying Cause of and Resolving Desktop Application Issues

Identifying and Resolving New Software Installation Issues

This section will help administrators:

- Troubleshoot software installation failures
- Verify installation requirements
- Understand how AppLocker:
    - Provides improvements over previous version Software Restriction Policies (SRP).
    - Facilitates digital signing.
    - Can block software installations.

You can encounter software errors and failures during or after installation:

- Errors that appear **during installation** can result from policy/permission constraints, availability issues, or installation settings.
- Errors displayed **immediately after installation** can be associated with policy restrictions or compatibility problems.
- Errors displayed **long after installation** commonly result from changes in configuration.

To successfully install software on Windows 7, you should understand concepts such as:

- Administrator privileges
- Installation code and data
- Application compatibility and dependencies
- AppLocker
- SRP

Generally, there are two means of installing software on systems running Windows 7:

- Manually install a program.
- Software deployment technology such as:
    - **Group Policy** – you may be required to use Group Policy to verify trusted sites, configure Application Control Policies (AppLocker), or to facilitate obtaining a certificate from a third-party software publisher store.
    - **Microsoft System Center Configuration Manager** – System Center Configuration Manager, formerly Systems Management Server (SMS), is a system management software product by Microsoft for managing large groups of Windows -based computer systems. Configuration Manager provides remote control, patch management, software distribution, operating system deployment, network access protection, and hardware and software inventory. The most frequently used feature is inventory management, which provides both hardware and software inventory across a business enterprise.)

- **Windows Automated Installation Kit (Windows AIK or WAIK)** – a collection of tools and technologies produced by Microsoft designed to assist in the deployment of Windows. It was first introduced with Windows Visa. Windows AIK Version 2.0 was released with Windows 7 beta. Significantly, a single new tool, DISM, took over the functions of several earlier tools including PEImg and IntlCfg, which were deprecated. The new WinPE 3.0 has AeroSnaps - a feature introduced for Windows 7. The User State Migration Tool (USMT) was added to this WAIK.

- **Microsoft Deployment Toolkit 2010 Kit 2010 Suite** (formerly Business Desktop Deployment) – a piece of server software that permits network deployment of Microsoft Windows. It can currently distribute Windows XP, Windows Vista, Windows 7, Windows Server 2003, Windows Server 2008, and Windows Server 2008 R2. Hardware drivers, Windows updates, and software can be included with the installation.

The following topics explain some causes of software errors/failures, and provide suggestions for how to resolve them.

- **Media Location** – before installing an application, ensure that all required files are saved in the right locations.
- **Logo Testing –** Windows 7 logo testing is a feature that examines software being installed and checks for:
  - Compliance with specific anti-spyware guidelines
  - Isolation from protected resources in Windows
  - Reversible installation
  - Digital signature on all files

  If you receive a warning that an application has not passed Windows 7 logo testing, you should avoid installing it.

- **Verifying External Connections –** determine if the software installation requires data (such as product key) from an external source. For example:
  - Database
  - Mainframe
  - Web site
  - License server
  - Application server
- **Verifying Application Dependencies** – if applicable, determine if the software requires any of the following to be pre-installed:
  - Updates
  - Features
  - Service packs
  - Other applications

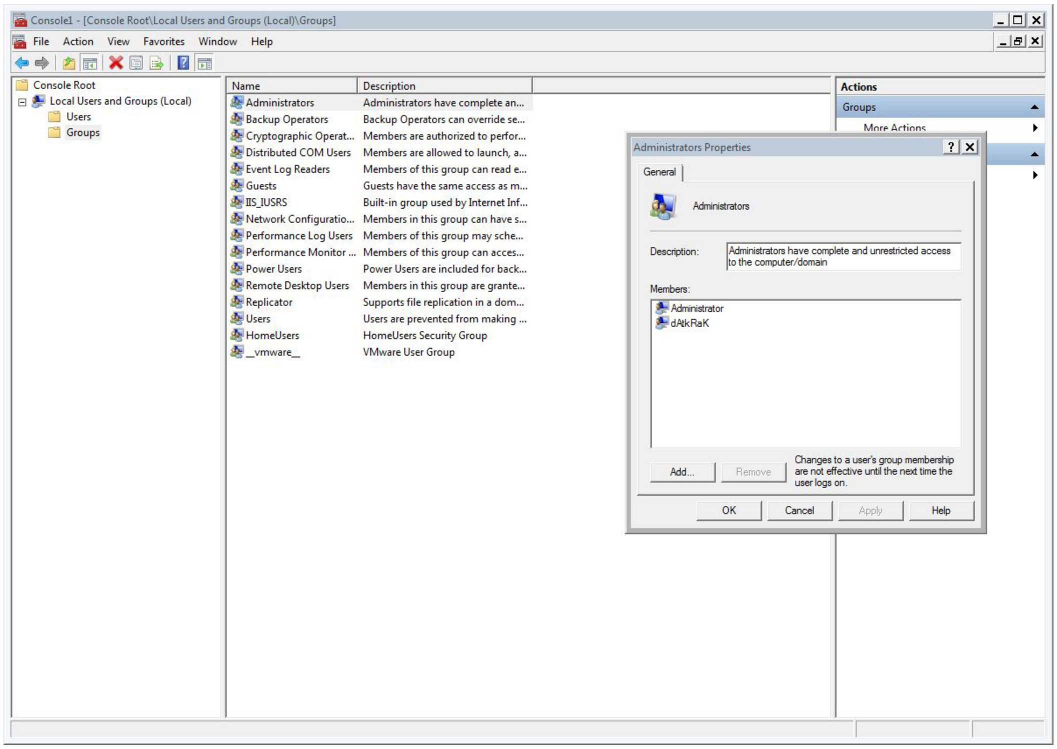
Local Administrator Requirements

To successfully install software, the user account normally must at least have local domain administrator privileges, and the account should have local administrator privileges on the computer uploading the software. Additionally, the account should be a member of the Administrators group on the computer to have rights to install software on the system.

If you get hung up on the User Account Control prompt while trying to install software on a computer, you should verify that the account used for installation is granted local administrator privileges on the computer. Normally having domain administrator privileges is sufficient because by default, domain administrators are members of the local Administrators group on every computer that is a member of the same domain. But, you may need to verify your access rights even if you are already a domain administrator; the Domain Administrators group may have been removed from the local Administrators group.

To determine whether you are a member of the local Administrators group on a particular computer, you can use the **Local Users and Groups** console. To open the console in Windows 7, click Start, type **edit local users and groups**, and press **Enter**.

Then, in the console tree of the **Local Users and Groups** console, select Groups, and double-click the Administrators group in the details pane. The Administrators Properties dialog box appears (as displayed below) listing all local administrators for that computer.


Console1 - [Console Root\Local Users and Groups (Local)\Groups]
File
Action
View
Favorites
Window
Help
Console Root
Local Users and Groups (Local)
Users
Groups
Actions
Groups
More Actions
Administrators Properties
General
OK
Cancel
Apply
Help
Add...
Remove

Name	Description
Administrators	Administrators have complete an...
Backup Operators	Backup Operators can override se...
Cryptographic Operat...	Members are authorized to perfor...
Distributed COM Users	Members are allowed to launch, a...
Event Log Readers	Members of this group can read e...
Guests	Guests have the same access as m...
IIS_IUSRS	Built-in group used by Internet Inf...
Network Configuratio...	Members in this group can have s...
Performance Log Users	Members of this group may sche...
Performance Monitor ...	Members of this group can acces...
Power Users	Power Users are included for back...
Remote Desktop Users	Members in this group are grante...
Replicator	Supports file replication in a dom...
Users	Users are prevented from making ...
HomeUsers	HomeUsers Security Group
__vmware__	VMware User Group

Administrators

Description: Administrators have complete and unrestricted access to the computer/domain

Members:
Administrator
dAtkRaK

Changes to a user's group membership are not effective until the next time the user logs on.

Figure 1: Local Users and Groups, Administrators Properties

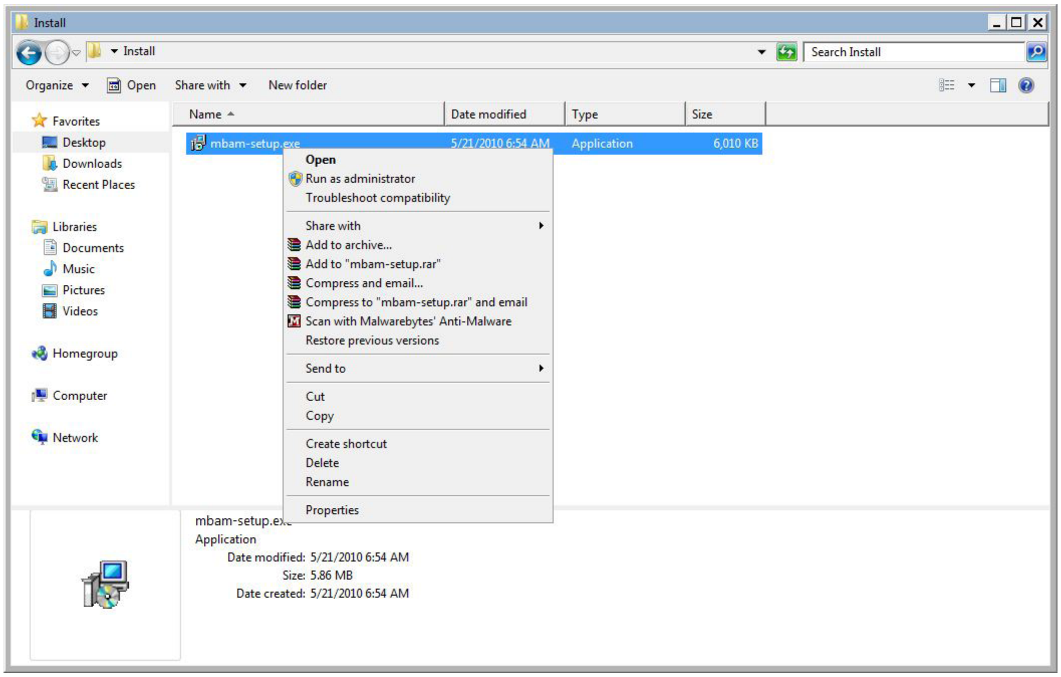
On the Local Administrators dialog box, local administrators can press the Add button to add new administrators.

In an enterprise network, it is preferable to control local group membership by using the Restricted Groups feature in Group Policy. Local Group Policy is the only local GPO that allows both computer configuration and user configuration settings to be applied to all users on a computer.

Use the following path to access and manage local GPO:

1. Click Start, type MMC, and press Enter
2. In Microsoft Management Console, click **File** → **Add/Remove Snap-in**
3. In the Add or Remove Snap-ins dialog box, click **Group Policy Object Editor** → **Add**
4. The Select Group Policy Object dialog box appears

After verifying that you are listed as an administrator, and you get a message while installing the program that administrator rights are required, then choose the option to run the installer program as an administrator. Right-click Installation and click Run as Administrator (as shown below). If a User Account Control consent or credential prompt appears, enter the required confirmation or administrator credentials.



mbam-setup.exe
Application
Date modified: 5/21/2010 6:54 AM
Size: 5.86 MB
Date created: 5/21/2010 6:54 AM

Figure 2: Running a Program as Administrator

Licensing Restrictions

You may not be able to install an application if it requires a license or product key; or the application may require that the computer is connected to a license server before allowing the installation.

Application Control Policies and Digital Signing vs. Software Restriction Policies (SRP)

Windows XP and Vista supported SRP, a means by which administrators created rules to restrict what programs particular users or groups could run, by specifying that what programs could run. Businesses that use SRP usually develop blacklists: Group Policy Objects (GPOs) that block known malware based upon source network zone, path name, hash or signed certificate. Specifically, SRP rules override a defined default security level by removing restrictions or adding restrictions. However, because robust SRP rules are hard to define, most businesses default to "unrestricted," giving any program not explicitly disallowed a free pass.

Microsoft's replacement for SRP, AppLocker, is available in Windows Server 2008 R2 and Windows 7 Enterprise and Ultimate editions. For backwards compatibility, GPOs can include both SRP and AppLocker rules. In such cases, AppLocker rules are only applied to PCs running Windows 7, while SRP rules are only applied to older PCs.

Like SRP, AppLocker can allow or deny a program to launch. However, AppLocker imposes a default "disallow" stance. After you start the Application Identity (AppID) service and apply an AppLocker rule, a program not encompassed by AppLocker rules will fail to launch, displaying the message: "The program is blocked by group policy."

In this way, AppLocker encourages businesses to define whitelists rather than blacklists. Although AppLocker whitelists still require maintenance, they make it easier to identify all of the programs with permission to run, instead of listing all the unknown and potentially harmful programs that want to block.

Rules

Like SRP, AppLocker lets you create rules defining what programs are allowed to run, and assign them to security groups or individual users (but not to individual computers). You can make three different types of rules:

- Path Rules (allow you to restrict users to launching apps only from specified folders)
- Hash Rules (identify allowed programs based on a cryptographic hash)
- Publisher Rules (identify allowed programs by the digital signature)

Publisher Rules in AppLocker replace the Certificate Rules in SRP. Publisher Rules work with a wider variety of applications and are more flexible. You can restrict applications based on the following information contained in rules:

- Publisher (software company)
- Program name
- File version

This information is in stored in the digital signature. You can apply any of the rules to the following:

- Executable files
- Scripts
- Installation files (such as .msi packages and .dll or .ocx libraries)

You configure AppLocker rules through Group Policy (either domain policies or local security policies). In the local security policy in Windows 7, you'll find AppLocker under the Application Control Policies node.

AppLocker rules are available and can be configured on the following Windows platforms:

- Windows Server 2008 R2
- Windows 7 Ultimate
- Windows 7 Enterprise

AppLocker rules **are not available** on computers running other versions of Windows, for example:

- Windows Server 2008
- Windows 7 Professional
- Windows Vista

AppLocker is a new and improved version of SRP; however, SRP is still included in newer operating systems for compatibility with networks running older versions of Windows.

In a Group Policy Objective (GPO) containing only SRP rules, the rules are enforced on all computers running Windows, including those running Windows Server 2008 R2, Windows 7 Ultimate, and Windows 7 Professional. But, if a GPO contains both SRP rules and AppLocker rules, all the operating systems only read the AppLocker rules. Desktops running other Windows operating systems will use the SRP rules. AppLocker rules will only apply if clients are running the Application Identity Service, which is not configured by default to automatically start Windows 7. Use Group Policy to enforce AppLocker rules; set the Startup Type field to Automatic for the Application Identity Service.

Sometimes the AppLocker feature prevents you from installing a program and you will receive an error message, such as the following.

Also, the SRP feature can block installation, which can also generate an error message.

Windows 7 Enterprise and Windows Server 2008 R2 contain both these security features. AppLocker is an improved version of SRP; however, SRP is still included for compatibility with networks running older Windows versions.

Use the following path to configure AppLocker for local group policy:

From the Group Policy Editor: **Computer Configuration → Windows Settings → Security Settings → Application Control Policies → AppLocker**

Note: Only Windows 7 Enterprise and Windows 7 Ultimate clients support AppLocker. To restrict applications on Windows 7 Professional clients, you must use SRP, in the same manner as with previous versions of Windows.

AppLocker and SRP are similar in the following ways:

- Configured in a GPO
- Establish rules to allow/deny access to applications
- Specify paths to files

However, AppLocker is an improvement over SRP in the following ways:

- AppLocker provides a publisher rule condition that provides administrators with the best way to specify a program; by extracting information from its digital signature.
- The publisher information, which replaces Certificate Rules in SRP, can be used to allow or deny access to programs.
- AppLocker blocks all programs that are not allowed.
- AppLocker assigns rules to specific users and groups (as opposed to SRP where you can only create universal rules).
- You can create a rule with an exception. For example, to run an application while excluding a certain file.
- AppLocker contains the audit only mode feature, which allows you to test configuration without enforcing AppLocker rules. This allows you to audit AppLocker rules for a certain file type. (You can configure Audit Mode in the properties of AppLocker node of a GPO.
- You can import and export rules from other computers, allowing administrators to easily copy and edit rules.

While working with AppLocker and creating a GPO to deploy a software package to Windows 7 users in your domain, use the Microsoft Installer (MSI) format. This provides the highest level of control for administrators.

Publisher information can be used to create rules pertaining to:

- General publisher
- General application version
- Specific application version
- Previous application version
- Future application version

Adding publisher information in AppLocker is a great improvement over SRP. In SRP, there is no comparable way to restrict access to an application through multiple updates. If you specify a path to an application to restrict, users can move the program to a new path to avoid the restriction. If you specify a hash for the application, you have to create a new rule every time you update the program.

AppLocker restricts all programs that are not specifically allowed. In SRP, rules by default are used to block access to chosen applications. However, within many company networks, the number of applications that you want to block typically far exceeds the number that you want to allow. AppLocker accounts for this contradiction by locking all applications that are not allowed. Windows 7 enables AppLocker to create rules for one of four file types:

- Windows Installer programs
- Executables
- Scripts
- DLL files

After AppLocker is enabled, all the applications of that file type are locked if the rule prevents them. AppLocker provides the Create Default Rules and Automatically Create Rules options to prevent system lockouts. These options allow administrators to enter rules for most applications. You can use AppLocker to make additional rules and change default configuration such as:

- Assign Rules to Users and Groups.
- Exceptions, such as applications containing specific files
- Audit-only mode (you can test your configuration without enforcing AppLocker rules)
- Import and export rules from other systems to edit or re-use rules

To display AppLocker related applications, use the following path from the Event Viewer:

Applications and Services Logs → Microsoft → Windows → AppLocker

Note: you can also automatically generate AppLocker rules by scanning a template computer for executables—any executable found on the template machine will be added to the allowed list.

Identifying and Resolving Software Configuration Issues

If a program on Windows 7 fails, during installation it is probably because:

- The program is not compatible with the version of Windows 7.
- The program configuration settings must be adjusted on the system for the program to upload properly.
- You must locate a different host for the program to install it.

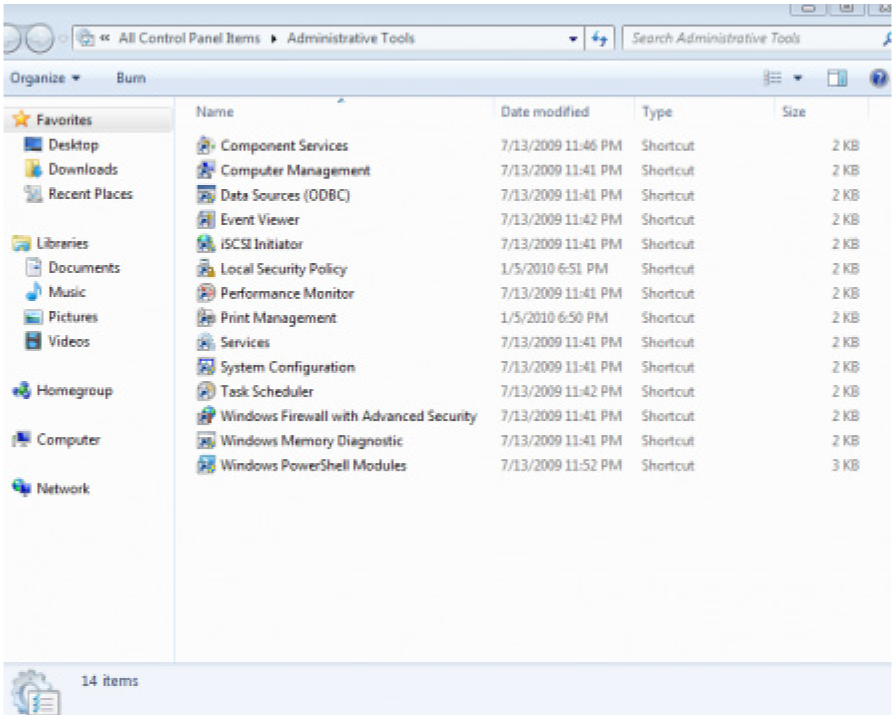
Installed programs that previously worked properly on a system sometimes fail. Configuration setting changes can be the source of the malfunction. The following lists suggested ways of resolving possible configuration issues:

- Application settings.
- If you can open the application, check menus and configuration area settings for compatibility to the software being installed.
- Ensure database or files are not corrupted, if applicable.
- Check network settings and accessibility, if applicable.
- Check out the software manufacturer on the Web for identifiable malfunctions; the installation problem could be resulting from corrupted software that requires a patch or a new issue.

Event Viewer

Event Viewer in Windows 7 can locate program error messages/application logs, and identify when they occurred. If you locate relevant errors, you can then search the Web for Use the following procedure to use the Event Viewer in Windows 7 to check a computer's logs and identify any problems.

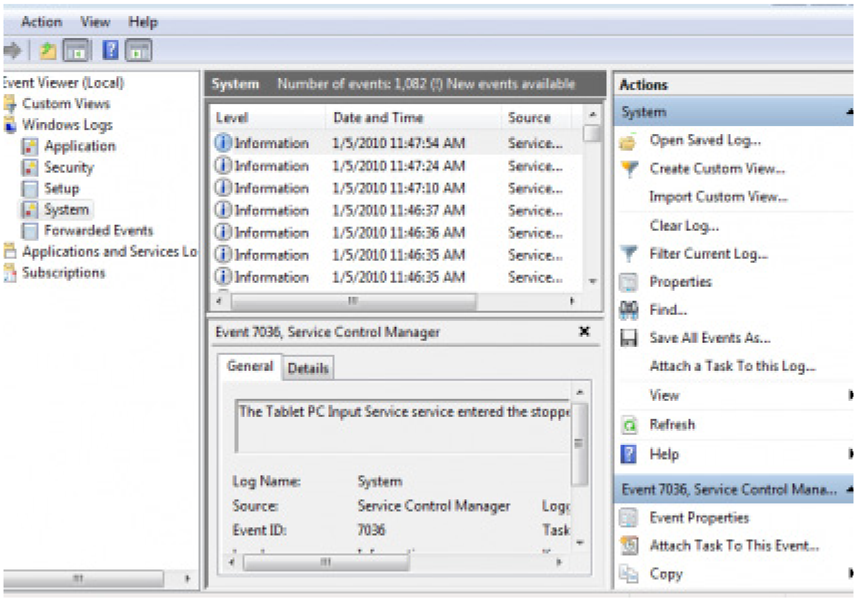
1. Open the Control Panel from the Start Menu.
2. Open Administrative Tools in the Control Panel. **Note:** If Administrative Tools is not available, change View by to Large icons at the top right of the Control Panel.
3. Open Event Viewer in the Administrative Tools window.



Name	Date modified	Type	Size
Component Services	7/13/2009 11:46 PM	Shortcut	2 KB
Computer Management	7/13/2009 11:41 PM	Shortcut	2 KB
Data Sources (ODBC)	7/13/2009 11:41 PM	Shortcut	2 KB
Event Viewer	7/13/2009 11:42 PM	Shortcut	2 KB
iSCSI Initiator	7/13/2009 11:41 PM	Shortcut	2 KB
Local Security Policy	1/5/2010 6:51 PM	Shortcut	2 KB
Performance Monitor	7/13/2009 11:41 PM	Shortcut	2 KB
Print Management	1/5/2010 6:50 PM	Shortcut	2 KB
Services	7/13/2009 11:41 PM	Shortcut	2 KB
System Configuration	7/13/2009 11:41 PM	Shortcut	2 KB
Task Scheduler	7/13/2009 11:42 PM	Shortcut	2 KB
Windows Firewall with Advanced Security	7/13/2009 11:41 PM	Shortcut	2 KB
Windows Memory Diagnostic	7/13/2009 11:41 PM	Shortcut	2 KB
Windows PowerShell Modules	7/13/2009 11:52 PM	Shortcut	3 KB

Figure 3: Administrative Tools in Control Panel

4. Expand Windows Logs and then select System or any of the other logs Windows 7 collects. Double-click one of the logged events in the top center pane of the Event Viewer to see details about the event.



System Number of events: 1,082 (!) New events available

Level	Date and Time	Source
Information	1/5/2010 11:47:54 AM	Service...
Information	1/5/2010 11:47:24 AM	Service...
Information	1/5/2010 11:47:10 AM	Service...
Information	1/5/2010 11:46:37 AM	Service...
Information	1/5/2010 11:46:36 AM	Service...
Information	1/5/2010 11:46:35 AM	Service...
Information	1/5/2010 11:46:35 AM	Service...

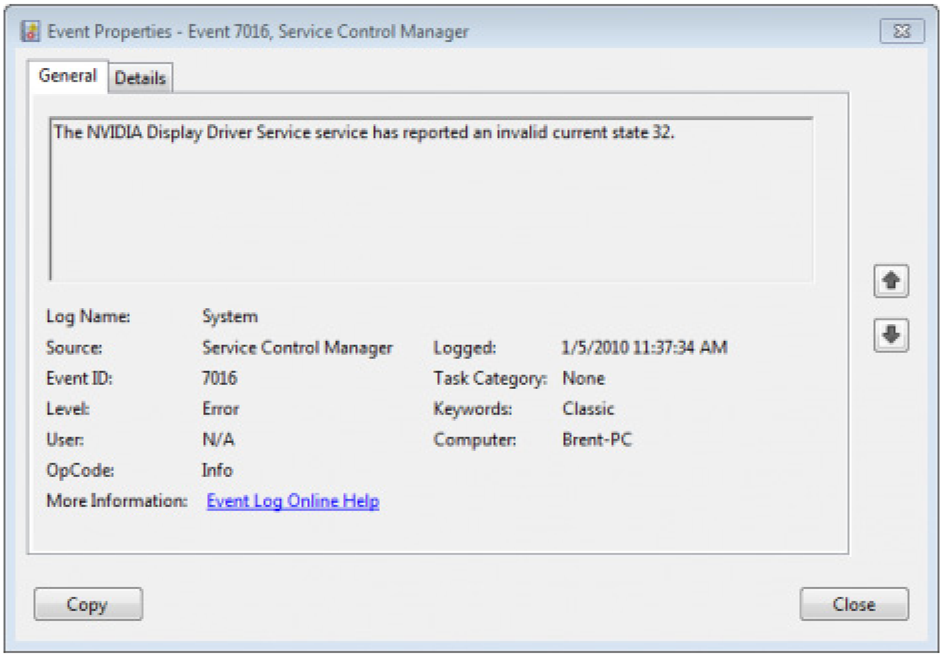
Event 7036, Service Control Manager

The Tablet PC Input Service service entered the stoppe

Log Name: System
Source: Service Control Manager
Event ID: 7036

Figure 4: Event Viewer

5. The Event Properties window shows details about the selected event.



The NVIDIA Display Driver Service service has reported an invalid current state 32.

Log Name: System
Source: Service Control Manager
Logged: 1/5/2010 11:37:34 AM
Event ID: 7016
Task Category: None
Level: Error
Keywords: Classic
User: N/A
Computer: Brent-PC
OpCode: Info
More Information: Event Log Online Help

Figure 5: An Event from Event Viewer

Event Forwarding

If available, use Event Forwarding to help troubleshoot entire networks for software malfunction issues. With this feature you can configure many computers to forward an event to a central collection computer for analysis. This requires you to configure the source computers, and the collector computer.

System Restore

Consider using System Restore to return a system back to a point before operating system configuration changes were made that may have corrupted software functionality. Use the following path to start the System Restore Wizard: Click Start → type **System Restore** → press Enter.

Repair or Reinstall Software

If available, a repair option reinstalls an application while keeping intact user application settings and files. An alternative is to user files, uninstall the software, and then reinstall it. Failing this, you can restore the entire operating system from the last functioning version after backing up all user folders and files.

Application Compatibility

Before making adjustments to improve application compatibility, you should understand security enhancements and operating system changes in Windows 7.

Security Enhancements

Many organizations deploying Windows 7 will be replacing Windows XP on their clients, not Windows Vista. Compared to Windows XP, the Windows 7 environment offers a number of important security-related enhancements. The following security features are the ones most likely to lead to compatibility problems with third-party applications:

- **Internet Explorer Protected Mode –** this feature is included in Windows Internet Explorer 8. It restricts browser access within the registry and file hierarchy, thereby protecting systems from malware. Protected Mode provides security while online; however, it can have adverse affects on the following:
    - Older programs
    - System operation
    - ActiveX controls
    - Script code
- **Operating System and Internet Explorer Versioning** – a variety of applications check the operating system and interface differently or crash when an incompliant version number appears. The solution to this scenario is to set appropriate compatibility modes or apply versioning shims.
- **User Account Control (UAC) –** this enhancement first appeared in Windows Vista. UAC divides standard user privileges from administrator privileges and reduces:
    - Malware
    - Unauthorized software installation
    - Unapproved system changes

  If logged on as an administrator, you are prompted by UAC to confirm tasks requiring administrator privileges. If logged on as a standard user attempting a task requiring admin privileges, UAC prompts you to type administrator credentials instead of just blocking you from performing the task. UAC can cause problems with programs that are not compliant with this enhancement. Therefore, administrators should test applications with UAC enabled before deploying.
- **Windows Resource Protection/File and Registry Virtualization –** this feature comes with Windows Server 2008, Windows Vista, and Windows 7. It functions to stop application requests that write to protected system files or registry locations. It then redirects the application to safe and temporary locations. Most applications adapt to this without generating error messages; however, some applications require full access to protected areas and will not comply with this new process.

Windows 7 System Features

The following Windows 7 operating system changes can create software compatibility issues:

- **64-bit –** Windows 7 does not support 16-bit applications or 32-bit drivers. The registry and system file redirection has changed in Windows 7. Applications must normally must comply with 64-bit technology to run on Windows 7, with the following exceptions:
    - Windows 7x86 does support 16-bit applications or 32-bit drivers.
    - Also, you can purchase 32-bit versions of Windows 7.
    - 64-bit Windows 7 can run Win32 applications in an emulated mode in most cases.

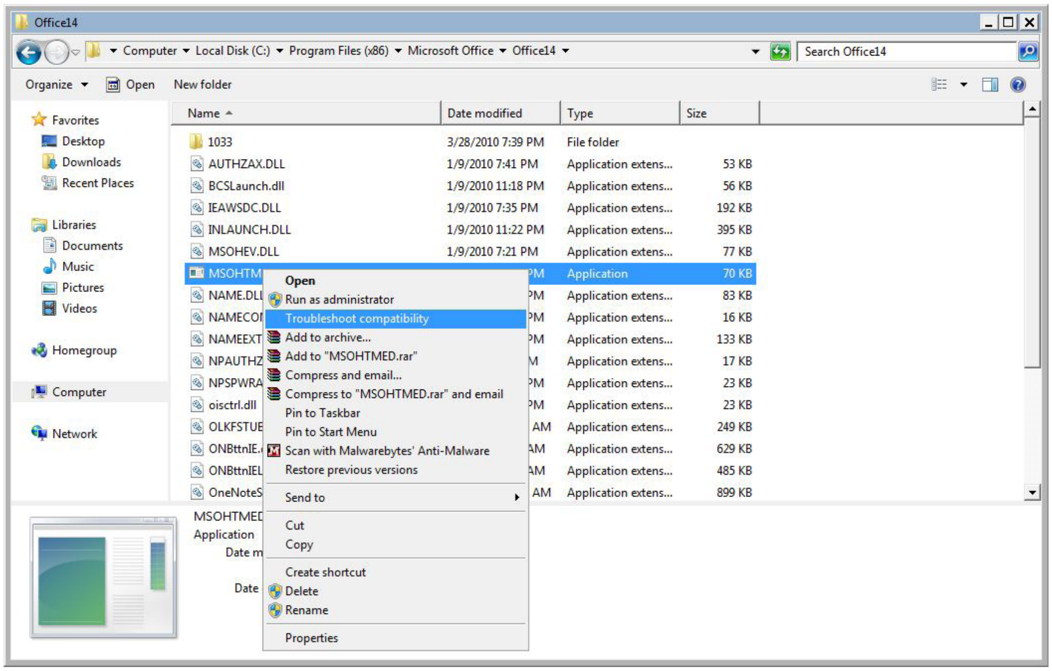
- **Application Programming Interfaces (API s) –** APIs in Windows 7 expose layers of the operating system differently than in other Windows versions. For example, antivirus and firewall software require APIs to monitor and protect Windows 7. Software relying on outdated APIs will require updating or replacement.

- **Operating System –** Some applications check for a specific version of Windows and won't respond if not located. The Program Compatibility Assistant features in Windows 7 usually fix this automatically, albeit automatic.

- **Folder Locations –** the following folder locations have changed on Windows 7:
  - User folders
  - My Documents folders
  - Folders with localization

Some applications with hard-coded paths to folders can fail because of this change. Windows 7 provides the following compatibility tools to help improve compatibility of older programs after deployment:

- **Program Compatibility Troubleshooter (PCT)**: This is a Control Panel program that you can use to configure the compatibility settings for an older program if the program is not running smoothly. To start the wizard, in Control Panel, click Programs>in the Programs and Features category, click Run Programs Made for Previous Versions of Windows. You can also start the Program Compatibility Troubleshooter by right-clicking an application and selecting Troubleshoot Compatibility from the shortcut menu, as shown below.



Name	Date modified	Type	Size
1033	3/28/2010 7:39 PM	File folder	
AUTHZAX.DLL	1/9/2010 7:41 PM	Application extens...	53 KB
BCSLaunch.dll	1/9/2010 11:18 PM	Application extens...	56 KB
IEAWSDC.DLL	1/9/2010 7:35 PM	Application extens...	192 KB
INLAUNCH.DLL	1/9/2010 11:22 PM	Application extens...	395 KB
MSOHEV.DLL	1/9/2010 7:21 PM	Application extens...	77 KB
MSOHTM	PM	Application	70 KB
NAME.DLL	PM	Application extens...	83 KB
NAMECOI	PM	Application extens...	16 KB
NAMEEXT	PM	Application extens...	133 KB
NPAUTHZ	M	Application extens...	17 KB
NPSPWRA	PM	Application extens...	23 KB
oisctrl.dll	PM	Application extens...	23 KB
OLKFSTUE	AM	Application extens...	249 KB
ONBttnIE.	AM	Application extens...	629 KB
ONBttnIEL	AM	Application extens...	485 KB
OneNoteS	AM	Application extens...	899 KB

Figure 6: Troubleshooting Compatibility

- **Compatibility tab** – this tab is found on a Properties dialog box: you can configure compatibility settings on the Compatibility tab within the Properties sheet of a program. The options provided on this tab are the same as those you can configure through the Program Compatibility Troubleshooter. This tab provides a shortcut to running the Program Compatibility Troubleshooter. You can configure compatibility settings on the Compatibility tab within the Properties sheet of any program. The options are the same as those you can configure with the Program Compatibility Troubleshooter wizard.
- **Program Compatibility Assistant (PCA) –** the PCA tool appears automatically when Windows 7 detects program compatibility issues. PCA can offer to fix the problem. For example, PCA can resolve conflicts with UAC, or run a program in a mode simulating earlier Windows versions. If you agree to the changes PCA suggests, the system then performs the fix automatically. If the compatibility issue is more threatening, PCA can display a warning message, or block the program. Alternately, you can **right-click** an application and select **Troubleshoot Compatibility** to start the wizard. If adjusting compatibility settings of a program does not fix the configuration problem, you should locate alternate hosting or obtain an updated version of the program.

Alternate Hosting for Application Compatibility

Sometimes you will be required to support an application with compatibility issues on Windows 7 that cannot be resolved immediately. For example, if you are running a 64-bit version of Windows 7, you cannot run 16-bit applications by adjusting the compatibility settings of the program. Until a more compatible version of the application is available or the client obtains different software that is compatible, you may be required to temporarily fix for this application compatibility problem.

Sometimes the only way to resolve these compatibility inconsistencies is to run the program in a virtual machine with the older Windows operating system that supports it. Or, run the software on a remote server and access it through Remote Desktop. The following lists ways to host an older application on an older operating system:

- Remote Desktop Services for Hosting Applications
- Microsoft Virtual PC 2007
- Windows XP Mode
- Hyper-V on Windows Server 2008

Application Compatibility Toolkit (ACT)

ACT is a tool you can use to identify application compatibility issues before deploying Windows 7. The following are some of the major components of ACT:

- **Setup Analysis Tool (SAT)** – Automates running of application installations and monitors actions taken by each application's installer.
- **Standard User Analyzer (SUA)** – Determines possible issues for applications running as a standard user in Windows 7.
- **Application Compatibility Manager** – This tool is basically the primary user interface of ACT. It helps you to collect and analyze data to identify any issues before deploying a new operating system or Windows update in an organization. This tool is particularly useful for initial phases of application migration.
- **Application Compatibility Toolkit Data Collector** – This interfaces with each computer in a network and uses compatibility evaluators to perform scans. It collects and stores data in a central compatibility database.

Application Compatibility Diagnostics Configuration

Windows Server 2008 includes policy options relating to application compatibility diagnostics. Use the following path to browse these settings in a GPO (this is an arbitrary example):

Computer Configuration → Policies → Administrative Templates → System → Troubleshooting and Diagnostics → Application Compatibility Diagnostics

The Application Compatibility Diagnostics container includes the following six policies, which administrators should understand for the exam:

- Notify Blocked Drivers
- Detect Application Failures Caused By Deprecated Windows COM Objects
- Detect Application Failures Caused By Deprecated Windows DLLs
- Detect Application Install Failures
- Detect Application Installers That Need To Be Run As Administrator
- Detect Applications Unable To Launch Installers Under UAC

Deployment Image Servicing and Management

Deployment Image Servicing and Management (DISM), is a new command-line tool for Windows 7 and Windows Server 2008 R2. DISM consolidates the core image management functions of multiple tools found in the Windows Automated Installation Kit (AIK) and enables administrators to view components of an applied or mounted operating system image and add or remove packages, software updates, and drivers.

Checking Whether the Application Runs in Safe Mode

Safe mode is useful for troubleshooting problems with programs and drivers don't start correctly or are preventing Windows from starting correctly. If a problem doesn't reappear when you start in safe mode, you can eliminate the default settings and basic device drivers as possible causes. If a recently installed program, device, or driver prevents Windows from running correctly, you can start the system in safe mode and then remove the program that's causing the problem.

1. Remove all floppy disks, CDs, and DVDs from the computer, and then restart it.
2. Click the Windows Start button and then click the arrow next to the Shut Down button. Click Restart.
3. Do one of the following:
    a. If the computer has a single operating system installed, press and hold the F8 key as the computer restarts. Press F8 before the Windows logo appears. If the Windows logo appears, you'll need to try again by waiting until the Windows logon prompt appears, and then shutting down and restarting the computer.
    b. If the computer has more than one operating system, use the arrow keys to highlight the operating system to start in safe mode, and then press F8.
4. On the Advanced Boot Options screen, use the arrow keys to highlight the safe mode option you want, and then press Enter.
5. Log on to the computer with a user account that has administrator rights.

When the computer is in safe mode, you'll see the words Safe Mode in the corners of the monitor. To exit safe mode, restart the computer and let Windows start normally.

Domain 2: Identifying Cause of and Resolving Networking Issues

Identify and Resolve Logon issues

Windows 7 supports a variety of authentication techniques, like the traditional user name and password, smart cards, and third-party authentication components. In addition, Windows 7 can authenticate users with the local user database or an AD DS domain.

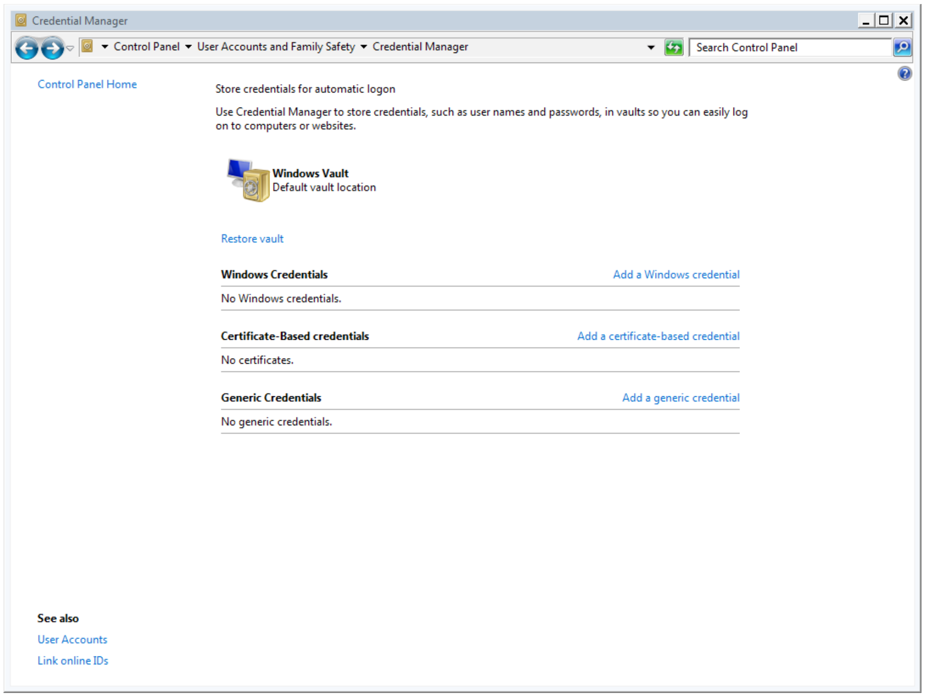
The Credential Manager handles three types of information:

- **Windows Credentials –** stores the usernames and passwords, and the network addresses required for you to access intranet.
- **Certificate-Based Credentials –** stores digitally signed public key certificates that contain your user ID information and your passwords and can be used to log you in to highly secure Web sites.
- **General Credentials –** stores usernames, and passwords, and the URL addresses, required for you to access other Web sites.

In Windows 7, Credential Manager can allow stored user names and passwords to roam between multiple Windows computers in an Active Directory Domain Services (AD DS) domain. Windows stores credentials in the user's AD DS user object. This enables users to store credentials once and use them from any logon session within the AD DS domain and store credentials for Web site access.

To add a user name and password manually to Credential Manager, follow these steps:

1. Click **Start**, and then click **Control Panel**.
2. Click the **User Accounts and Family Safety** link, then click the User Accounts link.
3. In the left pan**e, click the Manage Your Credentials** link.
4. Click **Add A Windows Credential**. Note that you can also add certificate-based and generic credentials.
5. In the **Internet or Network Address** box, type the server name. You can use an asterisk (*****) as a wildcard.
6. In the **User Name and Password** boxes, type your user credentials. Click **OK**.


Credential Manager
Control Panel ▸ User Accounts and Family Safety ▸ Credential Manager
Search Control Panel
Control Panel Home

Store credentials for automatic logon

Use Credential Manager to store credentials, such as user names and passwords, in vaults so you can easily log on to computers or websites.

Windows Vault
Default vault location

Restore vault

Windows Credentials Add a Windows credential

No Windows credentials.

Certificate-Based credentials Add a certificate-based credential

No certificates.

Generic Credentials Add a generic credential

No generic credentials.

See also
User Accounts
Link online IDs

Figure 7: The Credential Manager

Hardware vs. Network logon Issues

Account Lockout

If a user provides incorrect credentials several times in a row, Windows 7 can block all authentication attempts for a specific amount of time. Account lockout settings are defined by Group Policy settings in the Computer Configuration\ Windows Settings\Security Settings\Account Policies\Account Lockout Policies\ node as follows:

- **Account Lockout Threshold** – the number of incorrect attempts allowed before the account is no longer accessible (i.e., the lockout).
- **Reset Account Lockout Counter After** – the amount of time, in minutes, that must elapse before the lockout counter is reset to 0.
- **Account Lockout Duration** – the amount of time, in minutes, that the account is locked out.

Use the **Resultant Set of Policy** tool (**rsop.msc**) to identify a computer's Group Policy settings. To use the Resultant Set of Policy tool, follow these steps:

1. Click Start, type **rsop.msc**, and press **Enter**.
2. In the Resultant Set of Policy window navigate to **Computer Configuration** → **Windows Settings** → **Security Settings** → **Account Policies** → **Account Lockout Policies**.
3. The **Details** pane shows only the account lockout policy settings that have been defined, and which Group Policy object defined them.
4. Clear the **Account Is Locked Out** check box.

To unlock a user's account for Windows Server 2008 R2, AD DS, clear the "Unlock Account" check box and click Apply.

Password Expiration

Experts suggest that users should be required to change their passwords regularly. If hackers are attempting to guess a password, and a password is changed on a regular basis, it makes it harder for the hacker to figure out the passwords. If a hacker has guessed a password, changing the password on a regular basis will cause the hacker to start their efforts over.

In AD DS domains, accounts can be configured to expire. If you want to have a domain user prompted to change their password at specific intervals, then you must make sure that the Password never expires checkbox is not checked for the user account. Edit the account's properties, select the Account tab, and set the Account Expires value to a date in the future.

Password expiration settings are configured by Group Policy settings in the Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy node.

- **Maximum Password Age –** specifies the time before a password expires.
- **Password History –** specifies the number of different passwords that users must have before they can reuse a password.
- **Minimum Password Age –** specifies the time before users can change their password again.

Windows prompts a user to change their password automatically if their password has expired. Accounts can be configured to expire in AD DS domains. To reactivate an expired account, edit the account's properties, select the Account tab, and set the Account Expires value to a date in the future. If the account should never expire, you can set the value to Never.

Changing Passwords

To change the current user password:

1. Ctrl+Alt+Del
2. Select Change a password option
3. Type the current password for the account in the old password text box
4. For a Domain account, specify the domain and the account name
5. Type in the new password
6. Confirm the new password
7. Click arrow to confirm the change

Trust Relationships with Machine Accounts

A trust relationship is a logical relationship created between domains to allow pass-through authentication. A trusting domain honors the logon authentications of a trusted domain. There are two domains in a trust relationship—the trusting and the trusted domain.

Domains located in separate forests are not automatically set up to trust each other. As an administer you have to manually request that a trust relationship be created between the two domains. Open GPMC, (Group Policy Management Console), located in Administrative Tools.

If an attempt to logon to a domain server fails, and you get the following error: "The trust relationship between this computer and the primary domain failed." You should remove the machine from the domain and then join the domain again. This process will recreate the trust relationship between the machine and the domain and regenerate the machine or computer account in the domain. **You must be a domain administrator to run this command.**

To remove a computer from the domain:
Open a command prompt:
Type:
net computer \\computername /add

To join a computer to a domain:

1. Open the System Properties window by clicking the Start button, right-clicking Computer, and then clicking Properties.
2. Under **Computer name, domain, and workgroup settings**, click **Change settings**. If you're prompted for an administrator password or confirmation, type the password or provide confirmation.
3. Click the **Computer Name** tab, and then click **Change**. Alternatively, click Network ID to use the Join a Domain or Workgroup wizard to automate the process of connecting to a domain and creating a domain user account on your computer.
4. Under **Member of**, click **Domain**.

Determining Logon Context

User logon restrictions set for the domain only apply to the domain accounts, and logon restrictions set for local accounts only apply to the local account. One way to determine a user logon context is to display the current variables.

To display current variables:

1. Open a command prompt.
2. Type SET without parameters to display all the current environment variables.

Look at the USERDOMAIN line, if the user logged on with a local user account, this will be the computer name. If the user logged on with an AD DS user account, this will be the name of the domain.

If more than one user logs into either a laptop or stationary computer running Windows 7, you can keep the last user name that logged into the computer from not being displayed the next time a user logs into the same computer. Using the **Interactive Logon** group policy setting, select "Do not display last user name". This would require the users to enter their logon name and password each time and would not allow the logon name to be retained between logons.

When roaming profiles are used, it can cause a delay in the first logon when the user logs onto another computer if the user has any files saved onto their desktop.

To determine if a connectivity issue is in the network or a problem with the computer, you can connect a laptop to the same network connection as the PC computer. If the laptop makes a connection to the network, then the problem is likely in the PC's configuration. Anytime you suspect a network issue, the first things you should always check are:

Make sure the network cable is connected from the Ethernet port on the computer to the network outlet on the wall (or into a router or switch). Check the LED lights on the network adapter are lit, indicating an active network connection.

To verify if a computer is logged into a specific domain Go to the command prompt:

1. Type in **whoami**.
2. The user account will be displayed/Domain Name/ User name.

User accounts that are set up as part of a domain will have mandatory profiles. An administrator can set up the user accounts so that they will not be able to change colors, wallpapers or other settings. The set profiles will remain the same each time the user logs into the domain.

Logon Hours Compliance

Logon Hour Restrictions

Administrators can configure logon restrictions to enforce a company's security needs. The logon restrictions that can be set include locking accounts after several incorrect attempts entering in an incorrect password, setting up specific hours that users can log on, setting up user accounts that would require the user to change their passwords regularly, setting accounts to expire on a specific date, and disabling accounts.

To restrict a users logon hours:

1. Use the Account tab of an AD DS user's properties to restrict logon hours.
2. Click Logon Hours to display the dates and times for setting the logon limitation for the user.
3. If the user logs on during a time not allowed, Windows 7 displays an error message "Your account has time restrictions that prevent you from logging on at this time. Please try again later." See the sample window, below:

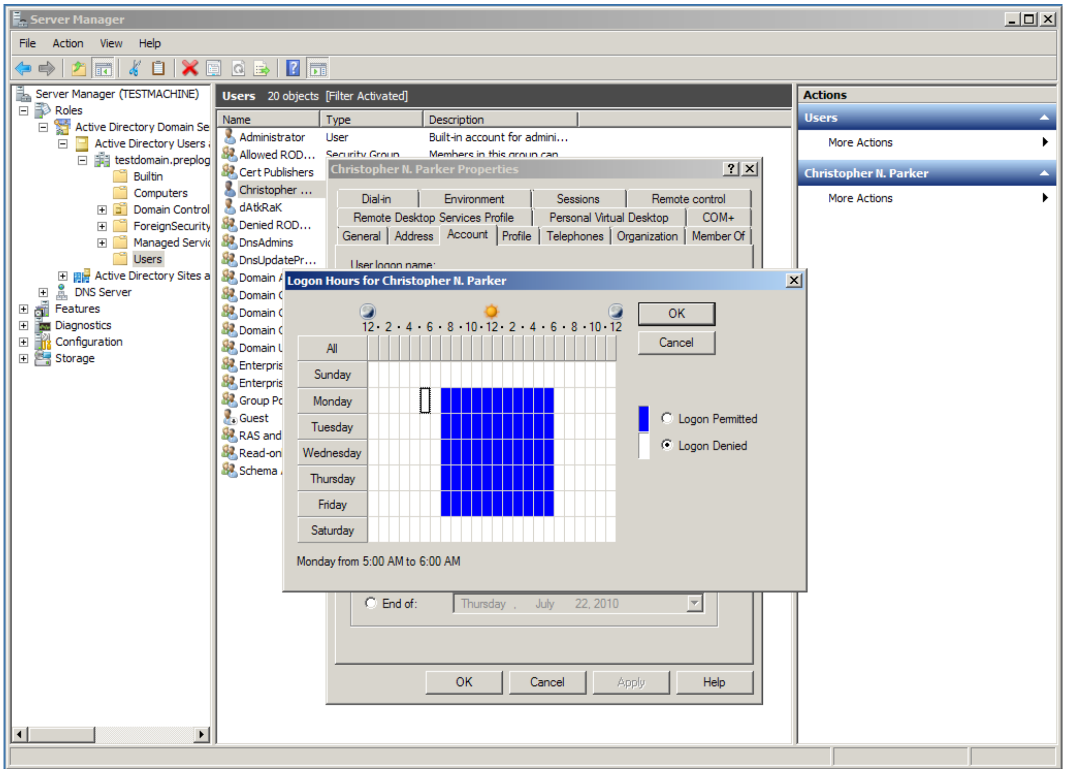


Figure 8: Setting Logon Hour Restrictions

Identify and Resolve Connectivity Issues

Determining the Scope of an Issue

For computers running on a Widows 7 network to communicate with servers on a different subnet, there must be a default gateway (usually a router) for clients to communicate with the nodes on the other subnet.

Determining whether it's a PC or Network Connectivity Issue

Control Panel Troubleshooters

Open the Action Center and click Troubleshooting. If you want to review a complete list of all available troubleshooters without categories, click View All. To troubleshoot a network adapter, you would choose Hardware and Sound, select Network Adapter. This will troubleshoot Ethernet, wireless, or other network adapters.

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

Windows Network Diagnostics

Windows 7 can automatically test for and resolve common network issues. To start the automatic troubleshooter, perform the following steps:

1. Open **Network And Sharing Center**.
2. On the **Network Map**, if there's a problem, you should see an **X**. Click it.
3. Click the **Troubleshoot Problems** link, near the bottom of the right pane.
4. The **Network Sharing** page appears.

Once Windows Network Diagnostics completes the diagnostics, it will list the detected problems. In the sample window below, the "Problems found" message shows that the Domain Name System (DNS) server was unavailable by stating "Windows can't communicate with the device or resource (primary DNS server)". Since no computers were able to be identified by host name, there is a total connectivity failure. To correct this problem, either bring the DNS server back online, or you may need to configure a different IP address for the DNS server.

Windows Network Diagnostics can quickly identify problems that would normally take a person a good amount of time to diagnose.

You can use Event Viewer to review the detailed Windows Network Diagnostics information after running the diagnostics. This helps you to understand the problem, and further assists in troubleshooting, if required. Use the following procedure to perform this task:

1. Click **Start**, right-click **Computer** and click **Manage.**
2. Select **Computer Management** then expand **System Tools** and finally **Event Viewer**.
3. Choose the **System Log** under **Windows Logs.**
4. In the **Actions** pane, click **Filter Current Log.**
5. In the dialog box, click the **Event Sources** list and select Diagnostics-Networking. Click **OK.**

The Event Viewer displays a list of events generated by Windows Network Diagnostics.

Network Troubleshooting Tools

In Windows 7, you can use many other tools manually to assist you in troubleshooting.

Ipconfig is the most common network tool used by administrators. To see a computer's current IP address, from the command prompt, you can simply type ipconfig.

For a much more comprehensive look at a computer's network configuration, type:

```
C:\ipconfig /all
        Windows IP Configuration
        Host Name ............: WIN7
        Primary Dns Suffix .......:
        Node Type ............: Mixed
        IP Routing Enabled.........: No
        WINS Proxy Enabled.........: No
        Ethernet adapter Local Area Connection:
        Media State ...........: Media disconnected
        Connection-specific DNS Suffix . :
        Description ...........: Broadcom NetXtreme 57xx Gigabit Controller
        Physical Address..........: 00-15-C5-07-BF-34
        DHCP Enabled...........: Yes
        Autoconfiguration Enabled ....: Yes
        Wireless LAN adapter Wireless Network Connection:
        Connection-specific DNS Suffix . :
        Description ...........: Intel(R) PRO/Wireless 3945ABG Network Connection
        Physical Address..........: 00-13-02-1E-E6-59
        DHCP Enabled...........: Yes
        Autoconfiguration Enabled ....: Yes
        IPv4 Address...........: 192.168.1.122(Preferred)
        Subnet Mask ...........: 255.255.255.0

        Lease Obtained..........: Wednesday, August 05, 2009 12:48:35 PM
        Lease Expires ..........: Thursday, August 06, 2009 12:48:34 PM
        Default Gateway .........: 192.168.1.1
        DHCP Server ...........: 192.168.1.1
        DNS Servers ...........: 192.168.0.1
        NetBIOS over Tcpip.........: Enabled
```

In this sample ipconfig result, you should notice the following information:

- The wired Ethernet controller is disconnected
- The computer is connected to a wireless network
- A Dynamic Host Configuration Protocol (DHCP) server assigned the computer the IP address of 192.168.1.122
- The default gateway is IP address 192.168.1.1
- The DNS server address is 192.168.0.1

To refresh a computer's current IPv4 address assignment, from the command line type:

```
ipconfig /release
```

This causes Windows 7 to drop the current IP configuration (if it has one). Next, enter:

```
ipconfig /renew
```

This attempts to contact a DHCP server to retrieve a new configuration.
To change a computer's current IPv6 address, from the command prompt:

```
ipconfig /release6
ipconfig /renew6
```

Ping

Ping is another network diagnostic tool, which uses Internet Control Message Protocol (ICMP). Most local area networks (LANs), will allow this type of request, however, many new computers and routers block ICMP, so ping will not work in these environments.

To use Ping, from the command prompt:

```
ping www.sample.com

Pinging sample.com [207.46.197.35] with 32 bytes of data:
Reply from 207.46.197.35: bytes=32 time=95ms TTL=105
Reply from 207.46.197.35: bytes=32 time=210ms TTL=105
Reply from 207.46.197.35: bytes=32 time=234ms TTL=105
Reply from 207.46.197.35: bytes=32 time=258ms TTL=105
Ping statistics for 207.46.197.35:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milliseconds:
Minimum = 95ms, Maximum = 258ms, Average = 199ms
```

In this sample ping result, you should notice the following information:

- When you receive replies, you know that the network host is connected to the network.
- The time, measured in milliseconds (ms), indicates the round-trip latency (delay between sending a packet and receiving a response) between you and the remote host. *Latency* is the delay between sending a packet and receiving a response. If you notice a surprisingly high latency, there may be a network issue impeding traffic.

PathPing

To test the connectivity to a remote host and all the routers between a computer and the remote host, use PathPing, which also uses ICMP. PathPing can help diagnose problems with your network routing, such as a failed router, routing loops, and networks that are performing poorly.

To use PathPing, from the command prompt:

```
pathping www.sample.com
```

If the information received from PathPing shows a single router with an extremely high latency, that node could be causing network problems. Usually, a router that has a high latency affects the latency for all the routers after it with an increase in latency. Routers respond to ICMP requests at a low priority, so be aware that if PathPing shows a high latency, it does not always mean an overall latency issue.

The syntax for pathping is as follows:

Pathping [-g *host-list*] [-h *maximum_hops*] [-I *address*] [-n] [-p *period*] [-q *num_queries*] [-w *timeout*] [-P] [-R] [-T] [-4] [-6] *target_name*

Option	Description
-g *host-name*	
-h *maximum_hops*	Specifies the maximum number of hops to search for the target.
-I *address*	Specifies a source address.
-n	Forces pathping not to resolve addresses to hostnames.
-p *period*	Specifies a period (in ms) to wait before sending a ping.
-q *num_queries*	Specifies a number of queries per hop.
-w *timeout*	Specifies a timeout (in ms) to wait before timing out each reply.
-P	Tests for RSVP PATH connectivity.
-R	Tests whether or not each hop is RSVP aware.
-T	Tests connectivity to each hop with Layer-2 priority tags.
-4	Forces pathping to use IPv4.
-6	Forces pathping to use IPv6.

Figure 9: Pathping Command-Line Switches

Nslookup

To verify a host name to an IP address from a DNS server, you can use Nslookup.

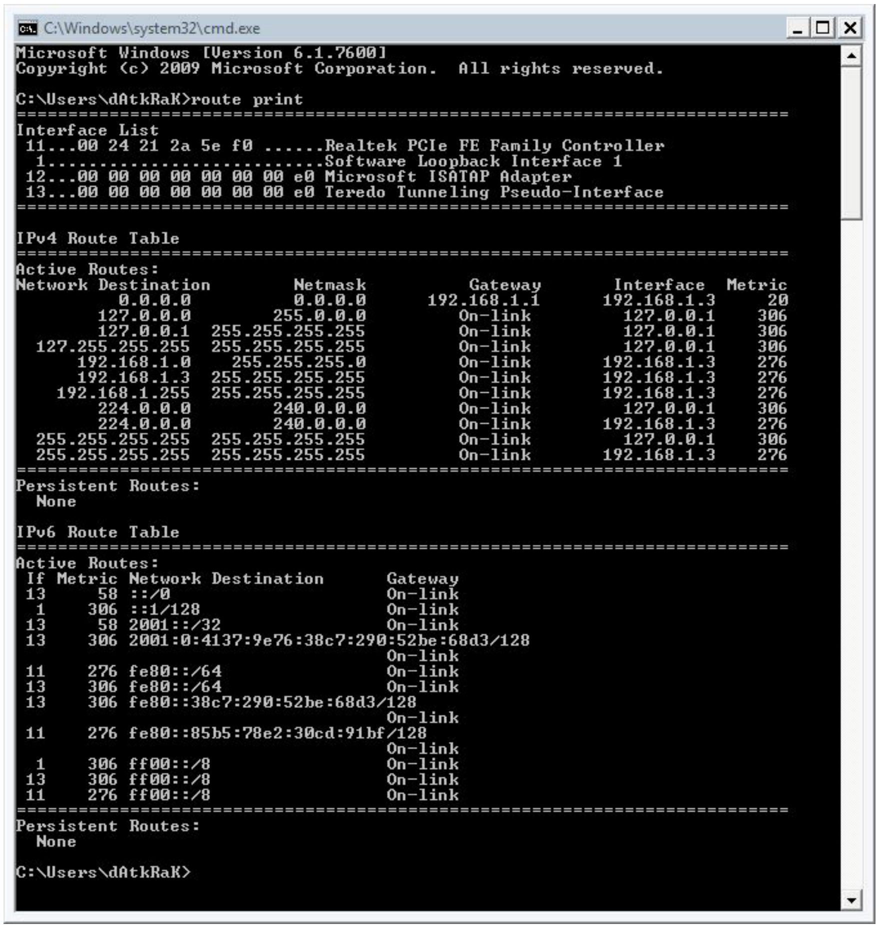
To use Nslookup, from the command prompt, type:

```
nslookup sample.com
Server: dns.example.com
Address: 192.168.1.1:55
Non-authoritative answer:
Name: sample.com
Addresses: 207.46.232.185, 207.46.197.35
```

In this sample nslookup result, you should notice the following information:
The DNS server appears to be working correctly since the client contacted the default DNS server (192.168.1.1) and successfully received a response indicating that sample.com has two IP addresses: 207.46.232.185 and 207.46.197.35.

Route Print

Routing tables are an important part of Windows' TCP/IP protocol stack. To view routing tables, you will have to open a Command Prompt window and then enter the ROUTE PRINT command. Upon doing so, you will see a screen similar to the one that's shown below:



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

C:\Users\dAtkRaK>route print
===========================================================================
Interface List
 11...00 24 21 2a 5e f0 ......Realtek PCIe FE Family Controller
  1...........................Software Loopback Interface 1
 12...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
 13...00 00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.1.1      192.168.1.3     20
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    306
      192.168.1.0    255.255.255.0         On-link       192.168.1.3    276
      192.168.1.3  255.255.255.255         On-link       192.168.1.3    276
    192.168.1.255  255.255.255.255         On-link       192.168.1.3    276
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link       192.168.1.3    276
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link       192.168.1.3    276
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
 13     58 ::/0                     On-link
  1    306 ::1/128                  On-link
 13     58 2001::/32                On-link
 13    306 2001:0:4137:9e76:38c7:290:52be:68d3/128
                                    On-link
 11    276 fe80::/64                On-link
 13    306 fe80::/64                On-link
 13    306 fe80::38c7:290:52be:68d3/128
                                    On-link
 11    276 fe80::85b5:78e2:30cd:91bf/128
                                    On-link
  1    306 ff00::/8                 On-link
 13    306 ff00::/8                 On-link
 11    276 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None

C:\Users\dAtkRaK>
```

Figure 10: The Route Print Command

If you look at the Route Print screen, you will notice that the routing tables are divided into five different columns. The first column is the network destination column. This column lists all of the network segments that the router is attached to. The netmask column provides the subnet mask not of the network interface that's attached to the segment, but of the segment itself. This basically allows the router to determine the address class for the destination network.

The third column is the gateway column. Once the router has determined which destination network it needs to send the packet to, it looks at the gateway listing. The gateway listing tells the router which IP address the packet should be forwarded through in order to reach the destination network.

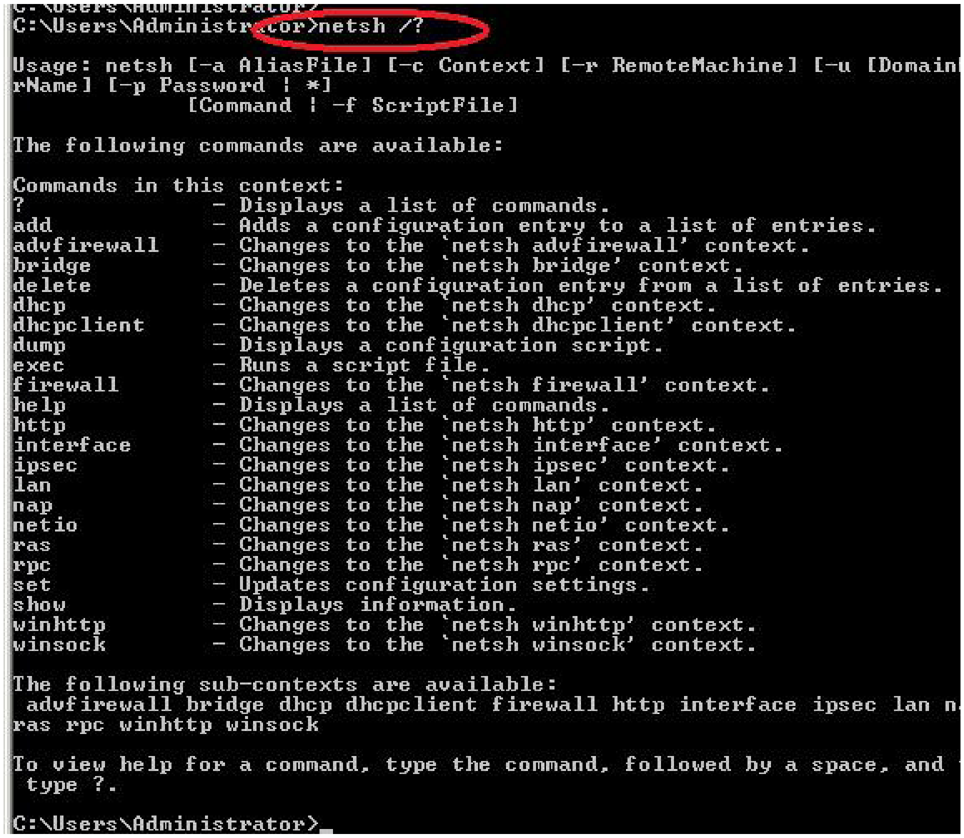
The Interface column tells the router which NIC is connected to the appropriate destination network. Technically, the interface column only tells the router the IP address that has been assigned to the NIC that connects the router to the destination network. However, the router is smart enough to know which physical interface the address has been bound to.

The final column in the routing table is the Metric column.

NETSH

Network shell (netsh) is a command-line utility that you can use to configure and display the status of network communications server roles and components.

Every Windows admin should know how to get guided help with netsh. This is easy – just use the "/?" command to be guided through what you are trying to do. For example, to show all netsh contexts (categories of options), just type: *netsh /?*



```
C:\Users\Administrator>
C:\Users\Administrator>netsh /?

Usage: netsh [-a AliasFile] [-c Context] [-r RemoteMachine] [-u [Domain
rName] [-p Password | *]
             [Command | -f ScriptFile]

The following commands are available:

Commands in this context:
?              - Displays a list of commands.
add            - Adds a configuration entry to a list of entries.
advfirewall    - Changes to the `netsh advfirewall' context.
bridge         - Changes to the `netsh bridge' context.
delete         - Deletes a configuration entry from a list of entries.
dhcp           - Changes to the `netsh dhcp' context.
dhcpclient     - Changes to the `netsh dhcpclient' context.
dump           - Displays a configuration script.
exec           - Runs a script file.
firewall       - Changes to the `netsh firewall' context.
help           - Displays a list of commands.
http           - Changes to the `netsh http' context.
interface      - Changes to the `netsh interface' context.
ipsec          - Changes to the `netsh ipsec' context.
lan            - Changes to the `netsh lan' context.
nap            - Changes to the `netsh nap' context.
netio          - Changes to the `netsh netio' context.
ras            - Changes to the `netsh ras' context.
rpc            - Changes to the `netsh rpc' context.
set            - Updates configuration settings.
show           - Displays information.
winhttp        - Changes to the `netsh winhttp' context.
winsock        - Changes to the `netsh winsock' context.

The following sub-contexts are available:
 advfirewall bridge dhcp dhcpclient firewall http interface ipsec lan n
ras rpc winhttp winsock

To view help for a command, type the command, followed by a space, and
 type ?.

C:\Users\Administrator>
```

Figure 11: Results of netsh /? help options

APIPA Address

When a computer is configured to use automatic IP addressing but is unable to contact a DHCP server, Windows 7 assigns an **Automatic Private IP Addressing (APIPA)** address in the range of 169.254.0.0 through 169.254.255.255, with a subnet mask of 255.255.0.0.

An APIPA address allows a computer to connect to a LAN when it is unable to communicate with, or doesn't have access to, a DHCP server. When a computer is assigned an APIPA address, that computer will only be able to connect to other computers that have APIPA.

An APIPA address can be assigned to a computer due to some of the following reasons:

- The DHCP server was temporarily unavailable.
- The computer was not connected to the network properly.
- The computer was not authorized to connect to the network.

Troubleshooting Connectivity Problems

Network connectivity problems keep all applications from accessing a network resource. Some of the most common reasons are as follows:

- Misconfigured network adapter
- Misconfigured network hardware
- Failed network connection
- Faulty network cables
- Failed network adapter
- Failed network hardware

Application connectivity problems keep only specific applications from accessing resources. Some of the most common reasons are as follows:

- The remote service is not running.
- Remote Desktop may not be enabled on the remote computer.
- A firewall on the remote server may be configured to block a specific application's communication from a client computer.
- A firewall between the server and client computer may be blocking a specific application's communications.
- The local computers Windows Firewall may be set to block a specific application.
- A port number other than the default port number may have been set on the remote service.

TCP/IP

The minimum IPv4 configuration items that must be set on a Windows 7 computer for a multi-segment network are:

- A unique IP address for each computer
- A subnet mask that specifies the network address and the host address of the IP
- A DNS server is required in a domain environment

Network Connection Problems

There can be many causes when troubleshooting connections problems, so try these steps first:

- Open Network Diagnostics by right-clicking the network icon in the notification area, and then clicking Diagnose and repair.
- Make sure that all wires are connected such as your modem being connected to a working cable connection either directly or through a router.
- If you're trying to connect to another computer, make sure that computer is on and that you have enabled file and printer sharing on your network.
- If your computer has a wireless network adapter, Windows will automatically detect wireless networks that are nearby. To see a list of wireless networks that Windows has detected, click the Start button, and then click Connect to. If Windows does not detect a network that you think is in range of your computer, open Help and Support and search for "Troubleshoot problems finding wireless networks."
- If the problem began after you installed new software, check your connection settings to see if they have been changed.

    1. Open Network Connections by clicking the Start button, clicking Control Panel, clicking Network and Internet, clicking Network and Sharing Center, and then clicking Manage network connections.
    2. Right-click the connection, and then click Properties. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.

- Check your router, there are some older routers that are not fully compatible with Windows Vista or Windows 7, and can cause problems.

Identify and Resolve Name Resolution Issues

Before two computers can communicate, the client must translate the server's host name to an IP address or the IPv6 address. This is called *name resolution*. Usually, a DNS server performs name resolution and returns the IP address to the client computer. If you are having problems connecting to the DNS server, you should first try and diagnose the problem with Windows Network Diagnostics. If that does not solve the problem, verify that the computer is connected to the local network by going through the following steps:

- Try connecting to other computers using IP addresses. If you still cannot connect to a server by using its IP address, then your problems is most likely network connectivity instead of a name resolution issue.
- Use ipconfig to get the default gateway, then use ping to see if you get a reply from the server. If you do receive a reply, then the problem is most likely due to a name resolution issue.
- Use Nslookup using the host name you are trying to connect to. If this resolves the name, then the name resolution is not the issue. It could be possible that the server is offline, or traffic could be blocked by a firewall, it's possible that the DNS server is incorrect and is returning an invalid IP address, or it could be the program being used is not configured properly.
- If you get the message "DNS request timed out" when you run Nslookup, make sure that the computer has the correct IP addresses listed for the DNS servers. If the IP addresses are listed correctly then it is possible that the server or the network they are connected to is offline.
- If you get the message "Default servers are not available" when you run Nslookup, then the problem would appear to be that the computer doesn't have a DNS server configured. You would then need to setup the client network configuration with the DNS server IP addresses.

The Hosts file is where the computer checks first to find name to IP address mappings. You can use the hosts file to make it easy for you to identify your computers with names instead of IP addresses.
In Windows 7, the location of the hosts file hasn't changed.

Managing the DNS Cache

To View the DNS Cache:

- Open a command prompt and run the following command:
  - ipconfig /displaydns

The output shows every record in the DNS cache, the type of record, the time to live (TTL), and the address or CNAME record that the record resolves.

To Clear the DNS Cache:

- Open a command prompt and run the following command:
  - ipconfig /flushdns

Afterwards, you can run **ipconfig /displaydns** to verify that the DNS cache is empty. If it is empty, Windows 7 displays the message, "Could not display the DNS Resolver Cache."

Note: the DNS cache can also be cleared by stopping and restarting the DNS Client service.

Checking which DNS is Assigned

To ensure that dynamic DNS registration occurs on a Windows 7 client computer, verify that the "Register this connection's addresses in DNS" has been checked in the Advanced TCP/IP Settings.

Identify and Resolve Network Printer Issues

Using the Printer Troubleshooter

If you are having a problem connecting to a **shared printer**, follow these steps to open the Printer Troubleshooter:

1. Click **Start** and then click **Control Panel**.
2. Click **System and Security**.
3. Under **Action Center**, click **Troubleshoot Common Computer Problems**.
4. Under **Hardware and Sound**, click **Use a Printer**.
5. The **Printer Troubleshooter** appears and attempts to diagnose the problem. Follow the steps that appear.
6. On the **Troubleshoot and Help Prevent Computer Problems** page, click **Next**.
7. On the **Which Printer Would You Like To Troubleshoot?** page, click **My Printer Is Not Listed**. Click **Next**.
8. Respond to the prompts that appear to troubleshoot your problem.

If you are having a problem printing to an **existing printer**, follow these steps to run the Printer Troubleshooter:

1. Click **Start** and then click **Devices and Printers**.
2. Right-click the printer and then **Troubleshoot**.
3. The **Printer Troubleshooter** appears and attempts to diagnose the problem.
4. Respond to the prompts that appear.

The Printer Troubleshooter can detect the following problems:

- The printer is turned off.
- The printer has a paper jam.
- The printer is out of paper.
- The printer is out of toner.
- No physical printer is installed.
- A new printer hasn't yet been detected.
- The printer is not the default printer.
- The printer is not shared.
- The printer driver needs to be updated.
- A print job is preventing other print jobs from printing.
- The Print Spooler service is not running or has an error.

Monitoring Printer Events

In Windows 7 printer-related events are stored in: Applications and Services Logs\Microsoft\Windows\PrintService\Admin event log. You must be logged in as an administrator to access the event log. Common events (or errors) can surround:

- Connecting to a network printer
- Sharing a printer
- Changing the default printer
- Initializing a new printer or driver

Windows 7 can add events to the Security event log when users connect to a printer. To add an event when users connect, use Group Policy to enable success or failure auditing for the Audit Logon Events policy in the Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy node.

Windows 7 provides many Group Policy settings that configure the behavior of printers and printer drivers in the Computer Configuration\Administrative Templates\Printers node. Also, you can configure client computers to connect automatically to a shared printer by adding the printer to the Computer Configuration\Windows Settings\Deployed Printers or User Configuration\Windows Settings\Deployed Printers node.

- **Override Print Driver Execution Compatibility Setting Reported by Print Driver –** print drivers contain driver isolation compatibility flags that indicate if the driver should be run in a separate process from the print spooler. If you enable this setting, the print spooler runs all print drivers in a separately, despite their driver isolation compatibility flag. If the print spooler is failing, you should enable this setting.
- **Execute Print Drivers in Isolated Processes** – the print spooler, by default, stores print drivers in isolated process, so the print spooler functions if a print driver fails. The default setting is best for troubleshooting, but if the print spooler is failing, you should verify the setting is disabled.
- **Allow Print Spooler to Accept Client Connections –** this setting prevents a computer from acting as a print server. If you experience problems sharing a printer, verify that this setting is enabled (the default).

Print Servers

Connecting a printer directly to the network can reduce your costs by not requiring a server. Also, a printer that is shared from the network does not go offline if the server fails. Depending on the capabilities of the printer, a direct network connection can be the best choice for a client. However, configuring a computer to act as the print server can present the following advantages:

- Integration with Windows security
- Integration with AD DS browsing
- Automatic installation of printer drivers
- Integration with enterprise management tools

For a computer to share printers, it must have two services running:

- **Server –** this service is required for sharing either files or printers across the network.
- **Print Spooler –** this service is required for printing.

Printer Sharing Management

Follow these steps to manage a shared printer in Windows Server 2008 R2 or Windows 7:

1. Click **Start**, and **Devices and Printers**.
2. **Right-click** the printer and click **Printer Properties**.
3. Select the **Share This Printer** check box on the Sharing tab.

How to Manage Print Jobs on a Printer

In Windows Server 2008 R2 or Windows 7, follow these steps to manage a shared printer:

1. Click **Start**, and then click **Devices and Printers**.
2. Double-click the printer you want to manage.
3. Click **See What's Printing**.
4. Windows displays the print queue, a list of documents waiting to be printed. You can right-click any document and click Pause, Restart, or Cancel.

Print Queue
If a document won't leave the print queue, you can restart the Print Spooler service and do one of the following:

- Use the Services node in the Computer Management tool.
- Run net stop spooler and net start spooler from an administrative command prompt.
- Run net stop spooler & net start spooler in one command.

Or, you can remove documents in queue by:

1. Stopping the Print Spooler service.
2. Delete all files in the %WinDir%\System32\Spool\
3. The Printers folder (through Explorer). The folder has two files for every document in the print queue: (SHD file, and.SPL).
4. Start the Print Spooler service.

Driver Problems

Drivers control communications between the operating system and hardware. Use the Device Manager Device Manager\Printer Properties dialog box to manage printer drivers.

How to Update a Driver for the Print Server
Windows 7 detects the new hardware and attempts to install a driver automatically when you connect a new printer. If the default driver causes installation issues, follow these steps to install a different driver:

1. Click **Start**, and then click **Devices and Printers**.
2. Right-click the printer you want to manage and then click **Printer Properties**.
3. On the **Advanced** tab, click **New Driver** to add a driver.
4. The **Add Printer Driver Wizard** guides you through the process. You can select a driver built in to Windows, download a driver from Windows Update, or choose a driver that you have saved to the hard disk.

If a driver installation fails, causing the printer to stop working. The fastest way to reinstall the driver is to reinstall the printer. If reinstalling the printer does not solve the problem, you can remove files related to the driver installation manually.

How to Add Drivers for Shared Printer Clients
When connecting to a new printer, clients running Windows can install automatically drivers that are stored on the print server. By default, the print server has only the drivers required for the print server to print. For example, a 64-bit print server running Windows 7 has 64-bit printer drivers but not 32-bit printer drivers. Therefore, 64-bit clients running Windows 7 automatically install the driver from the print server, but 32-bit clients running Windows 7 need to download a driver from Windows Update or prompt users to provide their own drivers.

While managing the print server, you can store drivers for different processor architectures for a specific printer, or you can store drivers for any model of printer you specify. For example, you can add a 32-bit printer driver to a 64-bit print server and allow 32-bit Windows 7 clients to automatically download the driver.

If updating the driver does not solve the problem, or only one version of the driver is available, you should determine whether disabling advanced printing features resolves the problem. To disable advanced printing features for a printer, follow these steps:

1. Click Start, and then click Devices and Printers.
2. Right-click the printer and then click Printer Properties.
3. On the Advanced tab of the printer properties dialog box, clear the Enable Advanced Printing Features check box and click OK.

Domain 3: Managing and Maintaining Systems That Run Windows 7 Client

Identify and Resolve Performance Issues

Windows 7 was designed to perform better than any previous Windows operating system; but issues can still arise with computers have limited processor, memory, and disk resources. Because you can't create a completely problem free computing environment, Administrators must identify and resolve performance problems quickly when they do occur. Windows 7 has several features that help resolve performance problems, including:

- Task Manager
- Analyzing started services
- Analyzing forwarding events
- Disk Cleanup
- Performance Monitor
- System Configuration

To prepare for the exam, you should have access to a system with Windows 7 installed and connected to a network.

Task Manager

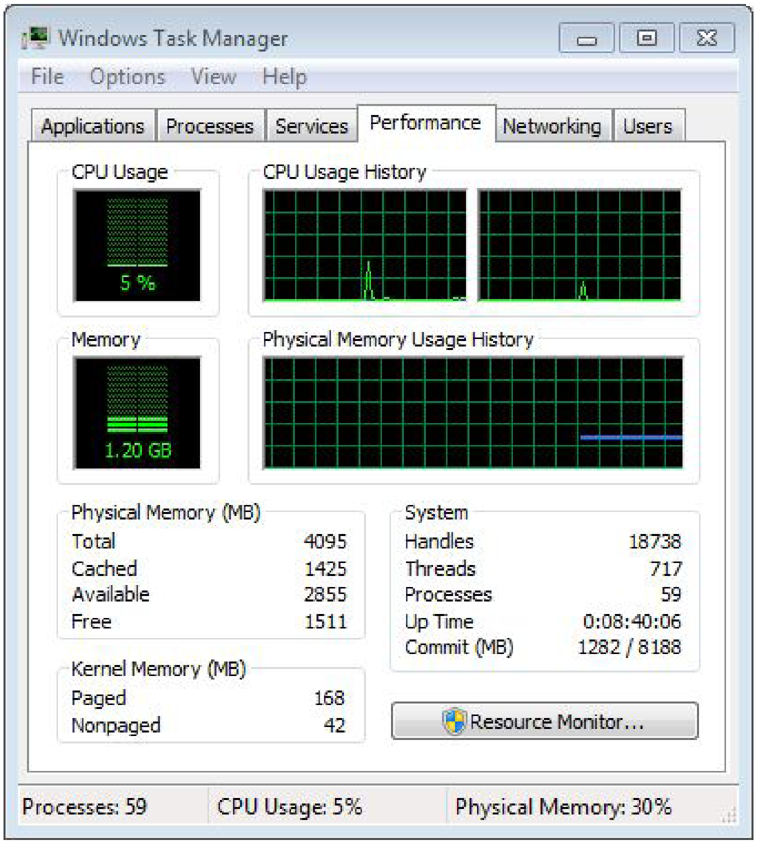
Task Manager is the quickest way to identify typical performance problems. Use the following path to open Task Manager:

Right-click the taskbar and then click **Start Task Manager**. Alternately, you can press Ctrl+Alt+Del and click **Start Task Manager** or go directly to the Task Manager with Ctrl+Shift+Esc.

Task Manager has six tabs, five of which are explained below for the purposes of our discussion on Task Manager in this Domain:

- **Networking:**
    - This tab starts the network utilization interface.
    - Can identify if an application is using up too much bandwidth making the network run slowly.
- **Services:**
    - This tab lists all the services logged on the computer. This access through Task Manager is an alternative to accessing the Services console. You can start and stop services here.

- **Applications:**
    - This tab provides a list of open applications; click End Task to close a program.
- **Processes:**
    - This Tab provides a list of open processes. Click Show Processes from All Users to view the list. This helps determine if a certain process is using too much processing time and draining the CPU. You can end the process from here.
- **Performance:**
    - This tab displays processor and memory use. You can troubleshoot a slow running system here.



Physical Memory (MB)

Total	4095
Cached	1425
Available	2855
Free	1511

Kernel Memory (MB)

Paged	168
Nonpaged	42

System

Handles	18738
Threads	717
Processes	59
Up Time	0:08:40:06
Commit (MB)	1282 / 8188

Processes: 59 CPU Usage: 5% Physical Memory: 30%

Figure 12: The Windows Task Manager

Windows 7 Processor Sharing

- Processes and threads are related.
- A service or application normally has only one process related to it.
- Processes run within threads. Each application has a minimum of one thread, and the application can start multiple threads.
- A processor can only run one thread at a time.
- A computer with one processor can run multiple applications: Windows 7 switches the processor between different processes and threads.
- Higher-priority threads get more processor time than lower-priority threads. Newer computers have multiple cores. Processor cores act like separate processors.

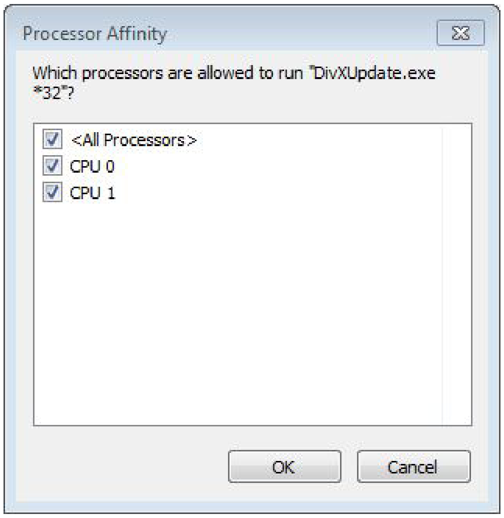
From Task Manager, click the Performance tab to view CPU usage on the History graph. Windows 7 automatically distributes processor time among applications and their threads and processor cores.

Sometimes you may be required to adjust these default control process settings, for example, the following scenarios:

- A certain process is using too much processor time.
- You want a certain application to get more processing time than others.
- You want to manually end an application.

Locating Programs and Their Processor Time
Task Manager can identify a process that uses too much processor time. Follow these steps to end the process if required:

- Start Task Manager.
- Click CPU on the Processes tab.
- On the top of the list, processes appear that use excessive processing time.
- You can then:
    - end the process.
    - change the priority of the process.
    - direct the process to specific processor cores. Do this by right-clicking the process and selecting "Set Affinity…"



Which processors are allowed to run "DivXUpdate.exe *32"?

☑ <All Processors>
☑ CPU 0
☑ CPU 1

Figure 13: Setting Processor Affinity

Stopping a Program

Occasionally, a program might not respond. Typically, you can right-click the application on the task bar and then click Close. In a few seconds, Windows prompts you to terminate the nonresponsive application. If that approach does not work, you can use Task Manager to close an application as follows:

1. In Task Manager, on the Applications tab, select the application.
2. Click End Task.
3. If Task Manager cannot end the application, the End Program dialog box appears. Click End Now. If you want to identify which process is associated with an application, right-click the Application on the Applications tab, and then click Go to Process.

Analyzing Forwarding Events

In Windows 7, the operating system and applications can contain different events; some just provide information, other events are more critical such as the following:

- Indicating hard disk failure.
- Identifying security compromise.
- Controlling network access.

How Event Forwarding Works

Event forwarding in Windows 7 and Windows Vista help enterprises manage local event logs. You can configure computers running Windows to forward important events to a central location. You can then more easily monitor and respond to centralized events.

Event forwarding in Windows 7 and Windows Vista helps you manage local event logs; you can configure systems to forward important events to a central location to monitor.

Event forwarding uses the same protocols as Web sites use to send events to a central computer where Web masters monitor them:

- Hypertext Transfer Protocol (HTTP)
- or HTTPS (Hypertext Transfer Protocol Secure)

Domain environments such as Microsoft Negotiate security support provider (SSP) or Microsoft Kerberos SSP encrypt information in workgroup environments. HTTPS uses a Secure Sockets Layer (SSL) certificate for additional encryption if necessary.

Note: Event forwarding uses encryption despite choosing an HTTP protocol; as opposed to unencrypted Web browsers.

How to Configure Event Forwarding or Workgroup

Event Subscription is used in Windows 7 to configure the forwarding and collecting of events on computers in AD DS Domains or a workgroup.

To use event forwarding, the **forwarding** and **collecting** computers must be running:

- Windows Remote Management
- Windows Event Collector
- And, the forwarding computer must have a Windows Firewall exception for the HTTP protocol

How to Configure the Forwarding Computer

Use the following steps to configure the forwarding computer running Windows 7 to forward events: click **Start** → type **cmd** → press Ctrl+Shift+Enter. At the Admin command prompt, type **winrm quickconfig** to start the Windows Remote Management service. If WinRM is not set up to receive requests, then make the following changes:

- Set the WinRM service type to delayed auto start. Start the WinRM service.
- Type Y at the prompt and press Enter. The Windows Remote Management service prompt appears:
    - WinRM has been updated to receive requests.
    - WinRM service type changed successfully.
    - WinRM service started.

If WinRM is not set up to allow remote access to this machine for management, then create a WinRM listener on HTTP://* to accept WS-Man requests to any IP on the system:

1. Enable the WinRM firewall exception, choose y (yes).
2. Type **Y**, and then press Enter. The Windows Remote Management service prompts you again. WinRm) configures the computer to accept WS-Management requests from other computers. Make the following system changes:
3. Set the Windows Remote Management (WS-Management) service to Automatic (Delayed Start) and starts the service.

4. Configure a Windows Remote Management HTTP listener. A listener configuration setting forwards specific incoming network communications to an application.
5. Creates a Windows Firewall exception to allow incoming connections to the Windows Remote Management service using HTTP on Transmission Control Protocol (TCP) port 80. This exception applies only to the Domain and Private profiles; traffic will still be blocked while the computer is connected to Public networks.

Adding Computer Account to Local Event Log Readers on Forwarding Computer
Use the following steps to add the computer account of the collector computer to the local Event Log Readers group on each of the forwarding computers:

1. Click **Start → right-click Computer → click Manage**.
2. Access **System Tools → Local Users and Groups → select Groups/double-click Event Log Readers → click Add**.
3. In the Select Users, Computers, Service Accounts, Or Groups dialog box, click Object Types.
4. Select the Computers check box and clear the Groups, Users, and Service Accounts check boxes. Click OK.
5. In the Select Users, Computers, Or Groups dialog box, type the name of the collecting computer. Then, click OK.
6. Click OK again to close the Event Log Readers Properties dialog box.

You could also complete this task from an elevated command prompt or a batch file by running the following command: **net localgroup "Event Log Readers" <computer_name>$@<domain_name> /add**

How to Configure the Collector Computer
There are two types of event forwarding subscriptions in Windows 7:

- **Collector-initiated –** the collecting computer establishes (pulls) a connection to the forwarding computer.
- **Source computer–initiated –** the forwarding computer establishes a connection (pushes) to the collecting computer. Source computer–initiated subscriptions are the only subscription type available in workgroup environments. If you plan to use collector-initiated subscriptions, Windows 7 prompts you to configure the collecting computer when you create a subscription.

Use the following steps to pre-configure a collecting computer:

1. Click Start to open an elevated command prompt, type **cmd**, and press **Ctrl+Shift+Enter**.
2. Run the **wecutil qc** command to configure the Windows Event Collector service.
3. Press Y when prompted. Windows configures the Windows Event Collector service. If you want to use source computer–initiated subscriptions (only available on Windows 7), you must run **winrm quickconfig** on the collecting computer.

Analyzing System Application Event Logs

If you are working in the Event Viewer on a Windows 7 client, and you are required to locate an entry in the System log with a certain Event ID, without filtering the log, you should perform the following steps. Click the Find item in the Actions panel and enter the Event ID code in the Find What field, and then click Find Next. The search dialog is accessed by clicking the Find item in the Actions panel. You can also press F3 to cycle through the list of matching event log entries after you've entered the search phrase in the Find dialog. Alternatively, you can press CTRL+F to initially bring up the Find dialog.

To monitor a system for a specific event log entry to be added to the Windows 7 Security event log without having to continually monitor the log, attach a task to an event. Use the Event Viewer to create a scheduled task that watches for the event to occur. Should the event occur, the specified action is taken in the scheduled task.

If you want to configure the system's Security log to a specific maximum size, but you want to automatically archive the Security log file when it is full rather than overwriting the file. Perform the following:

- Check the **Archive the log when full, do not overwrite events** option on the General tab of the Security Log Properties dialog. This option will ensure that the log is backed up whenever it reaches the **Maximum log size (KB)** setting. The archive is stored in the same directory as the active log.
- Also you can Right-click on the Security log in the **Event Viewer –Windows Logs** section and select Properties. This action will open the Security Log Properties dialog for modification.
- Alternatively, you can manually set the maximum log size (KB) value to required size. The Security log defaults to a size of 20480 in Windows 7. You will have to change this value to meet the demands of the scenario.

Disk Performance Problems

For many tasks on a computer, the hard disk limits performance. Opening and saving files requires reading from and writing to the hard disk, which is much slower than accessing system RAM.

If Windows needs to allocate more memory with now available physical RAM, it uses the hard disk as virtual memory, reducing performance.

You can perform several tasks to improve performance without necessarily upgrading to a faster hard disk.

Fragmentation

When disks begin to run out of space, Windows must divide files into different fragments, this is known as fragmentation. Disks perform better when files are not fragmented, fragmentation slows disk performance. The more available disk space, the better the disk will perform.

To reduce fragmentation, increase the amount of free disk space. When a disk begins to run out of space, Windows needs to separate files into different fragments (fragmentation). Fragmentation slows disk performance. In general, the more free disk space available, the better the system performs.

Disk Cleanup

Traditional, magnetic hard disks have a drive head that must move across several spinning round platters to read data, much like a record player. These drives perform best when reading and writing sequentially, which does not require the drive head to move to a different part of the disk. To read a fragmented file, the drive head must move several times, slowing performance. Flash drives do not have a drive head, and fragmentation does may not reduce their performance. Windows 7 automatically disables defragmentation for flash drives.

Use Windows 7 Disk Cleanup tool to free up disk space automatically by following these steps:

1. Click Start\Computer.
2. Right-click the drive to clean, and then click Properties.
3. On the General tab, click Disk Cleanup.
4. Click Clean up System Files to remove system files.
5. Select the files to delete. Click OK. The Disk Cleanup tool removes the specified files.

Defragmentation

Note: You can use Windows 7 Disk Cleanup to automatically free up disk space. However, Windows 7 automatically defragments your files, so you should rarely need to defragment manually.

If you need to defragment files manually, perform these steps:

1. Click Start\Computer.
2. Right-click the drive to defragment, and click Properties.
3. On the Tools tab, click Defragment Now.
4. Click Configure Schedule to configure the defragmentation schedule.
5. Select the disk to defragment in the Disk Defragmenter tool, and click Defragment Disk. The Disk Defragmenter begins defragmenting the drive.
6. Click Close\OK.

Virtual Memory

For many common tasks on a system, the hard disk limits overall performance. Opening and saving files requires reading from and writing to the hard disk, which is much slower than accessing built-in system RAM. If Windows needs to allocate more memory than it has physical RAM available, it uses the hard disk as virtual memory, reducing performance for any task that requires the memory stored on the hard disk. There are several ways to improve performance upgrading to a faster hard disk. The sections discuss fragmentation and virtual memory.

Verify that adequate free space exists on your disk volumes for virtual memory paging files and application data files. Insufficient free space might cause Stop messages and other symptoms, including disk corruption. Check the minimum system requirements recommended by the software publisher before installing an application. Determine the amount allocated to paging files you can move, delete, or compress unused files manually or by using Disk Cleanup (Cleanmgr.exe) to increase free space on disk volumes.

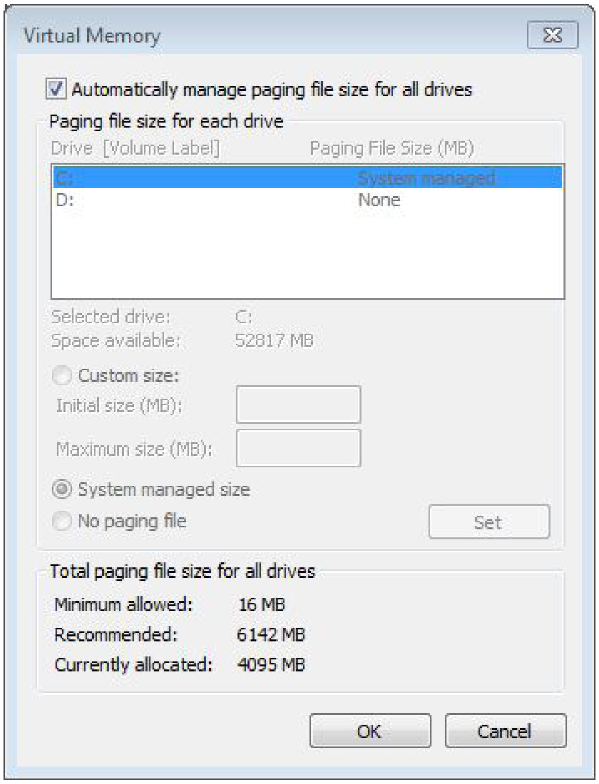
Depending on the disk configuration, you can maximize the performance of virtual memory paging files on a system by storing it on a different physical hard disk from other files.

Storing Virtual Memory Paging Files on a Separate Disk

Although you can improve performance benefits by storing virtual memory paging files on a separate hard disk, you will not see any benefits by storing virtual memory on a different volume or partition of a single hard disk. For best performance with multiple disks, configure the disks in a redundant array of independent disks (RAID) array, and store all data on that RAID array.

Complete these steps to configure a certain disk for Windows 7 to store virtual memory paging files:

1. Click **Start**, right-click **Computer** and click Properties.
2. Click **Advanced System Settings**.
3. On the **Advanced** tab of the **System Properties** dialog box, click **Settings** in the **Performance** group.
4. On the **Advanced** tab of the **Performance Options** dialog box, click **Change**.
5. Clear the **Automatically Manage Paging File Size for All Drives** check box.
6. Select the drive (paging file) to store virtual memory.
7. Click **System Managed Size**, then OK.
8. Select the system drive which currently has the paging file assigned to it. Click **No Paging File**, and then click **Set**.
9. Click **Yes** when prompted.


Virtual Memory

☑ Automatically manage paging file size for all drives

Paging file size for each drive

Drive [Volume Label]	Paging File Size (MB)
C:	System managed
D:	None

Selected drive: C:
Space available: 52817 MB

○ Custom size:
Initial size (MB):
Maximum size (MB):
● System managed size
○ No paging file

Total paging file size for all drives

Minimum allowed:	16 MB
Recommended:	6142 MB
Currently allocated:	4095 MB

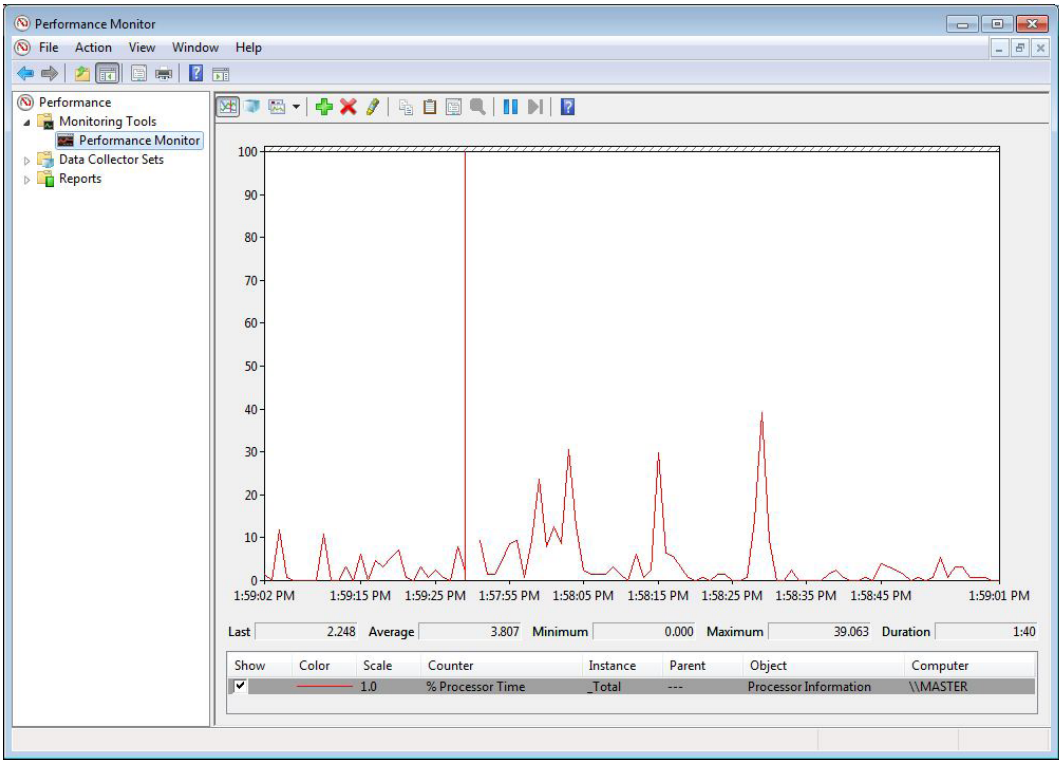
Figure 14: Virtual Memory Settings

10. Click OK four times; then Restart.

Performance Monitor

The most recommended tools for identifying system performance problems are Task Manager and Performance Monitor. Both tools can determine which process use the most processor time and memory in real-time. You can then examine the application and determine why it was consuming so many resources.

The Performance Monitor snap-in displays real- time data:



Last 2.248 Average 3.807 Minimum 0.000 Maximum 39.063 Duration 1:40

Show	Color	Scale	Counter	Instance	Parent	Object	Computer
☑	🟥	1.0	% Processor Time	_Total	---	Processor Information	\\MASTER

Figure 15: Performance Monitor

To open Performance Monitor to monitor real-time data, follow these steps:

1. Click **Start**, right-click **Computer**, and then click **Manage**.
2. Expand **System Tools**, expand **Performance**, and then expand **Monitoring Tools**. Select **Performance Monitor**.
3. Add counters to the real-time graph by clicking the green plus button on the toolbar. You can also display data from other computers on the network. Each line on the graph appears in a different color. To make it easier to view a specific graph, select a counter and press Ctrl+H. The selected counter appears bold and in black on the graph. Performance Monitor automatically assigns line colors and styles to the counters you select. You can change these manually if you want (Action Menu\Properties\Data).

Configuring Power Settings

Power usage can affect computer performance and lifetime. For example, laptop computers batteries fail in correspondence with usage. To help with this issue, Windows 7 provides different power plans and switches between them automatically when a computer is plugged in or running on battery. However, the default battery power plan can reduce performance. To set the power plan manually, perform these steps:

1. Click the power icon in the system tray, and then click More Power Options.
2. Click Change Plan Settings.
3. Click Change Settings That Are Currently Unavailable.
4. Change the display and sleep settings for times when the computer is plugged in or running on battery.
5. To change other settings, click Change Advanced Power Settings. Adjust the settings, and then click OK. Some helpful performance-related settings include:
    - **Turn Off Hard Disk After –** Windows can turn the hard disk off to save power if it is not used for a specific amount of time. Realistically, though, applications continue to use the hard disk even if the user is not actively working with the computer.
    - **Wireless Adapter Settings –** wireless adapters can use a significant amount of battery power because they must transmit and receive radio signals. By default, Windows 7 enables power saving for wireless connections when running on battery power. If wireless performance significantly decreases while on battery power, you can change the power saving mode to Maximum Performance while on battery power.
    - **Sleep –** in Windows Vista and Windows 7, Sleep is a power-saving mode that combines both *Standby* (a low-power state that allows the computer to recover in a few seconds) and *Hibernation* (a zero-power state that stores the computer's memory to disk, but takes longer to recover). By default, Sleep in Windows 7 initially enters Standby mode and then enters Hibernation 20 minutes later. Adjust this setting to change that default.
    - **USB Settings –** USB devices draw power from a computer. With USB selective suspend, Windows 7 can reduce the power usage of some USB devices. By default, USB selective suspend is enabled while Windows 7 is on battery power.
    - **Power Buttons and Lid –** by default, Windows 7 automatically enters sleep mode when the lid of a mobile computer is closed. You can change this setting and configure how the power button functions.
    - **PCI Express –** some mobile computers have a PCI Express interface. This setting configures the power savings mode used for the PCI Express interface when on battery power or plugged in.
    - **Processor Power Management –** most modern processors can run at different speeds depending on the current processing requirements. When less processor time is needed, the processor runs slower, requiring less power. You can use these settings to change the minimum and maximum speed of the processor.
    - **Multimedia Settings –** you can use this setting to adjust video quality when on battery power. Enabling a higher video quality increases battery usage.
    - **Battery –** adjust how Windows responds when a battery begins to run out of power.
6. Click Save Changes.

Checking Hard Drive Space

The **chkdsk** command checks a disk drive for errors; it also reports the free space on the drive. See the chkdsk topic later in this manual. You can also use the following to check for disk drive for errors:

- Windows Explorer for a graphical view.
- Disk Management MMC snap-in.

Defrag Command

Execute the defrag d: /v /u /x command if you want to:

- Defragment the **D:** drive on a local machine.
- View verbose information about the defragmentation process.
- Show the progress of the process on the screen.
- Consolidate free space during defragmentation.

The **d:** parameter specifies that the **D:** drive should be defragmented. The **/v** parameter specifies verbose output. The **/u** parameter indicates that the progress of the operation should be printed to the screen. The **/x** switch indicates that free space consolidation should be performed.

System Configuration

To disable a startup program or service by using the System Configuration Utility, follow these steps:

1. Click Start, type **msconfig**, and press Enter.
2. To disable a service at startup, select the Services tab and clear the check box for the service.
3. To disable a startup program, select the Startup tab and clear the check box for the application.
4. Click OK. When prompted, click Restart. When Windows restarts, the changes you have made take effect.
5. When the computer restarts, determine whether your changes improved the computer's performance. If disabling the startup program or service did solve the problem, you can investigate it further. If there was no benefit, use the System Configuration utility to re-enable the startup program or service. You can remove a startup program permanently using Control Panel. To prevent a service from starting automatically, use the Services console.

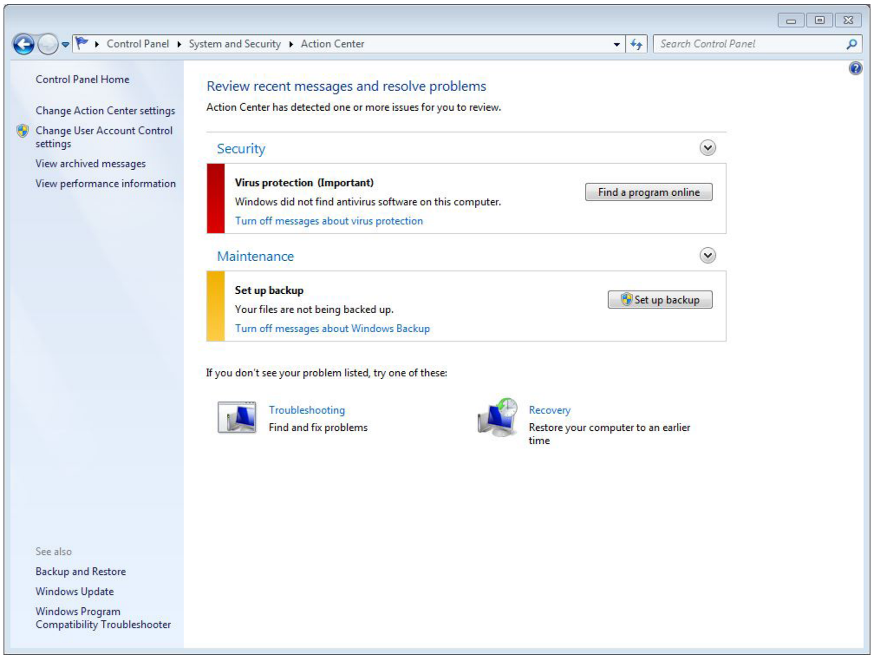
Identify and Resolve Hardware Failure Issues

This domain helps you diagnose faulty hardware on Windows 7, using built-in support such as:

- Hardware Troubleshooting Tools
- Action Center
- Windows 7 Troubleshooter
- Device Manager
- Reliability Monitor
- Event Viewer
- Startup Repair
- Memory Diagnostic
- Chkdsk (Hard Disk)
- Disk Defragmenter

Windows 7 Action Center

The Action Center (previously referred to as Security Center) is normally the best place to start troubleshooting a problem with a system. Security warnings and action alerts appear in the Action Center. They can be software or hardware related. Click the flag icon in the notification area of the taskbar to display the Action Center.



Control Panel ▸ System and Security ▸ Action Center
Search Control Panel
Control Panel Home
Change Action Center settings
Change User Account Control settings
View archived messages
View performance information
See also
Backup and Restore
Windows Update
Windows Program Compatibility Troubleshooter

Review recent messages and resolve problems

Action Center has detected one or more issues for you to review.

Security

Virus protection (Important)

Windows did not find antivirus software on this computer.

Turn off messages about virus protection

Maintenance

Set up backup

Your files are not being backed up.

Turn off messages about Windows Backup

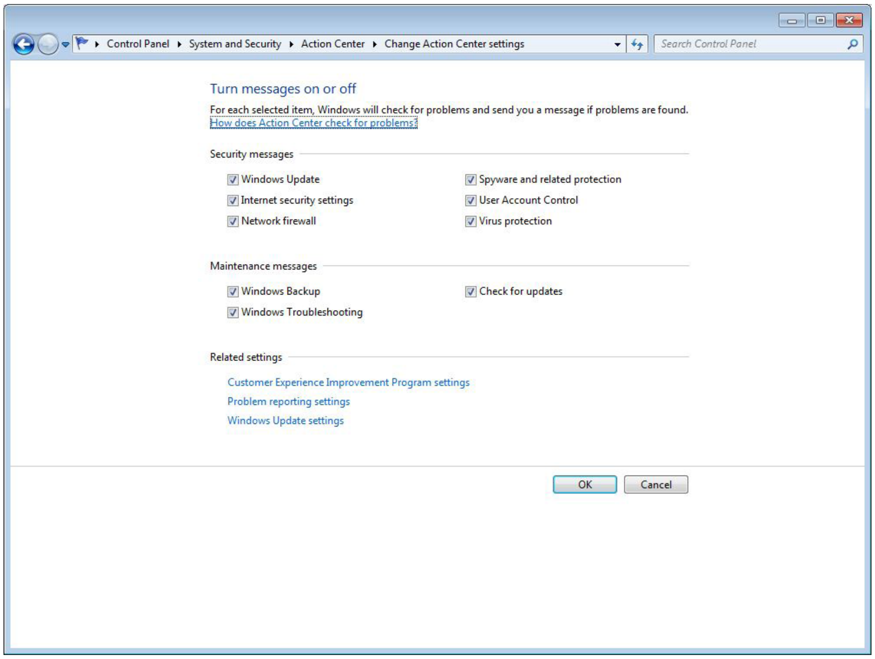
If you don't see your problem listed, try one of these:

Troubleshooting
Find and fix problems

Recovery
Restore your computer to an earlier time

Figure 16: The Action Center

Make sure settings for troubleshooting messages are set to appear. You can also open the Control Panel troubleshooters and Reliability Monitor from here.



Control Panel ▸ System and Security ▸ Action Center ▸ Change Action Center settings
Search Control Panel

Turn messages on or off

For each selected item, Windows will check for problems and send you a message if problems are found.

How does Action Center check for problems?

Security messages

☑ Windows Update ☑ Spyware and related protection
☑ Internet security settings ☑ User Account Control
☑ Network firewall ☑ Virus protection

Maintenance messages

☑ Windows Backup ☑ Check for updates
☑ Windows Troubleshooting

Related settings

Customer Experience Improvement Program settings
Problem reporting settings
Windows Update settings

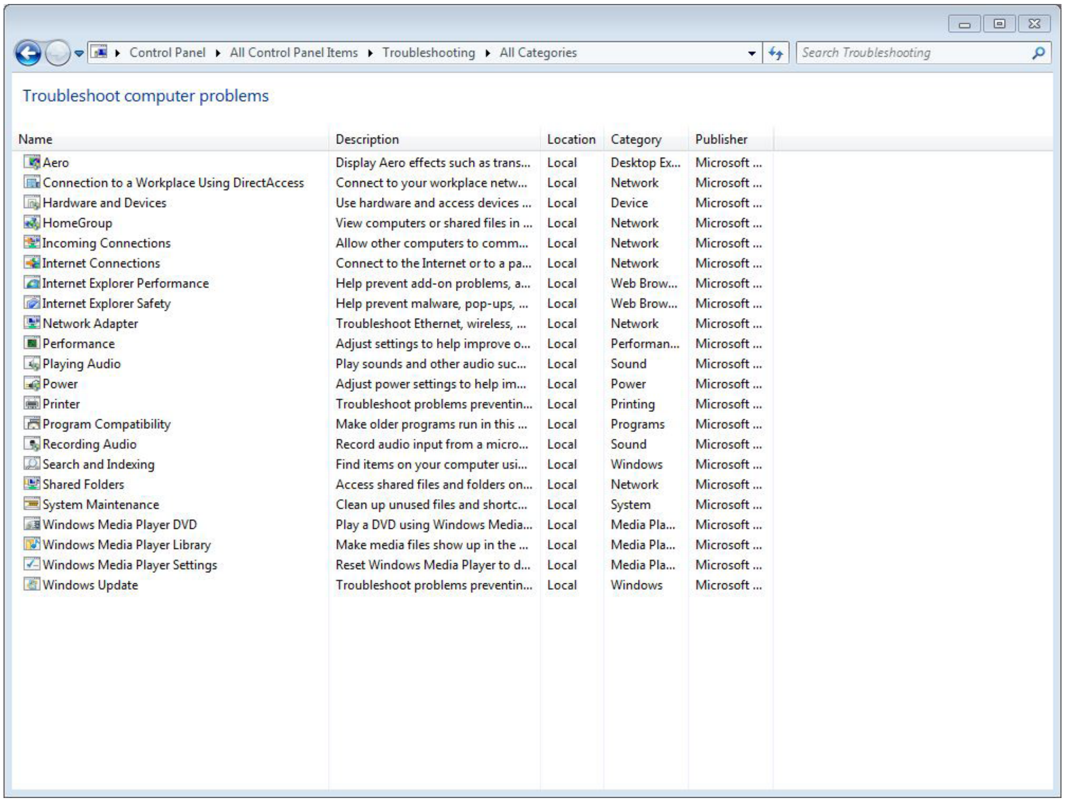
Figure 17: Action Center Settings

Windows 7 Troubleshooters

Troubleshooters are wizards that automatically diagnose and repair common problems. Windows 7 includes many built-in troubleshooters; however, many additional third-party troubleshooters can be accessed from the Windows Troubleshooting Platform. Windows 7 currently includes 22 troubleshooters accessed from the Control Panel.

The majority of troubleshooters built into Windows 7 are accessed through the Troubleshooting item in Control Panel. Administrators should be familiar with these Control Panel troubleshooters so you know which ones are appropriate for certain computer malfunctions.

To access Control Panel troubleshooters, click the flag icon on the taskbar; the Action Center appears. Then, click Troubleshooting to display Control Panel Troubleshooters.


Control Panel ▸ All Control Panel Items ▸ Troubleshooting ▸ All Categories
Search Troubleshooting

Troubleshoot computer problems

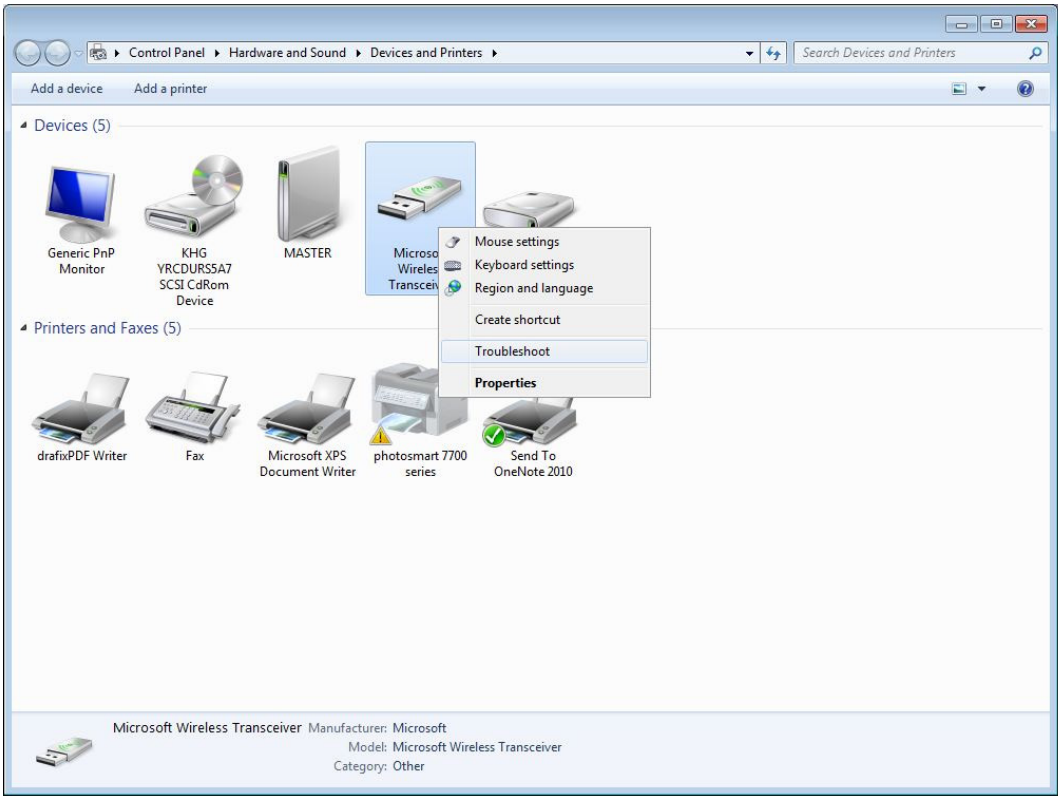
Name	Description	Location	Category	Publisher
Aero	Display Aero effects such as trans...	Local	Desktop Ex...	Microsoft ...
Connection to a Workplace Using DirectAccess	Connect to your workplace netw...	Local	Network	Microsoft ...
Hardware and Devices	Use hardware and access devices ...	Local	Device	Microsoft ...
HomeGroup	View computers or shared files in ...	Local	Network	Microsoft ...
Incoming Connections	Allow other computers to comm...	Local	Network	Microsoft ...
Internet Connections	Connect to the Internet or to a pa...	Local	Network	Microsoft ...
Internet Explorer Performance	Help prevent add-on problems, a...	Local	Web Brow...	Microsoft ...
Internet Explorer Safety	Help prevent malware, pop-ups, ...	Local	Web Brow...	Microsoft ...
Network Adapter	Troubleshoot Ethernet, wireless, ...	Local	Network	Microsoft ...
Performance	Adjust settings to help improve o...	Local	Performan...	Microsoft ...
Playing Audio	Play sounds and other audio suc...	Local	Sound	Microsoft ...
Power	Adjust power settings to help im...	Local	Power	Microsoft ...
Printer	Troubleshoot problems preventin...	Local	Printing	Microsoft ...
Program Compatibility	Make older programs run in this ...	Local	Programs	Microsoft ...
Recording Audio	Record audio input from a micro...	Local	Sound	Microsoft ...
Search and Indexing	Find items on your computer usi...	Local	Windows	Microsoft ...
Shared Folders	Access shared files and folders on...	Local	Network	Microsoft ...
System Maintenance	Clean up unused files and shortc...	Local	System	Microsoft ...
Windows Media Player DVD	Play a DVD using Windows Media...	Local	Media Pla...	Microsoft ...
Windows Media Player Library	Make media files show up in the ...	Local	Media Pla...	Microsoft ...
Windows Media Player Settings	Reset Windows Media Player to d...	Local	Media Pla...	Microsoft ...
Windows Update	Troubleshoot problems preventin...	Local	Windows	Microsoft ...

Figure 17: Troubleshooters

If you identify a troubleshooter to run, then select that link. To review a complete list of all available troubleshooters without categories, click View All on the left side of the window. Otherwise, choose the required troubleshooting category.

Devices and Printers Troubleshooter

This is a new feature in Windows 7 for hardware and printers. Select Devices and Printers from the Start menu. Once you have your list of devices, right-click on one and select "Troubleshoot" from the menu.



Microsoft Wireless Transceiver Manufacturer: Microsoft
Model: Microsoft Wireless Transceiver
Category: Other

Figure 18: Troubleshooting Devices

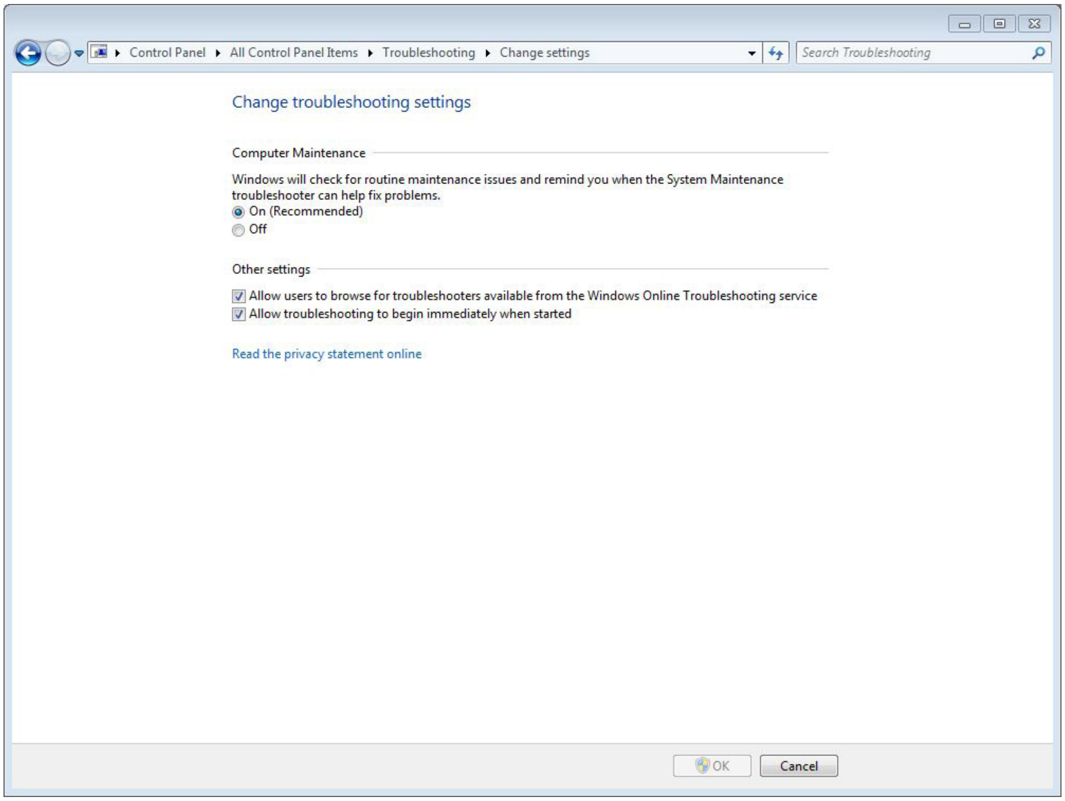
Hardware Troubleshooters

Troubleshooters identify errors. Troubleshooters primarily detect configuration errors; however, you can still use the troubleshooter to help determine if device issues exist with hardware.

If a troubleshooter detects a problem but can't determine the source, the hardware device could be faulty. You should then test the device with the manufacturer diagnostics.

Configuring Troubleshooter Settings

To open the Change Troubleshooting Settings page, click the Change Settings option on the main window of the Troubleshooting item in Control Panel.



Control Panel ▸ All Control Panel Items ▸ Troubleshooting ▸ Change settings
Search Troubleshooting

Change troubleshooting settings

Computer Maintenance

Windows will check for routine maintenance issues and remind you when the System Maintenance troubleshooter can help fix problems.

● On (Recommended)

○ Off

Other settings

☑ Allow users to browse for troubleshooters available from the Windows Online Troubleshooting service

☑ Allow troubleshooting to begin immediately when started

Read the privacy statement online

Figure 19: Troubleshooter Settings

Use the Change Troubleshooting Settings page to change settings such as:

- **Computer Maintenance –** by default, the routine checks are enabled. This setting is relevant for diagnosing hardware problems—particularly problems detected with the physical disk.
- **Allow Users to Browse For Troubleshooters Available from the Windows Online Troubleshooting Service –** this setting is enabled by default. If you have problems viewing available troubleshooters, then ensure this setting is active.
- **Allow Troubleshooting to Begin Immediately When Started –** this setting is enabled by default. It only affects the Troubleshooting option in Devices and Printers, controls whether a troubleshooter should skip the opening page of the wizard when selected.

Device Manager

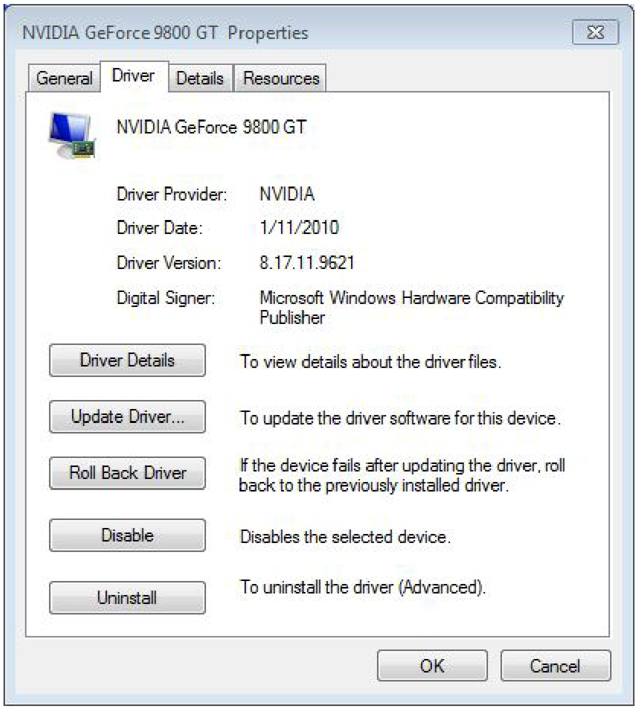
If a troubleshooter does not automatically fix a problem related to hardware, open Device Manager for more information. Device Manager is a basic tool that you can use to determine whether there are any malfunctioning devices connected to the system.

To view failed hardware in Device Manager, follow these steps:

1. Click Start, right-click Computer, and then click Manage.
2. Under System Tools, click Device Manager.
3. Device Manager displays all locally attached devices. Problem devices (including any devices with which Windows 7 has failed to communicate) are displayed with a warning sign. If no categories are expanded and no devices are visible, then Windows has not detected a problem with any device.

If Device Manager detects a problem with a device, right-click the device and open its Properties dialog box.

A common cause of hardware failure is a faulty driver. If the General tab of the Properties dialog box reports a problem with a device driver, click the Driver tab. From this tab, you can choose to update the driver or roll it back to the previously installed version.



NVIDIA GeForce 9800 GT

Driver Provider: NVIDIA

Driver Date: 1/11/2010

Driver Version: 8.17.11.9621

Digital Signer: Microsoft Windows Hardware Compatibility Publisher

Driver Details — To view details about the driver files.

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

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

Disable — Disables the selected device.

Uninstall — To uninstall the driver (Advanced).

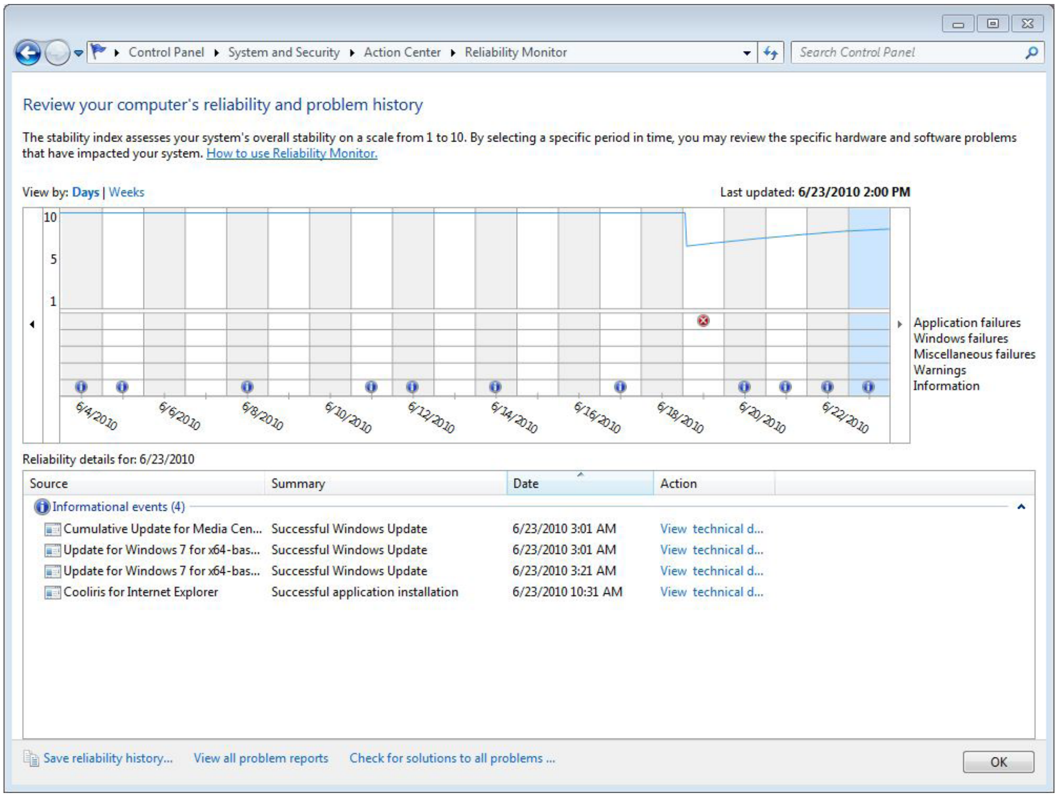
Figure 20: Device Properties

You should choose to roll back the driver if it was working before you last updated it. If the previously installed driver did not function, or if no previous driver was ever installed, you should update the driver. Note, however, that the suggested way to update a driver is to download and run the most recent driver installation program from the device manufacturer's Web site. You should use the Update Driver option only if no installation program is available for a functioning driver. If Device Manager indicates a problem with a device but can provide no resolution to the problem, you should investigate a hardware malfunction.

Reliability Monitor

Reliability Monitor tool measures the stability of a system over time. In Windows 7, you can access Reliability Monitor through the Action Center by expanding the Maintenance Area and then clicking View Reliability History, as shown below.

Reliability Monitor shows the computer's stability over a specific time-period (past 20 days or 20 weeks):



Review your computer's reliability and problem history

The stability index assesses your system's overall stability on a scale from 1 to 10. By selecting a specific period in time, you may review the specific hardware and software problems that have impacted your system. How to use Reliability Monitor.

Reliability details for: 6/23/2010

Source	Summary	Date	Action
Informational events (4)			
Cumulative Update for Media Cen...	Successful Windows Update	6/23/2010 3:01 AM	View technical d...
Update for Windows 7 for x64-bas...	Successful Windows Update	6/23/2010 3:01 AM	View technical d...
Update for Windows 7 for x64-bas...	Successful Windows Update	6/23/2010 3:21 AM	View technical d...
Cooliris for Internet Explorer	Successful application installation	6/23/2010 10:31 AM	View technical d...

Figure 21: Reliability Monitor

To assess a system's stability, Reliability Monitor tracks the following five categories of events:

- Information
- Warnings
- Miscellaneous failures
- Windows failures
- Application failures

Using Reliability Monitor to Diagnose Hardware Failures

Reliability Monitor assembles data about software failures that have occurred in the recent history of the system, for example, power failures. Because hardware failures lead to software failures, this information is useful even when faulty hardware is the root problem.

While troubleshooting a failure, hardware or software, check Reliability Monitor to determine if Windows has recorded any relevant information about the problem over time, especially critical events.

Event Viewer

As mentioned previously, Event Viewer stores events that are written to event logs in Windows7 and other applications. Event viewer can also be used to troubleshoot hardware issues. On most computers, Event Viewer contains thousands of events, most of which are informational and can be safely ignored. However, when troubleshooting, you should examine the Event Log to find events that might help to uncover the source of the problem you are trying to diagnose.

Remember, however, that not all problems generate an event. For this reason, it is possible that you will not see any events related to the issue you are troubleshooting.

To open Event Viewer and view hardware-related events, follow these steps:

1. Click Start\right-click Computer/click Manage.
2. Expand Event Viewer under System Tools.
3. Expand Windows Logs under Event Viewer.
4. Click System.
5. In the Actions pane, click Filter Current Log.
6. In the Filter Current Log dialog box, select the Critical and Error check boxes, and click OK.

After performing these steps, Event Viewer lists only critical events and errors. Examine this list of events, looking for events related to hardware components in particular.

Startup Repair

A physically malfunctioning disk, motherboard, or RAM module can prevent a system from starting, but so can a faulty disk configuration. If you need to troubleshoot a system that does not start, you first need to rule out software configuration or data corruption errors on the disks as the cause.

Startup Repair automatically detects and fixes many hard disk errors that prevent Windows from starting. Startup Repair begins by analyzing the following:

- Boot sectors
- Boot manager
- Disk configuration
- Disk integrity
- Boot configuration data (BCD)
- Registry file integrity
- System file integrity
- Boot logs
- Event logs

Then, Startup Repair attempts to solve any problems it has found.

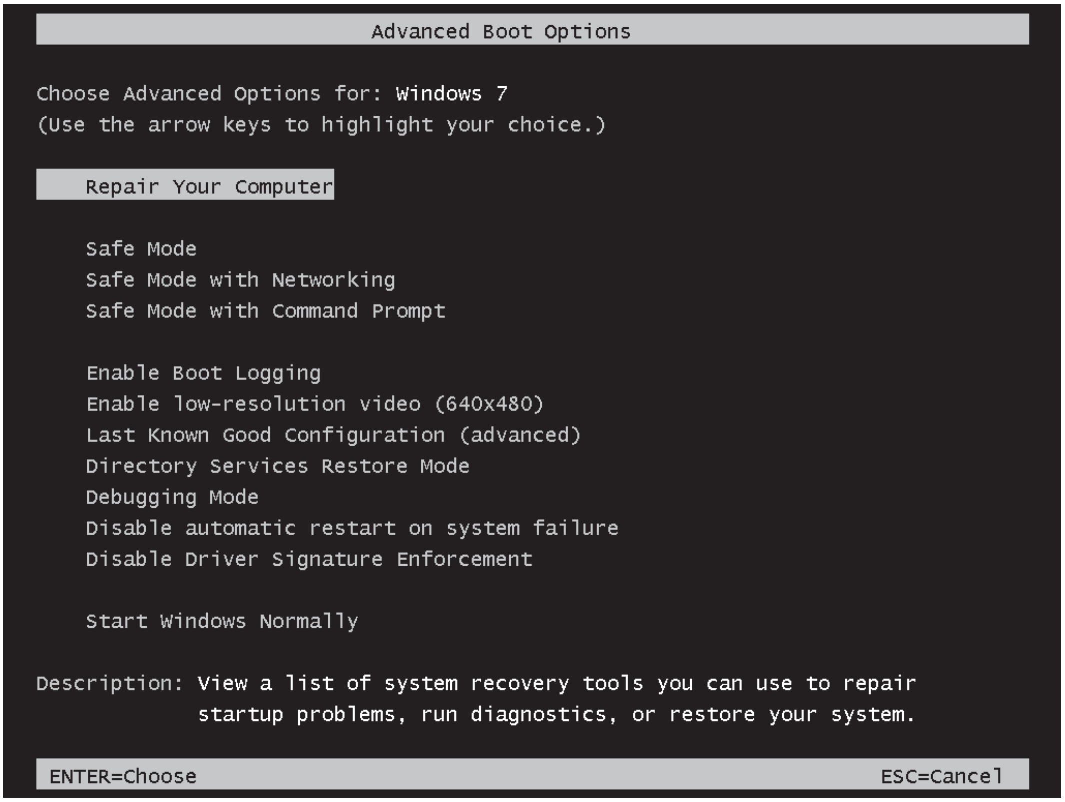
This repair process can involve repairing configuration files, solving simple disk problems, replacing missing system files, or running System Restore to return the computer to an earlier state. Because Startup Repair performs these tasks automatically, you can solve startup problems much faster by using this tool than you would otherwise if you had to perform this analysis and repair manually.

Startup Repair helps you diagnose hardware failures because it repairs common software configuration errors found on boot disks (typically hard disks). If Startup Repair fails to fix a Windows startup problem, you can normally remove disk configuration from the list of potential sources of the error you want to resolve. You can then turn your attention to other possible causes, such as a third-party disk partitioning utilities, physical disk problems, physical drive problems, an incorrectly configured basic input/output system (BIOS), faulty memory, or a faulty motherboard.

Startup Repair Tool

You access Startup Repair through the Windows Recovery Environment and its associated System Recovery Options, which are installed automatically on the boot disk by the Windows 7 Setup program. The Windows Recovery Environment is a light operating system that you can use to fix Windows problems offline.

To open the Windows Recovery Environment, press F8 as your computer starts to open the Advanced Boot Options menu. Then, choose the Repair Your Computer option, as shown below. If the startup problem that you are diagnosing prevents you from accessing the Advanced Boot Options menu, you can access the Windows Recovery Environment and System Recovery Options by booting from the Windows 7 DVD. With this latter method, the Install Windows wizard opens. Then, select your language, click **Next**, and choose the **Repair Your Computer** option on the second page of the **Install Windows** wizard, as shown in below.



```
                         Advanced Boot Options

Choose Advanced Options for: Windows 7
(Use the arrow keys to highlight your choice.)

    Repair Your Computer

    Safe Mode
    Safe Mode with Networking
    Safe Mode with Command Prompt

    Enable Boot Logging
    Enable low-resolution video (640x480)
    Last Known Good Configuration (advanced)
    Directory Services Restore Mode
    Debugging Mode
    Disable automatic restart on system failure
    Disable Driver Signature Enforcement

    Start Windows Normally

Description: View a list of system recovery tools you can use to repair
             startup problems, run diagnostics, or restore your system.

 ENTER=Choose                                                ESC=Cancel
```

Figure 22: Advanced Boot Options

Either method of starting the Windows Recovery Environment opens the first page of the System Recovery Options wizard. The **Choose a Recovery Tool** page is the last page of the System Recovery Options wizard. To launch the Startup Repair tool, choose that option on the page.
When Startup Repair tool is running, you can perform the following tests:

- Check for updates
- System disk test
- Disk failure diagnosis
- Disk metadata test
- Target OS test
- Volume content check
- Boot manager diagnosis
- System boot log diagnosis
- Event log diagnosis
- Internal state check
- Boot status test

After it runs the tests and repairs the disk, Startup Repair displays a diagnosis of the startup error.
If Startup Repair finds no errors, you can troubleshoot other system components, such as the physical memory or the physical disk.

Memory Diagnostics

Damaged RAM is a common cause of system failures. Memory problems can prevent Windows from starting or can cause unpredictable stop errors when Windows is running. Memory-related problems typically cause intermittent failures. This can be difficult to diagnose. If you suspect memory errors might be the cause of a computer problem, Use Windows 7 Memory Diagnostic to test the system's memory.
You must run Windows Memory Diagnostic offline, but you can start the tool in numerous ways Windows 7, such as:

- Windows interface, you can schedule Memory Diagnostic to run the next time the system starts.
- Windows Boot Manager.
- System Recovery Options.

Running Chkdsk

The Chkdsk tool automatically finds and repairs disk volume problems related to:

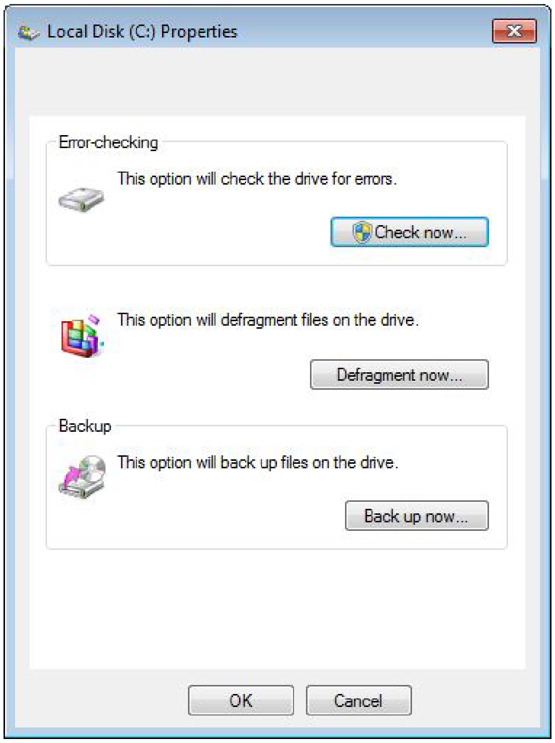
- Bad sectors
- Lost clusters
- Cross-linked files
- Directory errors

You can run Chkdsk either in Windows or offline; however, if you want to specifically scan the system volume, you must run the tool outside of Windows. In this case, as with Windows Memory Diagnostic, you can schedule the tool to run the next time Windows starts.

Troubleshooting with Chkdsk

Disk errors are a common cause of problems. Bad sectors on a hard disk, for example, can result in stop errors, system freezes, or other errors. When you are troubleshooting problems that do not appear to be the result of a recent system change, you use Chkdsk to scan your disks for errors as relating to hardware failures.

Chkdsk refers to the spelling of the command-line version of the tool, but you can also start Chkdsk through the GUI. To do this: open the properties of the volume you want to check and click the Tools tab. Then, click Check Now, as shown below.



Local Disk (C:) Properties

Error-checking

This option will check the drive for errors.

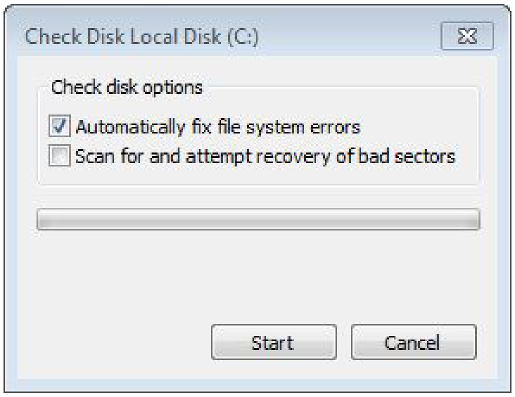
This option will defragment files on the drive.

Backup

This option will back up files on the drive.

Figure 23: Starting Disk Checking

This step opens the Check Disk dialog box. In this dialog box, you choose whether to fix both file system errors and bad sectors, or just file system errors. Once you have made the selection, click Start.



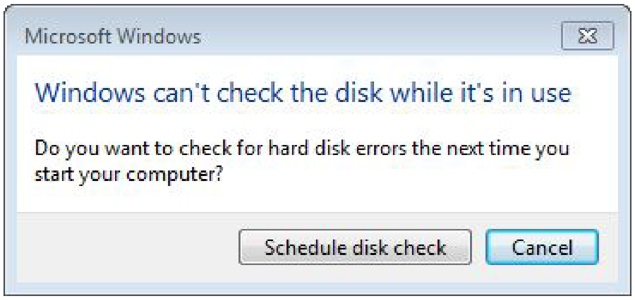
Check Disk Local Disk (C:)

Check disk options

☑ Automatically fix file system errors
☐ Scan for and attempt recovery of bad sectors

Figure 24: Running Check Disk

If you have selected the system volume to check, you see the message shown below. This message indicates that the hard disk will be checked for errors the next time the computer starts.


Microsoft Windows

Windows can't check the disk while it's in use

Do you want to check for hard disk errors the next time you start your computer?

Figure 25: Disk Check Error

Additional chkdsk Scenarios

Use the chkdsk d: /f command to automatically attempt to repair discovered errors on a hard disk volume. The **/f** switch indicates that errors on the disk should be fixed. Also remember, when you want to check the system disk, you need to run Chkdsk offline.

Disk Defragmenter

Disk fragmentation refers to the gradual dispersion of data on a disk over time. Because disk fragmentation slows down computers, disks need to be defragmented regularly. Disk Defragmenter rearranges fragmented data so disks and drives can work more efficiently. Disk Defragmenter runs automatically on a schedule in Windows 7 (every Wednesday at 1 a.m.), but you can also analyze and defragment your disks and drives manually.

To run Disk Defragmenter manually, follow these steps:

1. Click Start. Type Disk Defragmenter, which appears highlighted in the Programs list.
2. Select the disk you want to defragment in Current Status.
3. Click Analyze Disk to see if the disk requires defragmentation.
4. After Windows finishes analyzing the disk, you can check the Last Run column for the percentage of fragmentation. If fragmentation is above 10%, you should defragment the disk.
5. If required, click Defragment Disk. Disk Defragmenter can take from several minutes to a few hours to complete, depending on the size and degree of fragmentation of the hard disk.

Troubleshooting Hard Disks

Hard disk drives are starting to be replaced by alternative forms of non-volatile storage, such as solid-state drives. The following section provides a set of basic strategies for troubleshooting hard disk problems.

You hear a loud whirring, screeching, or clicking.

1. Back up your data. The hard drive could be about to fail.
2. Replace the drive.

The operating system fails to start, and you receive an error message such as:

- Couldn't find loader.
- A disk-read error occurred.
- Invalid partition table.
- Hard disk error.

Try the following troubleshooting steps:

1. Confirm that the BIOS Setup program is configured to boot from the hard drive.
2. Confirm that the hard drive contains an operating system.
3. Run the Startup Repair tool.
4. Confirm power connectors are attached to the hard drive.
5. Make sure any jumpers on the hard drives are configured properly (according to manufacturer specifications).
6. Use the System Image Recovery option to recover the disk if possible.
7. Replace the hard drive.

The operating system loads, but performance decreases over time.

Run Disk Defragmenter.

The operating system loads, but there is evidence of data corruption or the system sometimes freezes and remains unresponsive.

1. Run Chkdsk.
2. Test the physical functionality of the hard disk drive; run software diagnostics from the hard disk drive manufacturer.

Domain 4: Supporting Mobile Users

Troubleshooting Wireless Networks

Users can encounter problems while accessing wireless networks. For example:

- The wrong network credentials
- Malfunctioning hardware
- Weak signals

Wireless Networking Advantages and Disadvantages

Advantages

Wireless networks are much more efficient than ordinary network access. A wireless access point can service a wide metropolitan area, and provide network access to many more remote systems. Wireless networks provide corporate advantages such as:

- Secured access point
- Ethernet cables are not required to connect to the network
- Cost savings from wireless network services

Disadvantages

The main disadvantage is that wireless networks are much more vulnerable to attacks than wired networks; hackers don't require access to system's physical location to connect to a network. Windows 7 supports wireless network security technologies that provide protection to meet most security requirements.

Wireless Networks Connection

You can connect wireless networks in the following ways:

- Scripts
- Group Policy
- Manually

Using Scripts

- You can use scripts and profiles to simplify the process of connecting to private wireless networks for your users. Ideally, you should use scripts and profiles to keep users from ever needing to type wireless security keys.
- You can also use Netsh to allow or block access to wireless networks based on their SSIDs. You can also configure wireless settings using commands in the **netsh wlan** context of the Netsh command-line tool. You can create scripts that connect to different wireless networks.

  Run the following command to list available wireless networks:

  ```
  netsh wlan show networks
  Interface Name: Wireless Network Connection
  There are 2 networks currently visible
  SSID 1 : Companyx1
  Network Type        : Infrastructure
  Authentication                     : Open
  Encryption                  :None
  SSID 1 : Companyx2
  Network Type        : Infrastructure
  Authentication                    : Open
  Encryption                 : WEP
  ```

- You must save a profile containing the SSID and security information before you can connect to a wireless network using Netsh. Profiles are required to connect to a network.
- To save a profile, run the following command after manually connecting to a network: **netsh wlan** export profile name=*"<SSID>"*
- Load a profile from a file before connecting to a new wireless network. For example: **netsh wlan add profile filename="C:\profiles\Companyx1.xml"**
- To connect quickly to a wireless network, use the **netsh wlan connect** command and specify a wireless profile.

  ```
  netsh wlan set autoconfig enabled=...
  ```

- To block all ad hoc networks, use the Deny all permission , for example :

  ```
  netsh wlan add filter permission=denyall networktype=adhoc
  ```

- To prevent Windows 7 from automatically connecting to wireless networks, run the following command:

  ```
  netsh wlan set autoconfig enabled=no interface="Wireless Network
  Connection" information
  ```

Manual Connection

Use the following procedure to connect to a wireless network that is in range:

1. Click the networking notification icon in the system tray, and then click the name of the network you want to connect to.. If you have never connected to the network previously and you want to connect to it automatically, select the Connect Automatically check box, and then click Connect.
2. The WLAN AutoConfig service must be started for wireless networks to be available. This service is set by default to start automatically.

   If the Type the Network Security Key dialog box appears, then type the network security key, and then click OK.
3. To disconnect from all wireless networks, click the networking notification icon in the system tray, click the name of the current network, and then click Disconnect.

Group Policy Settings

Use Group Policy settings to configure client computers in AD DS environments. Ideally, you should have Windows Server 2003 with SP1 or later installed on your domain controllers because Microsoft extended support for wireless Group Policy settings when they released Service Pack 1.

You must extend the AD DS schema through the command line or a graphical interface. One way of completing this task is to use the 802.11Schema.ldf file from *http://www.microsoft.com/technet/network/wifi/vista_ad_ext.mspx*. Before you can configure wireless networks for client computers running Windows XP, Windows Vista, or Windows 7. To extend the schema, follow these steps:

1. Copy the 802.11Schema.ldf file to a folder on a domain controller.
2. Log on to the domain controller with Domain Admin privileges and open a command prompt.
3. Select the folder containing the 802.11Schema.ldf file, and run the following command (where Dist_Name_of_AD_Domain is the distinguished name of the AD DS domain, such as "DC=contoso,DC=com" for the contoso.com AD DS domain: **ldifde -i -v -k -f 802.11Schema.ldf -c DC=X Dist_Name_of_AD_Domain**
4. Restart the domain controller.

If you have domain controllers running Windows Server 2008 or later or you have an earlier version of Windows, and you have extended the schema, you can configure a wireless network policy from a domain controller by following these steps:

1. Open the AD DS Group Policy Object (GPO) in the Group Policy Object Editor.
2. Expand Computer Configuration, Policies, Windows Settings, Security Settings, and then click Wireless Network (IEEE 802.11) Policies.
3. Right-click Wireless Network (IEEE 802.11) Policies, and then click Create a New Wireless Network Policy for Windows Vista and Later Releases (if the server is running Windows Server 2008 R2) or Create a New Windows Vista Policy (if the server is running an earlier version of Windows).
4. The New Wireless Network Policy Properties dialog box appears.
5. To add an infrastructure network, click Add, and then click Infrastructure to open the Connection tab of the New Profile Properties dialog box. In the Network Names list, type a valid internal SSID in the Network Names box, and then click Add. Repeat this to configure multiple SSIDs for a single profile. If the network is hidden, select the Connect Even If the Network Is Not Broadcasting check box.
6. In the New Profile Properties dialog box, click the Security tab. Use this tab to configure the wireless network authentication and encryption settings. Click OK.

These settings configure client computers to connect automatically to internal wireless networks and prevent them from connecting to other wireless networks.

Wireless Network Profile

To connect to a wireless network if it is in range and broadcasting a Service Set Identifier (SSID), click the networking notification icon. In the system tray, choose the network and follow the prompts.

Use the following procedure to reconfigure a wireless network so that Windows 7 can connect to it automatically when the network is in range:

1. Click the networking notification icon in the system tray, then click Open Network and Sharing Center.
2. In the Network And Sharing Center, click Manage Wireless Networks\Add.
3. The Manually Connect to a Wireless Network wizard appears. Click Manually Create A Network Profile.
4. On the Enter Information for the Wireless Network You Want to Add page, type required information\Next.
5. On the Successfully Added page, click Close.

Changing Priorities

When multiple networks are available, you should prioritize connection to the correct network. Use the following procedure to set the priority of wireless networks:

1. Click the networking notification icon in the system tray, and then click Open Network and Sharing Center.
2. Click Manage Wireless Networks.
3. In the Manage Wireless Networks window, click a wireless network profile, and then click Move Up or Move Down. When multiple networks are available, Windows 7 will connect to the network with the highest priority.

Reconfiguring

When first connecting to the network, Windows 7 stores settings for future connections; however, you may not be able to connect in the future if the configuration of the wireless access point changes.

Use the following procedure to change the configuration of a wireless network after the original configuration:

1. Click the networking notification icon in the system tray, and then click Open Network and Sharing Center.
2. In the Network and Sharing Center, click Manage Wireless Networks.
3. Right-click the network you want to reconfigure, and then click Properties. The Wireless Network Properties dialog box appears.
4. Use the Connection tab to specify whether Windows 7 will connect automatically to the network when it is in range (if no other wireless connection already exists).
5. As shown in above, you can use the Security tab to specify the security and encryption types. Depending on the security type, Windows 7 shows other options in the dialog box.
6. Click OK.

Try to reconnect to the network and verify settings after reconfiguring the network connection. Or, you can right-click a wireless network from the Manage Wireless Networks tool and click Remove Network. After removing the network, you can reconnect to the network as though it was a new network.

Profile Types

If mobile computers in an organization are shared between multiple users, you can configure wireless networks to use per-user profiles. With per-user profiles, one user can connect to a wireless network without other users being able to use the same wireless network connection.

Use the following procedure to change a wireless profile to per-user instead of all-user:

1. Click the networking notification icon in the system tray, and click Open Network and Sharing Center. The Network and Sharing Center appears.
2. In the left pane, click Manage Wireless Networks.
3. Click Profile Types.
4. In the Wireless Network Profile Types dialog box, click Use All-User and Per-User Profiles.
5. Click Save.

Security

Wired networks are often unencrypted, too (at least at Layer 2), but this normally does not present a threat because an hacker would need to connect an Ethernet cable on site to the network to gain access, and most organizations prohibit unauthorized personnel from coming onsite.

Many wireless networks are unencrypted and unauthenticated, with no security features in place. With a wireless network, a hacker can connect to the network from outside the physical walls of the organization. This can present a significant security risk.

Configuring WPA-EAP Security

The static keys used by WEP and WPA-PSK aren't manageable in enterprise environments. If an employee left, you'd need to change the key on the wireless access point to prevent the employee from connecting to the network in the future. Then, you would need to update every wireless client computer in your organization. EAP in WPA-EAP stands for Extensible Authentication Protocol. Because it is extensible, you can authenticate using several different methods:

- Certificates stored on smart cards
- Certificates stored on the user's computers
- PEAP-MS-CHAPv2 to enable users to connect to a wireless network using their domain credentials

Windows Server 2008 includes the Network Policy Server (NPS), which can actually be a RADIUS client to an organization, or it can act like a RADIUS server that is integrated tightly with AD DS. When configuring NPS, you can specify a domain security group that will be granted access to the wireless network. For this reason, you should create a group specifically for users with the right to access the wireless network.

By default, when you connect to a new WPA-EAP or WPA2-EAP network, Windows 7 is configured to use the Secured Password (EAP-MSCHAP v2) authentication method to allow users to authenticate with their domain credentials. If users should authenticate using a certificate (whether stored on the local computer or a smart card), create a wireless network profile for the network using the default settings, and then follow these steps to configure the wireless network security:

1. Click the networking notification icon in the system tray, and then click **Open Network and Sharing Center**.
2. In the **Network and Sharing Center**, click **Manage Wireless Networks**.
3. Right-click the network and then click **Properties**. Then, click the **Security** tab.
4. Click the **Choose a Network Authentication Method** list, and then click **Microsoft: Smart Card or Other Certificate**.

Notice that the **Remember My Credentials for This Connection Each Time I'm Logged On** check box is selected by default. If you want the user to insert her smart card every time she connects to the network, clear this check box.

1. Click **Settings**. If the certificate is stored on the local computer, click **Use a Certificate on This Computer in the When Connecting** group, as shown in. If you are using a smart card, click **Use My Smart Card**.
2. Click OK twice. The next time the user connects using the profile, Windows 7 automatically attempts to find a suitable certificate. If it cannot find one, or if the user needs to insert a smart card, Windows prompts the user to select a certificate.

Encryption

- Both WPA-Enterprise and WPA2-Enterprise require RADIUS servers.
- WPA2 will encrypt the wireless communication to prevent eavesdropping.
- All EAP-TLS implementation require both an authentication server certificate and a supplicant (client) certificate.
- The Advanced Encryption Standard (AES) encryption algorithm is used with WPA2-Enterprise.
- The main difference between the Personal and Enterprise editions of WPA and WPA2: Personal uses pre-shared keys and Enterprise uses EAP with an authentication server. The Enterprise edition provides for central management of authentication credentials and processes with a RADIUS server.

Encryption Keys

- When implementing WPA2 with AES encryption, the minimum key length required by the 802.11i amendment is 128 bits.
- EAPHost is the name for the new EAP architecture in Windows Vista and Windows 7 that provides several improvements over the 802.1X supplicant in Windows XP and earlier Windows versions. EAPHost implement compliance with newer RFCs and a modular supplicant architecture so that new supplicants can easily be added.

The wired equivalent privacy (WEP) protocol should not be considered secure for any network implementation.

- The following are valid management options for wireless devices on a Windows 7 Enterprise machine:
    - Wireless Profiles. You can create and export and import wireless profiles on Windows 7 machines.
    - Wireless Network Policies. The Wireless Network Policies node of the Windows Settings in Group Policies can be used to manage wireless network settings.

Implement a wireless network between two Windows 7 laptops where no access point is used is considered an Ad hoc network. An ad hoc network, also known as an independent basic service set (IBSS), consists of only individual client nodes and no APs.

Use the netsh wlan command script context to configure wireless LAN profiles when you want to configure more than one hundred clients with wireless profiles running Windows 7 Enterprise Edition. All clients run.

Event Viewer

When users connect to the network, Windows 7 records technical details. Use the following procedure to view wireless networks users have connected to:

1. Click **Start**. Right-click **Computer**, and then click **Manage**.
2. Under **Computer Management**, navigate to: **System Tools** → **Event Viewer** → **Applications and Services Logs** → **Microsoft** → **Windows** → **WLAN-AutoConfig**. Then, select **Operational**.
3. In the middle pane, select an event log entry. This event log shows the details of attempted and successful connections to a wireless network.

Successful and unsuccessful connections are recorded by Windows 7 and added to the list of events.

Wireless Network Problems

- You can use the same troubleshooting techniques used while connected to a wired network while logged on to a wireless network.
- Wireless networks require however different troubleshooting techniques during the connection process. Some of the most common problems include the following:

Network Adapter Can’t View Wireless Networks

The network adapter could be turned off at the hardware level if the adapter cannot view any wireless networks even if wireless networks are available. Most mobile computers include a dedicated hardware switch or a key combination that turns the wireless radio on or off. Windows Network Diagnostics correctly detects this condition.

Device Manager can also be used to verify if the wireless network adapter was detected and has a valid driver. To start Device Manager, click Start, type **devmgmt.msc**, and press Enter. Then, expand Network Adapters. If the wireless radio is off, Windows still detects the network adapter, but it may not function.

Weak Wireless Signal

The farther you move from the wireless access point, the weaker the signal. The weaker the signal, the slower the network performance. You can, however, perform some tasks to improve the range of a wireless signal:

- Increase the power at the client computer. Increasing the transmitter power can also increase battery usage.
- Adjust the antenna on the wireless access point.
- Use a high-gain antenna, also known as a directional antenna if possible. A low-gain antenna (also known as an omnidirectional antenna) broadcasts in all directions relatively equally. High-gain antennas are very directional.
- If attempting to connect from outdoors, remove screens from windows. Screens do not block a wireless signal, but they introduce a significant amount of noise. Increase the power at the transmitter if possible.

Click the network icon in the status bar or by opening the Network and Sharing Center to view the wireless signal strength.

Reconnecting to a Wireless Network

If you cannot connect to a wireless network that you have connected to previously, it is normally because security settings on the network have changed. You can access Reconfiguring a Wireless Network to rectify this. Or, you could remove the wireless network profile and connect to the network as if it were a new network.

Poor Performance

Several factors can cause poor network performance:

- A weak wireless signal.
- Interference. 802.11b, 802.11g, and 802.11n use the 2.4 gigahertz (GHz) radio frequency, whereas 802.11a uses the 5.8-GHz frequency. Cordless phones and other wireless devices on the same frequency can introduce performance problems.

Overlapping Access Points

For best results, use channels 1, 6, and 11 when wireless access points overlap. Wireless access points can broadcast on 1 of 11 channels. If two wireless access points broadcast on the same channel or on a channel within five channels of another wireless access point, the performance of both can be reduced.

Multiple Wireless Frequencies

If possible, upgrade all wireless clients to the fastest wireless network standard supported by your wireless access points. Then, configure your wireless access point to use “802.11g only” or “802.11n only” mode.

Network Traffic

If one client is downloading a large file, that can affect the performance of all clients. All wireless clients compete for a limited amount of bandwidth.

Unexplained Problems

For best results, upgrade all wireless access point firmware and network adapter drivers to the latest versions. Then, work with the hardware vendor's technical support to continue troubleshooting the problem. Wireless network protocols have changed in a short time. It's common that wireless network hardware from different vendors have difficulty interoperating. If you're using a wireless network adapter that fully implements 802.11n and you're attempting to connect to a wireless access point based on pre-802.11n standards, you might not be able to connect, you might experience intermittent failures, or performance might be reduced.

Signal Strength Scenarios

While supporting Windows 7 laptops that connect to your network using a wireless LAN, several users are complaining that the signal strength is too weak in their work areas. You should increase the output power of the access points. If you increase the output power at the access points, the signal strength should increase in the coverage areas. Also, consider installing more access points closer to the weak coverage area. You can install additional APs to increase the coverage and signal strength in the problem areas.

To implement a wireless link for a Windows 7 user, running Windows 7 Enterprise on a laptop computer, and requiring a data rate of 70 Mbps or greater. Use the 802.11n amendment to provide for data rates up to 600 Mbps. This is the only standard amendment that provides data rates above 54 Mbps at the time of Windows 7's release.

To configure a wireless LAN to support Windows 7 laptop users after noticing that the 2.4 GHz 802.11 network channels were all in use. Choose one of the technologies to resolve the problem: 802.11n. 802.11n may operate in either the 2.4 GHz or the 5 GHz spectrum space. Or, 802.11a. 802.11a operates in the 5 GHz spectrum space.

Say you have a wireless LAN with a single access point. Twenty Windows 7 laptops use this wireless LAN. Users are complaining that the network is too slow. The access point is an 802.11g access point. Without implementing 802.11n, you can install an additional 802.11g access point to resolve the issue. Twenty users sharing the 54 Mbps data rate (which results in between 25-30 Mbps throughput) may simply be too much. By installing an additional AP, you can improve the performance by spreading users across the two APs.

In a Windows 7 Enterprise environment, users often connect to public hotspots to check their email messages while traveling. If wireless access is not displayed in the view available networks system tray tool; however, a coworker located in the same area can see three different networks. The most common cause is that the wireless adapter is turned off on the laptop. It is not uncommon for laptops to allow users to turn off the wireless adapter to save battery power and for use on airplanes. Ensure that the adapter is turned on.

If you are having a connection problem on a Windows 7 laptop where the laptop connects to an 802.11n wireless network and the laptop contains an 802.11a wireless adapter, and the users is experiencing intermittent connection losses while moving around in their work area, but have connection while the laptop is stationary at their workstation, the most common cause of the problem is that the signal strength is weaker in some areas causing connection loss. You should evaluate the signal strength in the area and take action to improve it, if necessary.

Say you are implementing a new wireless network for the new Windows 7 laptops being installed in your organization. Before you begin installing the wireless infrastructure equipment, you should perform a site survey to validate appropriate coverage and usability of the wireless network in your facility. A site survey will verify coverage and available wireless channels.

Remote Access

Currently, most users remotely access networks through virtual private network (VPN). Windows 7 has now introduced an improved means of remote access, DirectAccess. There are a variety of VPN types compatible with Windows 7 and Windows Server 2008 R2. A VPN is a private, encrypted network connection that crosses the Internet.

VPN either connects two office sites or enables remote computers to access a single network. In a remote access VPN, the client running Windows 7 must be configured to negotiate a connection to the VPN server.

Therefore, exam 70-685 principally requires administrator's to understand client-side VPN configuration. You should understand the following VPN and DirectAccess related subjects:

- Authorization
- Authentication
- Infrastructure Configuration

DirectAccess

DirectAccess is a new feature of Windows 7 and Windows Server 2008 R2 that automatically connects a remote user to a private network from any location on the Internet. DirectAccess was developed to eventually replace VPNs, which require users to initiate a VPN connection after connecting to the Internet.

Key facts about DirectAccess:

- DirectAccess is supported on Windows 7 Enterprise, Windows 7 Ultimate, and Windows Server 2008 R2.
- Automatically establishes bidirectional connectivity between a remote user's computer and their intranet.
- The remote user is not required to manually initiate connection to the intranet.
- Administrators can control access and other remote computers through the DirectAccess connection.

DirectAccess Benefits

DirectAccess overcomes issues with VPNs and benefits remote connection in the following ways:

- It fully integrates with Server and Domain Isolation solutions and the NAP infrastructure. This helps ensure compliance with security, access, and health policies for both local and remote computers.
- It provides the flexibility to control access to internal resources for remote users and their computers. For example, you can configure DirectAccess to provide user access only to selected resources.
- The remote user can access the corporate intranet and their local workstation. Also, since the user's computer can be accessed from the intranet, administrators can use tools such as Group Policy to manage the remote computer just as though they were directly connected to the internal network.
- The connection to the corporate network is completely transparent to the user,. As long as there is no interruption to the Internet connection, the interface is the same as if connected directly to the corporate network.

- The connection is always on, even before the user logs on to his or her computer unlike with a VPN.
- It includes the following security features:
    - It is built on a foundation of standards-based technologies: IPSec and IPv6.
    - It uses IPSec to authenticate both the computer and user. If you want, you can require a smart card for user authentication.
    - It uses IPSec to provide encryption for communications across the Internet.

DirectAccess and IPv6 Transition

Clients using DirectAccess must have globally routable IPv6 addresses. If clients are using DirectAccess with IPv6 addresses, they can also access resources through the internet with IPv4.

If a client has not yet deployed IPv6, they can start deploying it with such technology regarding protocols, routers, and devices as discussed in the following sections.

- **ISATAP** – Intra-site Automatic Tunnel Addressing Protocol (ISATAP) is a tunneling protocol that allows an IPv6 network to communicate with an IPv4 network through an ISATAP router, ISATAP routers allow IPv4-only and IPv6-only hosts to communicate with each other. ISATAP allows IPv4 and IPv6 hosts to communicate by performing a type of address translation between IPv4 and IPv6. In this process, all ISATAP clients receive an address for an ISATAP interface. This address is composed of an IPv4 address encapsulated inside an IPv6 address. ISATAP is intended for use within a private network.
- **6to4** – 6to4 is a protocol that tunnels IPv6 traffic over IPv4 traffic through 6to4 routers. 6to4 clients have their router's IPv4 address embedded in their IPv6 address and do not require an IPv4 address. Whereas ISATAP is intended primarily for intranets, 6to4 is intended to be used on the Internet. You can use 6to4 to connect to IPv6 portions of the Internet through a 6to4 relay even if your intranet or your ISP supports only IPv4.
- **Teredo** – Teredo is a tunneling protocol that allows clients located behind an IPv4 NAT device to use IPv6 over the Internet. Teredo is used only when no other IPv6 transition technology (such as 6to4) is available. Teredo relies on an infrastructure that includes Teredo clients, servers, relays, and host-specific relays.
- **IP-HTTPS** – IP-HTTPS is a new protocol in Windows 7 and Windows Server 2008 R2. It facilitates hosts located behind a Web proxy server or firewall to connect by tunneling IPv6 packets inside an IPv4-based Hypertext Transfer Protocol Secure (HTTPS) session. HTTPS is used instead of HTTP so that Web proxy servers do not attempt to examine the data stream and terminate the connection. IP-HTTPS is used as the fallback technology for DirectAccess clients when neither 6to4 nor Teredo is available.
- **IPv6/IPv4 NAT –** some NAT routers are able to provide connectivity between global IPv6 addresses and private IPv4 addresses. To perform this function, these devices typically conform to the Network Address Translation/Protocol Translation (NAT-PT) standard or the Network Address Port Translation + Protocol Translation (NAPT-PT) standard, as defined in RFC 2766. Although these two technologies are still available on some networks, they have been deprecated by the Internet Engineering Task Force (IETF) because of technical problems. NAT64 is the name of another mechanism to perform this same function in the future.
  You can configure IPv6 client settings in Local Computer Policy or Group Policy (Computer Configuration → Policies → Administrative Templates → Network → TCPIPSettings → IPv6 Transition Technologies).

- **IPv6 Support** – while implementing DirectAccess for Windows 7 Enterprise clients using Teredo for IPv6 tunneling, use the UDP port 3544 for Teredo traffic for IPv4 traffic going to the Windows Server 2008 R2 server.

DirectAccess Infrastructure

Direct Access features include general network infrastructure requirements such as:

- PKI (including a certification authority and CRL distribution points)
- Domain controllers
- IPv6 transition technologies
- DNS servers

A DirectAccess infrastructure also has the elements that form the core of the DirectAccess solution, such as clients and servers.

DirectAccess Server

At least one domain-joined server must be running Windows Server 2008 R2 so it can act as the DirectAccess server. This server typically resides on your perimeter network and acts as both a relay for IPv6 traffic and an IPSec gateway. The server can accept connections from DirectAccess clients and (like a VPN server) facilitate communication with intranet resources. The DirectAccess server needs to be configured with two physical network adapters and at least two consecutive, publicly-addressable IPv4 addresses that can be externally resolved through the Internet DNS.

To create a DirectAccess server, use Server Manager to add the DirectAccess Management Console feature in Windows Server 2008 R2. Then use the DirectAccess Setup Wizard in this console to configure the server.

DirectAccess Client

Client computers must be domain-joined and running Windows 7 Enterprise or Ultimate to use DirectAccess. To perform the initial configuration of computers as DirectAccess clients, add them to a Windows group, and then specify this group when you run the DirectAccess Setup Wizard on the DirectAccess server and Windows Server 2008 R2. Include the Name Resolution Policy Table (NRPT). The NRPT is applied to clients only through Local Computer Policy or Group Policy—it cannot be configured locally on the client. To locate NRPT settings in a GPO, navigate to Computer Configuration → Policies → Windows Settings → Name Resolution Policy.

Network Location Server

A network location server is a Web server accessed by a DirectAccess client to determine whether the client is located on the intranet or Internet. The DirectAccess server can act as the network location server, but it is better to use a separate, high-availability Web server for the network location server.

The separate Web server does not have to be dedicated as a network location server. You can configure network location server settings in Local Computer Policy or Group Policy. Use the following path to locate settings in the GPO: Computer Configuration → Policies → Administrative Templates → Network → Network Connectivity Status Indicator.

Domain Controllers

An AD DS infrastructure is required for DirectAccess. At least one domain controller in the domain must be running Windows Server 2008 or later.

IPv6-capable Network

The following task lists the order of connection methods used by DirectAccess:

1. The Native IPv6 method is used if the DirectAccess client is assigned a globally routable IPv6 address.
2. The 6to4 method is used if the DirectAccess client is assigned a public IPv4 address.
3. The Teredo method is used if the DirectAccess client is assigned a private IPv4 address.
4. The IP-HTTPS method is attempted if the other methods fail. For remote client computers to reach computers on the internal corporate network through DirectAccess, the internal computers must be IPv6-compatible. Computers on your IPv4 network are fully IPv6-compatible if:
    a. The computers are running Windows 7, Windows Vista, Windows Server 2008, or Windows Server 2008 R2.
    b. You have deployed ISATAP on the intranet to enable internal servers and applications to be reachable by tunneling IPv6 traffic over your IPv4-only intranet.
    c. You are using a NAT-PT device to translate traffic between DirectAccess clients and intranet computers that support only IPv4.

IPSec

DirectAccess uses IPSec to provide end-to-end security for remote client computers accessing resources on the internal corporate network. IPSec policies are used for authentication and encryption of all DirectAccess connections. These policies can be configured and applied to client computers using Group Policy.

PKI

A PKI is required to issue computer certificates for client and server authentication and also for issuing health certificates when NAP has been implemented. These certificates can be issued by a CA on the internal network—they do not need to be issued by a public CA.

CRL Distribution Points (CDPs)

In a DirectAccess infrastructure, CDPs are the servers that provide access to the CRL that is published by the CA issuing certificates for DirectAccess. Separate CDPs should be published for clients internal to the corporate network and for external clients on the Internet.

Perimeter Firewall

The following ports must be opened on the corporate network perimeter firewall, to support DirectAccess:

- UDP port 3544 to enable inbound Teredo traffic
- IPv4 protocol 41 to enable inbound 6to4 traffic
- TCP port 443 to enable inbound IP-HTTPS traffic

If you need to support client computers that have native IPv6 addresses, the following exceptions will also need to be opened:

- ICMPv6
- IPv4 protocol 50

Manually Configuring DirectAccess for IPv6

DirectAccess clients normally are configured automatically while running the DirectAccess Setup wizard on the DirectAccess server; however, you can configure client IPv6 settings and features manually to help resolve connectivity problems. If necessary while troubleshooting, you can also manually configure DirectAccess for Teredo, 6to4, and IP-HTTPS.

Troubleshooting DirectAccess

The following list describes a number of areas in which a DirectAccess connection must be properly configured. You can use this list as a set of principles and procedures to help troubleshoot DirectAccess clients. The DirectAccess client must have a global IPv6 address.

Use the **ipconfig /all** command on the DirectAccess client.

If the DirectAccess client is assigned public IPv4 address, you should see an interface named Tunnel Adapter 6TO4 Adapter listed in the ipconfig output. This interface should be configured with an address that starts with 2002. The Tunnel Adapter 6TO4 Adapter should also be assigned a default gateway. If the DirectAccess client is assigned a private IPv4 address, you should see a listing for a Teredo interface, and this interface should be configured with an address that starts with 2001.

For IP-HTTPS, look for an interface named Tunnel Adapter Iphttpsinterface. Unless you had a native IPv6 infrastructure in place prior to running the DirectAccess Setup Wizard, the Tunnel Adapter Iphttpsinterface should be configured with an address that starts with 2002. The Tunnel Adapter Iphttpsinterface should also be assigned a default gateway.

The DirectAccess client must be able to reach the IPv6 addresses of the DirectAccess server. Use the i**pconfig /all** command on the DirectAccess server. Note the global IPv6 addresses of the DirectAccess server. From the DirectAccess client, you should be able to ping any of the global IPv6 addresses of the DirectAccess server.

If this attempt is not successful, troubleshoot the connection by looking for the break in IPv6 connectivity between the DirectAccess client and server.

Use the following methods to help fix IPv6 connectivity breaks: If your DirectAccess client is assigned a private IPv4 address, ensure that the local Teredo client is configured as an enterprise client and that the IPv4 address of the DirectAccess server is configured as the Teredo server. To do so, type the following command:

```
netsh interface teredo set state type=enterpriseclient
servername=FirstPublicIP v4AddressOfDirectAccessServer
```

If your DirectAccess client is assigned a public IPv4 address, ensure that the DirectAccess server IPv4 address is assigned as the 6to4 relay by typing the following command:

```
netsh interface 6to4 set relay name=FirstPublicIPv4AddressOfDi
rectAccessServer
```

If these methods fail, you can attempt to use IP-HTTPS to establish IPv6 connectivity to the DirectAccess server. To do so, type the following command:

```
netsh interface httpstunnel add interface client https://
FQDNofDirectAccessServer/ IPHTTPS
```

Using Ping over IPSec
To use Ping as a troubleshooting tool, ensure that Internet Control Message Protocol (ICMP) is exempt from IPSec protection between the DirectAccess client and the remote endpoint of the IPSec connection.

The intranet servers must have global IPv6 addresses. Use the ipconfig /all command on any intranet server that cannot be contacted. The output of the command should list a global IPv6 address. If not, troubleshoot the IPv6 infrastructure on your intranet. For ISATAP networks, ensure that your DNS servers running Windows Server 2008 or later have the name *ISATAP* removed from their global query block lists. In addition, verify that the DirectAccess server has registered an ISATAP A record in the intranet DNS.

Using IP v6/IP v4 NAT Devices
If you are using a NAT-PT or NAT64 device to reach the intranet server, the intranet server will not have a global IPv6 address. In this case, ensure that the NAT-PT or NAT64 device has a global IPv6 address. The DirectAccess client on the Internet must correctly determine that it is not on the intranet.

Type **netsh namespace show effectivepolicy** to display the NRPT on the DirectAccess client. You should see NRPT rules for the intranet namespace and an exemption for the fully qualified domain name (FQDN) of the network location server. If not, determine the network location server URL by typing the following command:

```
reg query HKLM\software\policies\microsoft\windows\
NetworkConnectivityStatusIndicator\ CorporateConnectivity /v
DomainLocationDeterminationUrl
```

Ensure that the FQDN of this URL either matches an exemption entry or does not match the DNS suffix for your intranet namespace in the NRPT.

- The DirectAccess client must not be assigned the domain firewall profile. Type **netsh advfirewall monitor show currentprofile** to display the attached networks and their determined firewall profiles. If you have not yet established a DirectAccess connection, none of your networks should be in the Domain profile. If any of your networks has been assigned the domain profile, determine if you have an active remote access VPN connection or a domain controller that is available on the Internet, and disable that connection.
- The DirectAccess client must be able to contact its intranet DNS servers through IPv6. Type **netsh namespace show effectivepolicy** on the client to obtain the IPv6 addresses of your intranet DNS servers. Ping these IPv6 addresses from the DirectAccess client. If not successful, locate the break in IPv6 connectivity between the DirectAccess client and the intranet DNS servers. Ensure that your DirectAccess server has only a single IPv4 default gateway that is configured on the Internet interface. Also ensure that your DirectAccess server has been configured with the set of IPv4 routes on the intranet interface that allow it to access all of the IPv4 destinations of your intranet.
- The DirectAccess client must be able to use intranet DNS servers to resolve intranet FQDNs. Type **nslookup *IntranetFQDN IntranetDNSServerIPv6Address*** to resolve the names of intranet servers (f*or example: nslookup dc1.corp.contoso.com* 2002:836b:2:1::5efe:10.0.0.1). The output should display the IPv6 addresses of the specified intranet server. If the intranet DNS server cannot be contacted, troubleshoot connectivity to that DNS server. If the server can be contacted but the server name specified is not found, troubleshoot the intranet DNS. (Determine why a Quad A record for the intranet server is not available.)

- The DirectAccess client must be able to reach intranet servers. Use Ping to attempt to reach the IPv6 addresses of intranet servers. If this attempt does not succeed, attempt to find the break in IPv6 connectivity between the DirectAccess client and the i**ntranet *servers.***
- The DirectAccess client must be able to communicate with intranet servers using application layer protocols. Use the application in question to access the appropriate intranet server. If File and Printer Sharing is enabled on the intranet server, test application layer protocol access by typing **net view \\IntranetFQDN**.

VPN

Encapsulation and Tunneling

A VPN works by taking the communication exchanges that computers would use if they were located on the same network, encrypting these exchanges, and then encapsulating the information with the additional networking data needed to cross the Internet.

VPN uses tunneling, where two private computers' IP addresses communicate with each other within the 192.168.10.0/24 subnet, like they were both located on the same network segment, while information passes through a public network. Data is protected with encryption by:

- Data integrity checking
- Data origin checking

Remote Access Infrastructure

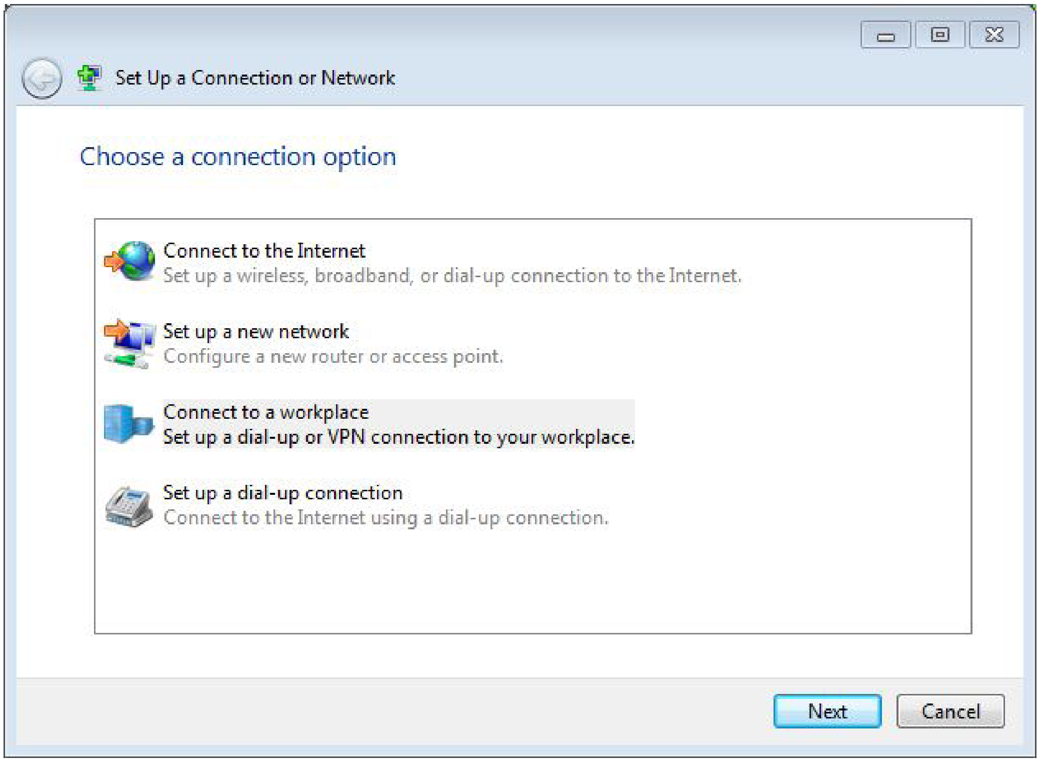
Windows network should include certain features to provide remote access to VPN clients, for example:

- Network connection in Windows
- VPN server running Routing and Remote Access Services (RRAS)
- Internal DNS server
- Domain controller
- Certificate server
- DHCP server
- Network Policy Server (NPS)

Windows 7 must to be configured with a VPN client, such as:

- VPN connection
- Connection Manager (CM) client
- A third-party client

To configure a VPN connection in Windows 7, access the **Set up a New Connection or Network** in **Network and Sharing Center**. Select **Connect to a Workplace** and complete the wizard.


Set Up a Connection or Network

Choose a connection option

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

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

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

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

Figure 26: Creating a VPN Connection

This method works well on a single computer; however, consider using Connection Manager Administration Toolkit (CMAK) to accommodate a network.

CM and CMAK

CM is a client network connection tool that allows a user to connect to a remote network, such as a corporate network protected by a VPN server. The CMAK is a feature in Windows Server 2008 that you can install by using the Add Feature Wizard. It allows you to automate for remote users the creation of predefined connections to remote servers and networks.

Authentication and Authorization

Authentication validates data through verification of a user password or alternative credentials.

Authentication validates user credentials through network policy allowing user access after checking configured permissions on the Properties dialogue box>Dial-in tab.

Remote access authentication precedes domain logon authentication; if a VPN user attempts to remotely log on to a domain, the VPN connection must be authenticated and authorized before they can log on to the domain.

Remote access authorization requirements:

- Verify dial-in properties of the user account for the VPN connection
- Apply the first matching network policy defined on the VPN or NPS

Network Policies

Network policies define various connection types with condition types to allow/decline access requests. For example:

- Windows group membership
- Health policies
- Operating system

DNS

VPN client computers connecting to a private network must be configured with the address of an internal DNS server. The domain controller authenticates the remote access user and acts as the DNS server.

Domain Controller

In a VPN, a domain controller authenticates and authorizes users trying to connect to the network via VPN or remote access. User accounts must be configured with Allow Access or the Control Access through NPS Network Policy network access permission. To set this up, follow this path on the computer: Active Directory Users and Computers console → Properties dialog box → Dial-in tab.

Some VPNs use encryption that relies on public key cryptography and a public key infrastructure (PKI). PKI uses certificates to validate the certificate holder's identities and to encrypt or decrypt data. Each certificate is associated with a key pair, composed of a public key and a private key.

DHCP Server

An internal DHCP server is used to provide VPN clients with an IP address. In this case, you must configure the external adapter of the VPN server a DHCP Relay Agent, which responds to DHCP requests from external VPN clients.

- You can also configure the VPN server to assign addresses to VPN clients without the help of the DHCP server on the corporate network NPS server NPS is the Microsoft implementation of a RADIUS server and proxy.
- An NPS server can be used to manage authentication and authorization centrally.
- NPS is the replacement for Internet Authentication Service (IAS) in Windows Server 2003.

VPN Tunneling Protocols

Windows 7 supports four tunneling protocols for remote access VPN connections to corporate networks. Each of these is used in different remote access scenarios, and each has different requirements for the operating system, configuration, and infrastructure. The following section introduces these four VPN protocols in more detail.

IKEv2

Administrators must thoroughly understand **VPN Reconnect**. The VPN Reconnect feature helps administrators maintain VPN connections when a VPN client moves between wireless hotspots or switches from a wireless to a wired connection. Only IKEv2 VPNs support this feature.

- IKEv2 is the preferred VPN type.
- Internet Key Exchange version 2 (IKEv2) is new in Windows 7 and Windows Server 2008 R2.
- Windows 7 for the VPN client and Windows Server 2008 R2 on the VPN server.
- This tunneling protocol uses Internet Protocol Security (IPSec) for encryption.
- It supports VPN Reconnect Mobility.
- The VPN Reconnect feature enables VPN connection maintenance when a VPN client moves between wireless hotspots or switches from a wireless to a wired connection.
- With IKEv2, client computers are not required to provide authentication through a machine certificate or a pre-shared key.
- Other VPN types function on IPSec encryption (L2TP); IKEv2 provides improved performance and faster connectivity.
- IKEv2 VPNs require.
    - PKI.
    - Server validated authentication certificate installed in the Trusted Root Certification Authorities certificate store.

SSTP

SSTP VPNs first appeared Windows Server 2008 and are compatible with Vista SP1 or later. It is based on the same HTTP-over-SSL protocol used for secure Web sites. The primary feature of an SSTP-type VPN is that it only uses TCP port 443 for communication, an open port on most firewalls facilitating secure Web traffic. Most firewalls do not need to be reconfigured because SSTP communication enables SSTP VPN clients to connect through most Network Address Translation (NAT) devices, firewalls, and Web proxies. Other VPN do not include this feature. An SSTP VPN is a flexible type of remote access VPN that can you can implement in more network scenarios than other VPNs.

SSTP VPNs can be used by clients running Windows Vista SP1 or later.

- SSTP-type VPN only uses TCP port 443 for communication, a port left open on most firewalls for secure Web traffic.
- SSTP uses the same HTTP-over-SSL protocol as secure Web sites.
- With SSTP, most firewalls do not require reconfiguration because SSTP communication allows clients to connect through most Network Address Translation (NAT) devices, firewalls, and Web proxies.

L2TP

L2TP is an industry-standard tunneling protocol designed to run natively over IP networks. Security for L2TP VPN connections is provided by IPSec, which performs the data authentication and encryption required to ensure L2TP tunnels are protected.

- The combination of L2TP with IPSec for tunneling purposes is usually referred to as L2TP over IPSec or L2TP/IPSec.
- L2TP/IPSec VPNs have drawbacks compared to IKEv2 and SSTP VPNs:
- It requires user authentication as all with all VPN protocols do, but L2TP/IPSec also requires client computer authentication. Therefore, all VPN client connected computers must be configured either with a computer certificate or a preshared key specific to the VPN server.
- L2TP/IPSec prevents users from establishing a VPN connection from public terminals or from any computer that has not been specially configured for the VPN.
- To configure a VPN client connection running Windows 7 to use either a computer certificate or a pre-shared key for L2TP/IPSec authentication:
    - Open the Properties dialog box of the VPN connection
    - Click the Security tab
    - Click Advanced Settings. This step opens the Advanced Properties dialog box. By default, certificate authentication is selected.
- To obtain a client authentication certificate to use with this setting, you typically need to submit a request to the CA on the corporate network and then install the certificate.
- For Authentication, you need to supply the key in the area provided.
- L2TP/IPSec VPNs do not natively support the traversal of NAT devices. But, you can enable L2TP/IPSec to cross a NAT device if you change a particular registry value on both the VPN client computer and the VPN server.

PPTP

Advantages

PPTP is the easiest VPN protocol to implement in Windows networks. PPTP, for the following reasons:

- Does not require any certificates or pre-shared keys on either the VPN client or server.
- Can be used with older Windows operating systems.
- Can run on Microsoft Windows NT 4.0, and it is compatible with all versions of Windows since Microsoft Windows 2000.

Disadvantages

PPTP has the following disadvantages compared to other VPN protocols:

- Is not as secure as other VPN protocols.
- Does not ensure data integrity or data origin authentication.
- Can traverse NAT devices only through PPTP-enabled NAT routers.

Troubleshooting Connectivity

Use the following list to help you troubleshoot VPN client connectivity:

- Verify that the VPN client connection is configured properly with the VPN server name or IP address.
- Verify that the VPN client computer has an active Internet connection. The VPN connection can be established only when the client is connected to the Internet.
- Verify that the proper user credentials are defined in the VPN connection.
- Verify that the user is authorized for remote access.
- If an error message with code 741 appears and indicates that the local computer does not support encryption, verify that that encryption settings defined in the VPN connection are compatible with those defined on the server.
- Verify that certificates are configured properly for the VPN connection. For instance, verify that the certificate of the root CA that has issued the VPN server's computer certificate is installed in the Trusted Root Certification Authorities store on the VPN client computer. In the case of an L2TP/IPSec VPN, verify that the VPN client computer has installed a computer certificate that can be validated by the VPN server.

Domain 5: Identifying Cause of and Resolving Security Issues

Identify and Resolve Internet Explorer Security Issues

In Windows 7, Windows Internet Explorer 8.0 is configured by default to minimize security risks. Therefore, Internet Explorer has minimal privileges and more Add-ons will **not** run by default.

Add-ons

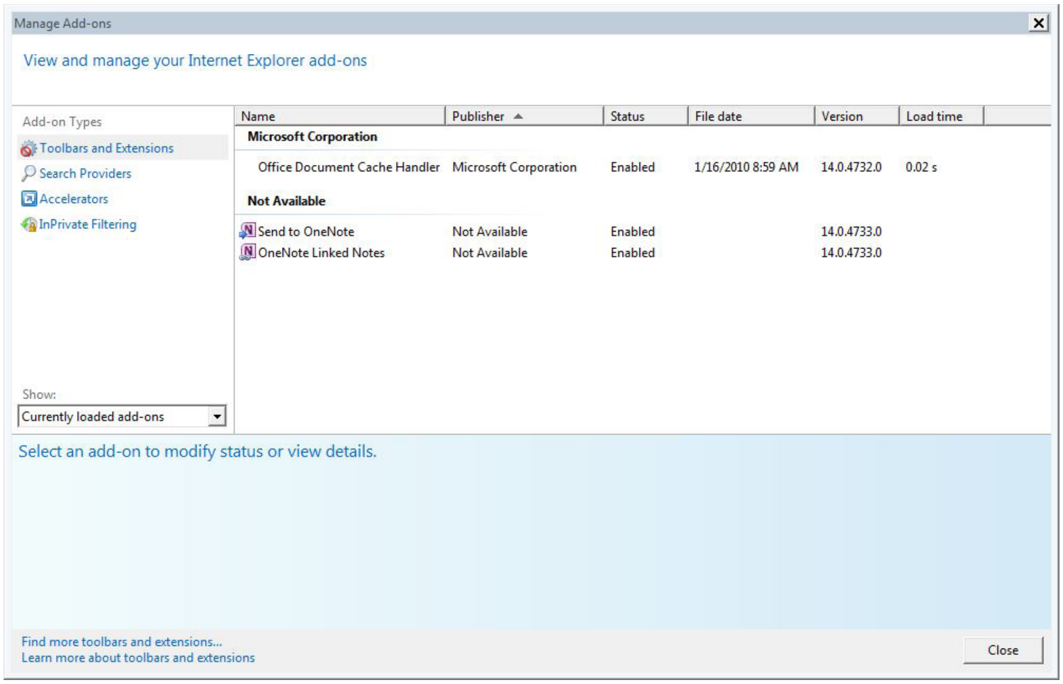
Add-ons work with Internet Explorer. Add-ons help Web sites provide more interactive content. Some common Add-ons are:

- Shockwave Flash
- Adobe PDF
- Windows Media Player

Enable and Disable Add-ons

After starting Internet Explorer, you can disable or delete Add-ons by following these steps:

1. Click the Tools button on the toolbar, and then click Manage Add-ons. The **Manage Add-ons dialog box** appears as below:



View and manage your Internet Explorer add-ons

Name	Publisher	Status	File date	Version	Load time
Microsoft Corporation					
Office Document Cache Handler	Microsoft Corporation	Enabled	1/16/2010 8:59 AM	14.0.4732.0	0.02 s
Not Available					
Send to OneNote	Not Available	Enabled		14.0.4733.0	
OneNote Linked Notes	Not Available	Enabled		14.0.4733.0	

Select an add-on to modify status or view details.

Figure 27: Managing IE8 Addons

2. To prevent the Add-on from automatically loading, select it, and click Disable.

Use the following task to disable Add-ons without opening Internet Explorer:

1. Click Start\Control Panel.
2. Click the **Network and Internet link.** . Under Internet Options, click the **Manage Browser Add-ons** line. The Internet Properties dialog box appears. Click Manage Add-ons.
3. In the Manage Add-ons dialog box, select an Add-on, then click Disable to prevent the Add-on from automatically loading.

Configure Add-ons in AD DS Domain Environments
You configure Group Policy settings in Windows 7 to enable or disable specific Add-ons in the same manner as with earlier versions of Internet Explorer. Use the Group Policy settings Management in: **User Configuration** → **Policies** → **Administrative Templates** → **Windows Components** → **Internet Explorer** → **Security Features** → **Add-on**

Most often you must enable the following settings in order to block all unapproved Add-ons:

- Add-on List
- Deny All Add-ons Unless Contained In The Add-on List

Two other **Group Policy settings** related to **Add-on management** are located within both **User Configuration** and **Computer Configuration** at: Administrative Templates →Windows Components → Internet Explorer

The settings that relate to managing Add-ons are:

- **Crash Detection**: When turned on, this setting allows Internet Explorer to detect an add-on that crashes, and then disables it the next time Internet Explorer is opened.
- **Enable Or Disable Add-ons**: When turned on, this policy setting allows users to open the Manage Add-Ons dialog box to enable or disable add-ons.

Configure ActiveX Add-ons

ActiveX technology enables powerful applications to run within a Web browser. Organizations have developed ActiveX components as part of a Web application. In retaliation, attackers have created ActiveX components to abuse the platform's capabilities. Some examples of ActiveX controls include:

- A component that enables you to manage virtual computers from a **Microsoft Virtual Server Web page**
- A **Microsoft Update component** that scans your computer for missing updates
- **Shockwave Flash**, which Web sites can use to publish complex animations and games

Note: Adobe doesn't currently have a 64-bit Flash Player. Windows 7 has the ActiveX Controller Service to manage legacy ActiveX controls.

Internet Explorer and 64-bit Windows 7

ActiveX was designed in earlier versions of Windows; however, with the incorporation of 64-bit technology, Windows 7 has some interface issues with it. 64-bit computing provides a wider data bus, allowing much greater scalability; future Windows platforms will certainly use it. Right now, however, most users run 32-bitversions of Windows on older Windows platforms.

For that reason, the 32-bit version of Internet Explorer is the default even in 64-bit versions of Windows. If a user chooses to use the 64-bit version of Internet Explorer, then test for any problematic Web pages in the 32-bit version of Internet Explorer before troubleshooting.

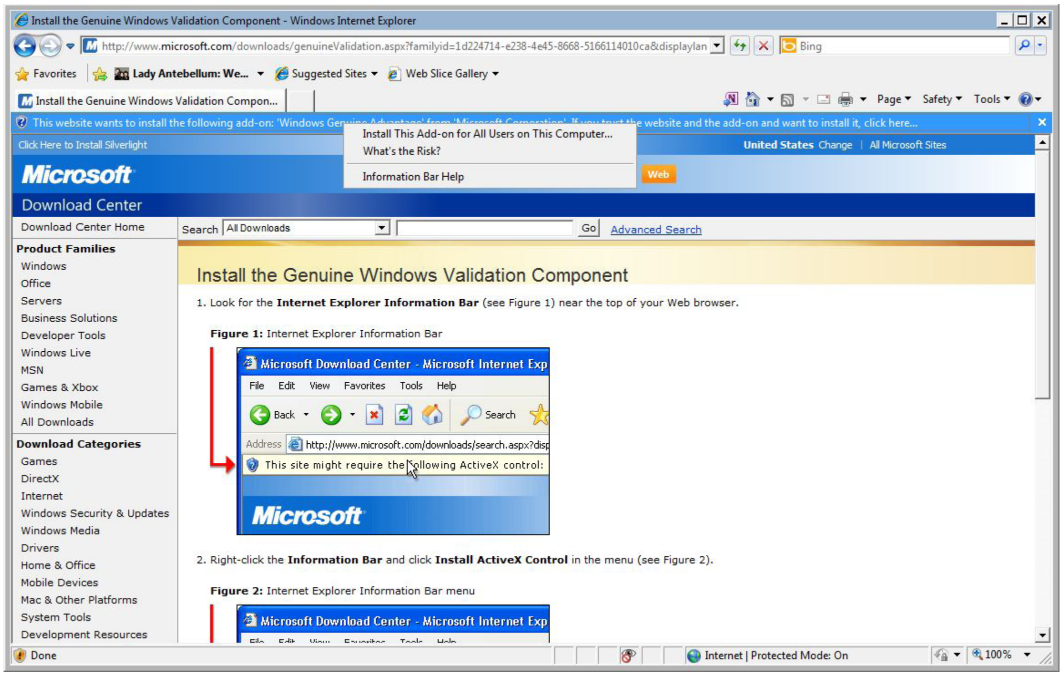
Earlier versions of Internet Explorer installed ActiveX controls without prompting the users. This improved Web site interaction that used ActiveX controls because the user was able to enjoy the control's features without install it. However, malware attackers have created malicious ActiveX controls that installed software on the user's computer or changed other settings. To help use ActiveX controls while blocking potentially dangerous ActiveX controls, Microsoft designed vibrant ActiveX management capabilities for Internet Explorer.

Configuring ActiveX

The following describes how to configure ActiveX on Internet Explorer 8 on a single computer and within an enterprise.

ActiveX controls are not installed by default. Instead, when users visit a Web page that includes an ActiveX control, they see an information bar that informs them that an ActiveX control is required. Users then must click the information bar and Install ActiveX Control.

The following screen sample gives an example of the **Genuine Microsoft Software Web page**, which requires users to install an ActiveX control before their copy of Windows can be genuinely validated.



This website wants to install the following add-on: 'Windows Genuine Advantage' from 'Microsoft Corporation'. If you trust the website and the add-on and want to install it, click here...

Install the Genuine Windows Validation Component

1. Look for the **Internet Explorer Information Bar** (see Figure 1) near the top of your Web browser.

Figure 1: Internet Explorer Information Bar

This site might require the following ActiveX control:

2. Right-click the **Information Bar** and click **Install ActiveX Control** in the menu (see Figure 2).

Figure 2: Internet Explorer Information Bar menu

Install the Genuine Windows Validation Component - Windows Internet Explorer
http://www.microsoft.com/downloads/genuineValidation.aspx?familyid=1d224714-e238-4e45-8668-5166114010ca&displaylan
Bing
Favorites
Lady Antebellum: We...
Suggested Sites
Web Slice Gallery
Install the Genuine Windows Validation Compon...
Page
Safety
Tools
Install This Add-on for All Users on This Computer...
What's the Risk?
Information Bar Help
Click Here to Install Silverlight
United States Change | All Microsoft Sites
Microsoft
Web
Download Center
Download Center Home
Search
All Downloads
Go
Advanced Search
Product Families
Windows
Office
Servers
Business Solutions
Developer Tools
Windows Live
MSN
Games & Xbox
Windows Mobile
All Downloads
Download Categories
Games
DirectX
Internet
Windows Security & Updates
Windows Media
Drivers
Home & Office
Mobile Devices
Mac & Other Platforms
System Tools
Development Resources
Microsoft Download Center - Microsoft Internet Exp
File Edit View Favorites Tools Help
Back
Search
Address
http://www.microsoft.com/downloads/search.aspx?disp
Microsoft
Done
Internet | Protected Mode: On
100%

Figure 28: Adding an ActiveX Control

After the user clicks **Install This Add-on**, the user must provide administrative credentials from a UAC prompt. The user then receives a second security warning from Internet Explorer. If the user confirms this security warning, Internet Explorer installs and runs the ActiveX control.

ActiveX Opt-in is enabled by default for the Internet and Restricted Sites zones, but disabled by default for the Local Intranet and Trusted Sites zones. Therefore, any Web sites on your local intranet should be able to install ActiveX controls without prompting the user.

Use the following procedure to change the setting default for a zone:

1. Open Internet Explorer. Click Tools on the toolbar, and Internet Options.
2. In the **Internet Options dialog box**, click the **Security tab**. Select the zone to edit, click the Custom Level button.
3. Scroll down in the Settings list. Under **ActiveX Controls and Plug-Ins**, change the setting for the first option, which is Allow Previously Unused ActiveX Controls to Run without Prompt. If this is disabled, ActiveX Opt-in is enabled. Click OK twice.

Enabling ActiveX Opt-in

- This causes Internet Explorer **not** to install ActiveX controls by default, instead it requires the user to choose to configure the Add-on.
- ActiveX Opt-in applies to most ActiveX controls; however, it does not apply for controls on the preapproved list. The preapproved list is maintained in the registry at **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Ext\PreApproved**.
- Within this key, there are several **subkeys**, each with a **Class ID (CLSID) of a preapproved ActiveX control**. You can identify an ActiveX control's CLSID by viewing the source of a Web page and searching for the <*object*> tag. For best results, try searching for "<object" in the source of a Web page.

Note: The previous section described how to configure ActiveX Opt-in on a single computer. In addition to that setting, you can configure several other per-zone settings related to ActiveX from the **Security Settings dialog box**:

- Download Signed ActiveX Controls
- Automatic Prompting For ActiveX Controls
- Download Unsigned ActiveX Controls
- Run ActiveX Controls And Plug-Ins
- Initialize And Script ActiveX Controls Not Marked As Safe For Scripting
- Script ActiveX Controls Marked Safe For Scripting

How to Manage ActiveX Add-Ons
Use the following procedure to configure ActiveX on a single computer:

1. Open **Internet Explorer**.
2. Click the Tools button, click **Manage Add-ons\Enable or Disable Add-ons**. The Manage Add-ons dialog box appears.
3. Click the **Show list\Downloaded ActiveX Controls**.
4. Select the ActiveX control you want to manage; then select either:
    a. Disable to disable the ActiveX control.
    b. Delete to remove the ActiveX control.

Configure ActiveX Installer Service
You can use the ActiveX Installer Service to enable standard users to install specific ActiveX controls. Use this procedure to configure the list of sites approved to install ActiveX controls:

1. Open the Group Policy Object (**GPO**) in the Group Policy Object Editor.
2. Browse to **Computer Configuration\Administrative Templates\Windows Components\ActiveX Installer Service**.
3. Double-click the **Approved Installation Sites for ActiveX Controls setting**. Enable it.
4. Click **Show to specify host Uniform Resource Locators (URLs) that are allowed to Distribute ActiveX controls**. In the Show Contents dialog box, click Add and configure the host URLs:
    a. **Configure each item name** as the host name of the Web site from which clients will download the updated ActiveX controls, such as *http://activex.microsoft.com*.
    b. **Configure each value name** using four numbers separated by commas (such as "2,1,0,0"). These values are described later in this section.
5. Click OK to save the setting for the new policy.

When you configure the list of approved installation sites for ActiveX Controls, you configure a name and value pair for each site. The name will always be the URL of the site hosting the ActiveX control. The value consists of four numbers:

- **Trusted ActiveX Controls –** define the first number as 0 to block trusted ActiveX controls from being installed, as 1 to prompt the user to install trusted ActiveX controls, or as 2 to install trusted ActiveX controls automatically, without prompting the user.
- **Signed ActiveX Controls –** define the second number as 0 to block signed ActiveX controls from being installed, as 1 to prompt the user to install signed ActiveX controls, or as 2 to install signed ActiveX controls automatically, without prompting the user.

- **Unsigned ActiveX Controls –** define the third number as 0 to block unsigned ActiveX controls from being installed or define this number as 1 to prompt the user to install unsigned ActiveX controls. You cannot configure unsigned ActiveX controls to be installed automatically.
- **Server Certificate Policy –** set this value to 0 to cause the ActiveX Installer Service to abort installation if there are any certificate errors. Alternatively, you can set it to 256 to ignore an unknown CA, 512 to ignore invalid certificate usage, 4096 to ignore an unknown common name in the certificate, or 8192 to ignore an expired certificate. Add these numbers to ignore multiple types of certificate errors.

Trusted Sites List

By default, Internet Explorer is configured to prevent Internet Web sites from performing many actions that could compromise the computer's security or the user's privacy. But, some legitimate Web sites may need to perform those actions to allow Web applications to run properly. Administrators can add sites to the Trusted Sites list to grant them additional privileges.

Use the following procedure to add a site to the Trusted Sites list:

1. In Internet Explorer, click the Tools menu on the toolbar, and **Internet Options**.
2. In the Internet Options dialog box, click the **Security tab**. Click **Trusted Sites**, and **Sites**.
3. In the **Trusted Sites** dialog box, clear the **Require Server Verification** check box if you access the server using HTTP rather than HTTPS.
4. In the **Add This Website to the Zone box**, type the URL of the Web site, and click Add.
5. Click Close.

The next time you visit the site, Internet Explorer grants it all the privileges assigned to the Trusted Sites list.

Protected Mode

In versions of Windows before Vista, many computers security was compromised when Web sites containing malicious code abused Web browsers of systems to run corrupt code on client computers. Since any new process spawned by an existing process inherits the privileges of the parent process and the Web browser ran with the user's full privileges, malicious processes could received the same privilege as the user. With the user's elevated privileges, the malicious process could install software and transfer confidential documents.

Protected Mode is only enabled if malicious code runs on the Web browser. If this occurs, Protected Mode limits the damage the process can cause without the user's permission. Protected Mode is not available when Internet Explorer is installed on Windows XP because it requires several security features that are only incorporated in Windows Vista and Windows 7 (interacting with Internet Explorer 8).

Mandatory Integrity Control (MIC) is a feature of Windows 7 that enables Protected Mode. MIC uses integrity access levels (ILs) to label processes, files, folders, and registry keys, as explained below. Internet Explorer runs with a low IL, therefore it can only access other low IL resources without the user's permission.

Protected Mode and Mandatory Integrity Control (MIC)

One of the features of Windows 7 that enables Protected Mode is Mandatory Integrity Control (MIC). MIC labels processes, folders, files, and registry keys using one of four integrity access levels (ILs), as shown below. Internet Explorer runs with a low IL, which means it can access only other low IL resources without the user's permission:

IL	System Privileges
System	**System** – processes have unlimited access to the computer.
High	**Administrative** – processes can install files to the Program Files folder and write to sensitive registry areas like HKEY_LOCAL_MACHINE.
Medium	**User** – processes can create and modify files in the user's Documents folder and write to user-specific areas of the registry such as HKEY_CURRENT_USER. Most files and folders on a computer have a medium integrity level because any object without a mandatory label has an implied default integrity level of Medium.
Low	**Untrusted** – processes can write only to low-integrity locations such as the Temporary Internet Files\Low folder or the following Key: HKEY_CURRENT_USER\Software\LowRegistry key.

Figure 29: Mandatory Integrity Control Levels

Compatibility Logging

Some web applications and Internet Explorer Add-ons developed for earlier versions of Internet Explorer have compatibility problems when you run them with Internet Explorer 8 and Windows 7. You can identify the exact compatibility problem by enabling compatibility logging with Group Policy. Use the following procedure to enable compatibility logging on a local computer:

1. Click Start, type **gpedit.msc**, and press Enter.
2. In the **Group Policy Object Editor**, browse to **User Configuration\Administrative Templates\Windows Components\Internet Explorer**. If you need to enable compatibility logging for all users on the computer, browse to Computer Configuration\Administrative Templates\Windows Components\Internet Explorer.
3. Double-click the **Turn on Compatibility Logging setting**. Select Enabled, and then click OK.
4. Start Internet Explorer or Restart it if it is currently open.

With compatibility logging enabled, reproduce the compatibility problem.

You should then be able to **view events in the Event Viewer snap-in** under **Applications and Service Logs\Internet Explorer**

Note: If the home page resets after a period of time passes, it means that group policy refresh is kicking in and resetting the home page. You must change the policy or disallow the user from setting the home page.

Certificate Problems

Certificates are basically handled the same in Windows 7 as in earlier versions of Windows. Certificates are used for many security-related tasks in Internet Explorer:

- Traffic Encryption
- Authenticating Server
- Authenticating Client Sites

If Internet Explorer detects a problem with a certificate, it displays the following message: **"There is a problem with this website's security certificate".**

The following list describes common problems that can occur when using certificates in Internet Explorer:

- The security **certificate** presented by this Web site was **issued for a different Web site's address**.
- **Administrator manual error**: for example, an administrator may have mistyped the server's host name when requesting the certificate or the administrator might have installed the wrong certificate on the server.
- The server is **impersonating a server** with a different host name. For example, an attacker might have set up a Web site to impersonate a site. However, the attacker may use a different SSL certificate on the Web site. Earlier versions of Internet Explorer display a less threatening error message; so many users may bypass the error and continued to the malicious site.
- Certificates have a **limited lifespan,** usually one to five years/or it can depend on what the domain administrators specifies for internal PKI, or the register for public certificates. If the certificate has expired, the server administrator should request an updated certificate and apply it to the server.
- **Certificate Authority (CA) –** anyone, including attackers, can create a CA and issue certificates. Therefore, Internet Explorer does not trust all CAs by default. Instead, Internet Explorer trusts only very few public CAs. If the certificate was issued by a speculative CA and the Web site is on the public Internet, the server administrator should acquire a certificate from a trusted CA. If the Web site is on the organization's intranet, a client administrator should configure Internet Explorer to trust the issuing CA. In AD DS domains, member computers automatically trust enterprise CAs.

Testing Windows 7 by Issuing an Untrusted Certificate
Use this procedure to issue an internal certificate to a Web server as a test to determine how Windows 7 handles it as a member of the domain and from outside the domain.

1. Connect to a **Windows Server 2008 R2 AD DS** domain controller in a test environment, and log on as an administrator.
2. Click Start, click **Administrative Tools**, and click **Server Manager**.
3. In **Server Manager**, click the **Roles node**, Add Roles.
4. On the **Before You Begin page**, click Next.
5. On the **Select Server Roles page**, select **Active Directory Certificate Services**, and click **Next**.
6. On the **Introduction to Active Directory Certificate Services page**, click **Next**.
7. On the **Select Role Services** page, select **Certification Authority, Certification Authority Web Enrollment**, and **Online Responder**. When prompted to add other services, click Add Required Role Services. Click Next.
8. Examine the results in Windows 7.

Group Policy Restrictions

Organizations require strict control over their users' Web browsing abilities. Internet Explorer provides allot of flexibility here. For example, administrators can use Group Policy settings to turn off tabbed browsing, allow pop-ups, turn off suggestions, restrict search providers, or turn off the Favorites bar.

If a user complains that an Internet Explorer feature is not working correctly, you should determine whether Group Policy restrictions could be the problem. You can use the Resultant Set of Policy tool to determine which settings have been defined for a user or computer, and which Group Policy objects are responsible.

Use the following procedure to use the Resultant Set of Policy tool:

1. Click Start, type **rsop.msc**, and press Enter.
2. In the **Resultant Set of Policy** window, within the **Computer Configuration or User Configuration**, select the **Administrative Templates\Windows Components\Internet Explorer node**.

Identify and Resolve Encryption Issues

Windows 7 provides two file encryption technologies that protect data in the event of a threat, such as hardware theft or hacking:

- **BitLocker** (for encrypting the entire system drive; new in Windows 7)
- **EFS** (for encrypting individual files, folders and non-system drives)

BitLocker

The following lists BitLocker differences from EFS:

- BitLocker encrypts entire volumes, including the system volume and all user and system files. EFS cannot encrypt system files.
- BitLocker protects the computer at startup before the operating system starts. After the operating system starts, BitLocker is transparent.
- BitLocker provides computer-specific encryption, not user-specific encryption. So, you still must use EFS to protect private files from other valid users.
- BitLocker can protect the integrity of the operating system, helping to prevent rootkits and offline attacks that modify system files.

Windows 7 and BitLocker

The BitLocker feature is only offered on:

- Windows 7 Enterprise
- Windows 7 Ultimate

Windows 7 setup automatically configures partitions compatible with BitLocker (as opposed to previous Windows versions).

BitLocker and Trusted Platform Module (TPM) Hardware

BitLocker seals the **symmetric encryption key** in a Trusted Platform Monitor (TPM) if an attacker modifies the computer. This is applicable for a computer with TPM.

Note: If available, BitLocker seals the symmetric encryption key in a Trusted Platform Module (TPM) 1.2 chip (available in some newer computers). If the computer does not have a TPM chip, BitLocker stores the encryption key on a USB flash drive when the computer starts.

Many computers with TPM have the TPM chip disabled in the basic input/output system (BIOS).
To determine if a computer has TPM and to initialize it, you should enter the computer's BIOS settings and enable it. After you enable the TPM chip, BitLocker automatically performs the TPM initialization.

To initialize TPM chips manually and turn them on or off at the operating system level, Windows 7 includes the TPM Management snap-in, as shown below. To use it, open a blank MMC console and add the snap-in.

- If a computer does not have a **TPM chip** (1.2 chip available in newer computers), BitLocker stores encryption keys on a USB flash drive.
- If TPM-equipped computers have the TPM chip disabled in the basic input/output system (BIOS), you must enter the computer's **BIOS settings**. After you enable the TPM chip, BitLocker automatically performs the TPM initialization.
- To manually initialize TPM chips (and turn them on or off through the operating system), Windows 7 provides the **TPM Management snap-in**. If required, open a blank MMC console and add the snap-in.

BitLocker and TPM
BitLocker handles TPM initialization. BitLocker includes several modes available on computers with TPM hardware, such as:

- **TPM only**: TPM-only mode provides protection from hard-disk theft and is transparent to the user. The user logon appears the same as it was before BitLocker was enabled; however, during startup, BitLocker communicates TPM hardware and validates the computer and operating system integrity. BitLocker enters recovery mode if:
  - critical startup files have changed.
  - the TPM is missing or changed.
  - the hard disk is moved to a different computer.

  To regain access to data while in recovery mode, the user must enter a 40-digit recovery key or insert a USB flash drive with a recovery key stored on it.
- **TPM with external key**: BitLocker performs the same checks as TPM-only mode; however, it also requires the user to provide an external key to start Windows (normally a USB flash drive with a certificate stored on it). This provides protection from both hard-disk theft and stolen computers.
- **TPM with PIN and external key**: BitLocker prompts the user to type a PIN and insert a USB flash drive to start Windows.
- **TPM with PIN**: BitLocker requires the user to enter a PIN to start Windows.
- **BitLocker Encryption on Non-TPM Compliant Computers**: BitLocker prompts the user to provide an external key and to type a PIN.

If TPM hardware is not available, BitLocker can store decryption keys on a USB flash drive instead of using a built-in TPM module. Windows 7 does not make this option available by default. To use BitLocker encryption on a computer without a compatible TPM, you need to change a computer Group Policy setting by performing these steps:

1. Open the **Group Policy Object Editor**, type **gpedit.msc**, and press Enter. A UAC prompt appears.
2. Follow the path: **Computer Configuration → Administrative Templates → Windows Components → BitLocker Drive Encryption → Operating System Drives**.
3. Enable the **Require Additional Authentication at Startup** setting. Then select the **Allow BitLocker without a Compatible TPM** check box. Click OK.

Note: Use Group Policy settings to deploy BitLocker in an enterprise using USB flash drives instead of TPM.

BitLocker Keys
Perform the following task to manage keys on the local computer:

1. Open Control Panel and click the System and Security link. On BitLocker Drive Encryption, click Manage BitLocker link.
2. In the **BitLocker Drive Encryption window**, click Manage BitLocker. Use Manage BitLocker to perform the following actions:
    - **Saving Recovery Key –** provides the following options:
        - Save The Recovery Key To A USB Flash Drive
        - Save The Recovery Key To A File
        - Print The Recovery Key
    - **Reset the PIN –** when you use a PIN for authentication, you can change the PIN. Use the Manage-bde tool (replaces the Manage-bde.wsf script in Windows Vista) to manage BitLocker from an elevated command prompt or from a remote computer.
    - **Duplicate Startup Key –** use a USB startup key for authentication to create a second USB startup key with an identical key.

Recovering BitLocker Data
If using BitLocker to protect the system partition, the partition will be locked if the encryption key is not available, causing BitLocker to go into recovery mode. Some common causes of the encryption key not being available include:

- A boot file is modified.
- The TPM is cleared.
- An attempt is made to boot without the TPM, PIN, or USB key.
- BIOS is modified and the TPM disabled.
- The BitLocker-encrypted disk has been transferred a new computer.
- Note to reviewer: added this definition of BitLocker and EFS to the Encryption Issues primary topic introduction above.
- After locking the drive, you can only boot to recovery mode.
- Press the Esc key to restart the computer. BitLocker reads the recovery key automatically during startup.

Identify and Resolve Issues due to Malicious Software

You need to know how to minimize the risk of damage from malware by implementing User Account Control (UAC) at an appropriate level, by using Windows Defender, and by removing unwanted software if it is discovered.

Windows 7 includes two features that assist you in this fight against malware. **User Account Control (UAC)** (introduced in Windows Vista, but refined in Windows 7) helps prevent programs from secretly altering protected areas of the operating system, and a new feature, **Windows Defender,** that scans your system for spyware and offers to remove any unwanted software that is detected.

You will also need to use additional applications such as Microsoft Forefront and a managed anti-malware solution to protect your network, however, understanding how to use and configure built-in features of Windows 7 such as UAC and Windows Defender are the essential skill knowledge you require to pass the test.

Malware Explained

Malware is generic term for many different types of unwanted software. It's important to understand the nature of these different threats, but it's also important to recognize that many malware applications combine features from more than one of these malware types. The following lists the most common types of malware:

- Virus
- Worm
- Trojan horse Spyware
- Adware
- Backdoor
- Rootkit

Diagnosing Malware Infection

Below lists common signs of a system infected by a virus, worm, or Trojan horse:

- Printing problems
- Sluggish computer performance
- Unusual error messages
- Unusual audio sounds
- Distorted menus and dialog boxes
- Antivirus software repeatedly turning itself off
- Inaccessible disk drives, or a CD-ROM drive that automatically opens and closes
- Screen freezing
- Computer crashing
- Computer restarting
- Applications not functioning correctly
- Notification messages that an application has attempted to contact you from the Internet

Understand that these symptoms can also indicate other types of hardware or software problems that are unrelated to malware. Symptoms of a spyware infection can differ from those of other types of malware. If you see any of the following symptoms, suspect Malware:

- The computer runs more slowly than usual.
- A new, unexpected application appears.
- Unexpected icons appear in the system tray.
- The Web browser displays additional advertisements when visiting a Web page, or pop-up advertisements appear when the user is not using the Web.
- Unexpected notifications appear near the system tray.
- When the user attempts to visit a Web page, she is redirected to a completely different Web page.
- The Web browser home page, default search engine, or favorites change.
- New toolbars appear, especially in Web browsers.
- The mouse pointer changes.

Spyware may not display any noticeable symptoms, but it still can compromise private data.

Resolving Malware Infections

The most important way to resolve malware infections is to prevent them in the first place by **running antivirus and anti-spyware programs daily** with the latest virus and spyware definitions. If malware is discovered on a system, use the application to remove the malware if possible and quarantine it if not. If it is a new malware program, you might need to run a removal tool or perform a series of steps to remove it manually.

These steps apply to malware that is detected. However, as important as it is to remember to use antivirus and anti-spyware daily, it is just as important to remember that no anti-malware application is perfect. Many malware programs are written around anti-malware software so that they cannot be detected. If only one malicious feature remains after a scan, that remaining malware program can install other malware programs.

If you suspect a problem related to malware after running antivirus and anti-spyware applications with the latest definitions, consider using UAC and Windows Defender to troubleshoot.

User Account Control (UAC)

UAC is a set of security features designed to minimize the danger of running Windows as an administrator and to maximize the convenience of running Windows as a standard user. In versions of Windows before Windows Vista, malware could use the credentials of a locally logged-on administrator to damage a system.

UAC basically works the same in Windows 7 as it does in earlier versions, with the following exceptions:

- Administrators in Windows 7 **do not see a UAC notification when they adjust Windows settings that require administrator privileges**.
- Administrators see **UAC prompts less frequently** in Windows 7.
- **Validated** When this policy setting is enabled, Windows 7 refuses to run any executable that isn't signed with a trusted certificate, such as a certificate generated by an internal.

- I’m trying to explain how UAC is different in Windows 7 here for quick reference.
- **Public Key Infrastructure (PKI)** When disabled, this policy setting allows users to run any executable, potentially including malware. If your environment requires all applications to be signed and validated with a trusted certificate, including internally developed applications, you can enable this policy to increase security greatly in your organization. This setting is disabled in **Local Security Policy** by default.
- **The Only Elevate UI Access Applications That Are Installed In Secure Locations Policy** When enabled, this policy setting causes Windows 7 to grant user interface access only to those applications that are started from Program Files or subfolders, from Program Files (x86) or subfolders, or from \Windows\System32\.

Other UAC Changes in Windows 7
For administrators, the default behavior of UAC in Windows 7 has significantly changed from that in Windows Vista and Windows Server 2008. In those operating systems, UAC generated a prompt by default whenever any type of elevation was requested, including when an administrator attempted to change Windows settings.

The UAC notification that normally appears for administrators is called **consent prompt**.
Insert screenshot of UAC consent prompt compared to a screen sample of UAC Elevation prompt here.

By default, the entire screen darkens when the notification appears and freezes until the user responds to the prompt. This feature is called the **Secure Desktop** and can be disabled.

Windows Defender

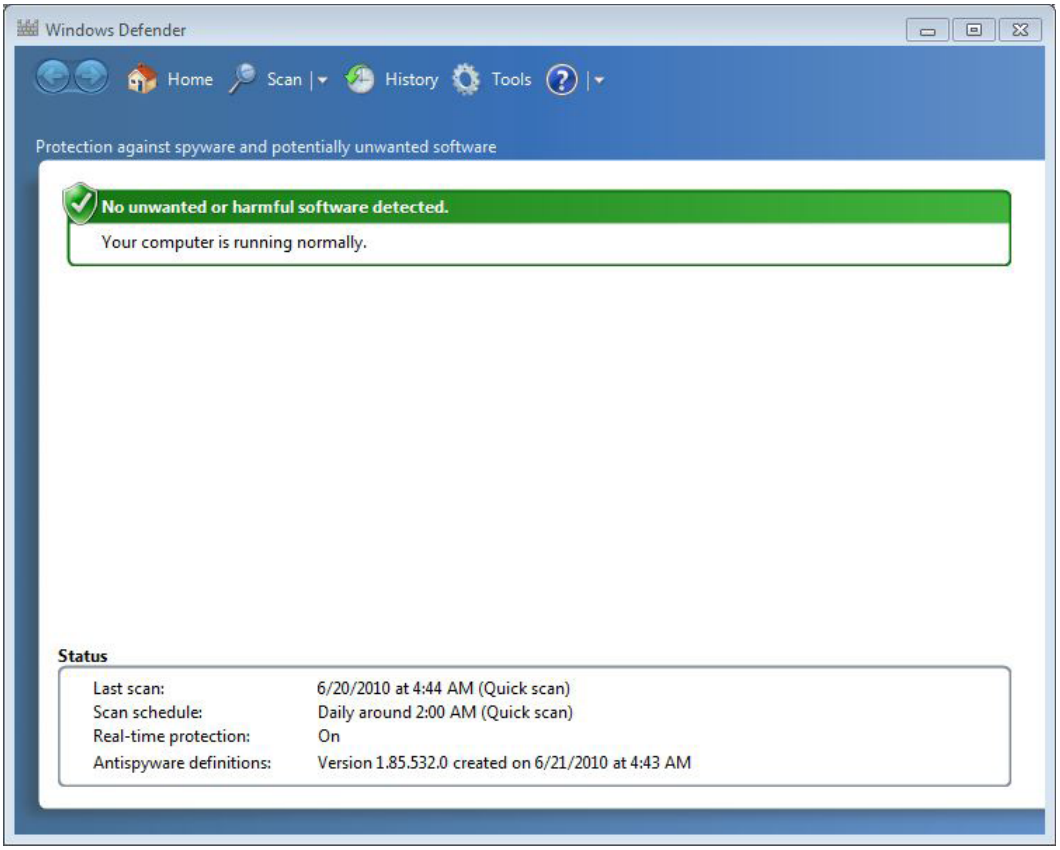
The **Windows Defender** tool in Windows 7 detects and removes spyware on a client system. By default, Windows Defender is configured to regularly download new spyware definitions through Windows Update and use these definitions to scan for spyware on the local system. In smaller networks, you do not necessarily need to change this default configuration. However, in large networks you may consider using Group Policy to disable some Windows Defender features.

Windows Defender is suitable for use in small networks or as a temporary solution before an advanced anti-malware solution is purchased. In large networks, you should use a centrally managed anti-malware solution such as **Microsoft Forefront Client Security**.

To view Windows Defender, open Control Panel, select View by Large Icons, and then scroll down to click Windows Defender.

By default, Windows Defender provides two types of protection:

- **Automatic scanning –** Windows Defender is configured by default to download new definitions and then perform a quick scan for spyware at 2 a.m. daily.
- **Real-time protection –** Windows Defender constantly monitors computer usage in areas such as the Startup folder, the Run keys in the registry, and Windows Add-ons. If an application attempts to make a change to one of these areas, Windows Defender prompts the user either to Permit (allow) or Deny (block) the change.



Protection against spyware and potentially unwanted software

No unwanted or harmful software detected.

Your computer is running normally.

Status

Last scan:	6/20/2010 at 4:44 AM (Quick scan)
Scan schedule:	Daily around 2:00 AM (Quick scan)
Real-time protection:	On
Antispyware definitions:	Version 1.85.532.0 created on 6/21/2010 at 4:43 AM

Figure 30: Windows Defender

In addition to providing this automatic functionality, Windows Defender can also perform a manual scan of the system. To start a manual scan from the Scan menu, select one of the following three scan types:

- **Quick Scan –** this scans for common infections by spyware or other potentially unwanted software, such as the memory and portions of the registry that link to startup applications. A quick scan is sufficient to detect most spyware.
- **Full Scan –** this scans every file on the computer, including common types of file archives and applications already loaded in the computer's memory. A full scan can take a long time to complete. You should only run a full scan if you suspect that a user's computer is infected with unwanted software after running the quick scan.
- **Custom Scan –** custom scans begin with a quick scan and then perform a detailed scan on specific areas of a system that you can choose.

Detected Spyware

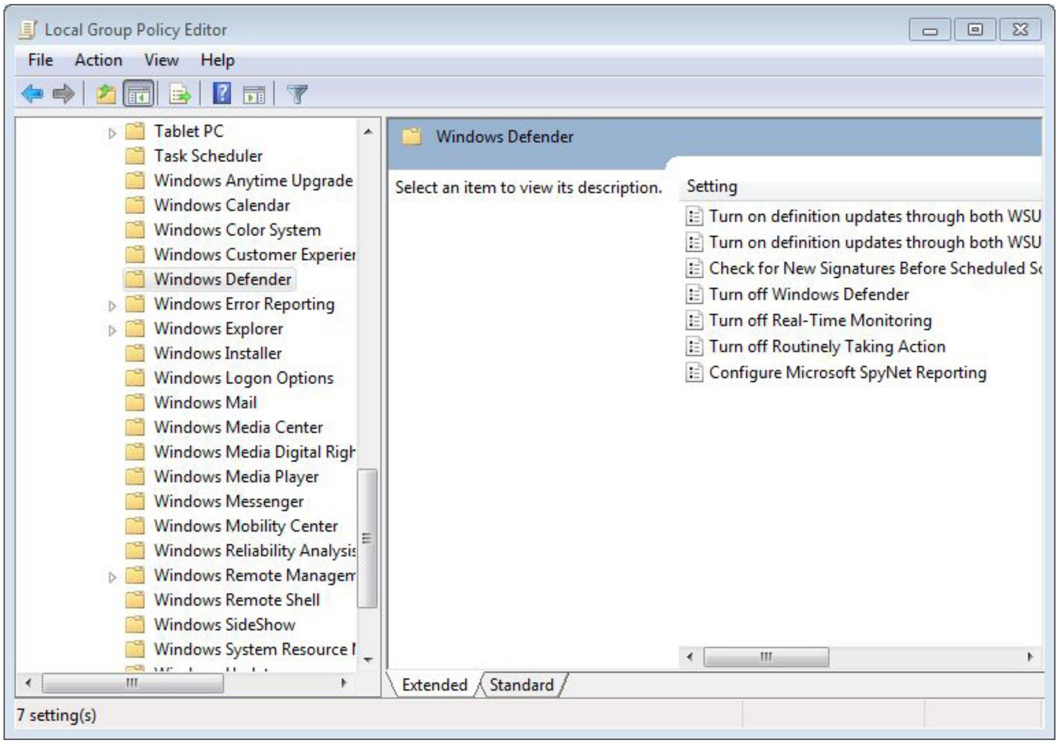
If Windows Defender finds spyware or unwanted software as a result of a scan, it displays a warning and provides you with four options for each item detected:

- Ignore
- Quarantine
- Remove
- Always Allow

Windows Defender Group Policy Settings

In an AD DS environment, use Group Policy to configure clients instead configuring each machine individually. To locate the Group Policy settings for Windows Defender, open a GPO and navigate to Computer Configuration → Policies → Administrative Templates → Windows Components → Windows Defender, as shown below.

The following sample provides the available policy settings for Windows Defender that you should be familiar with:



Windows Defender

Select an item to view its description.

Setting
- Turn on definition updates through both WSU
- Turn on definition updates through both WSU
- Check for New Signatures Before Scheduled S
- Turn off Windows Defender
- Turn off Real-Time Monitoring
- Turn off Routinely Taking Action
- Configure Microsoft SpyNet Reporting

7 setting(s)

Figure 31: Windows Defender in Group Policy

Windows Defender Best Practices

Best practices provide the highest level of security and cost efficiency:

- Do not use Windows Defender for large enterprises; use Forefront or another reputed security suite that can manage larger environments more efficiently.
- Use antivirus software with Windows Defender. Also, you can disable Windows Defender completely and use client-security software that provides anti-spyware and antivirus functionality.
- Test all applications with Windows Defender enabled to ensure that Windows Defender does not alert users to normal changes that the application might make before deploying Windows 7. If an application generates warnings, add the application to the Windows Defender Allowed list.
- By default, Windows Defender scans at 2 a.m., but you can change the scheduled scan time to meet business needs.
- Use WSUS to manage and distribute signature updates.

Using Bootable Antivirus CD

When a computer has become severely infected with malware, the computer might run so slowly that it's difficult to perform an anti-malware scan. In this case, the best practice is to perform an **offline scan from a bootable CD** if you have one available. You will avoid running the malware programs that consume resources and slow down the system by scanning outside of Windows.

In my opinion this would be a nice-to-have; again, we must consider the number of pages of content allotted for this domain. If you think this is crucial, then by all means insert these examples.

Identify and Resolve Software Update Issues

Windows 7 was designed to minimize security risks; however, online security risks are, of course, still prevalent. It is a high priority responsibility for administrators to regularly deploy updates to client systems and networks.

Using Update History for Verification

If a computer does not upload monthly updates, it becomes vulnerable. Use the following procedure to view update history:

1. Click Start\All Programs**Windows Update.**
2. On the Windows Update window, click View Update History.
3. Double-click the update to view.

Windows Server Update Services (WSUS)

WSUS is a version of the Microsoft Update service that you can host on your private network. WSUS connects to the Microsoft Update site, downloads information about available updates, and adds them to a list of updates that require administrative approval. WSUS enables administrators to approve updates before distributing them to computers on an intranet. You can distribute WSUS across multiple servers and locations. To deploy updates to computers running Windows 7, you must have **WSUS 3.0 SP2 or later** installed on your server. You can download WSUS service updates from Microsoft on the internet, and store them on a local network for retrieval, thus eliminating unnecessary internet downloading.

Windows Server Update Services:

- Connects to the **Microsoft Update** site, downloads Update information, and adds them to a list of updates after administrators approve them.
- Automatically makes updates available to any computer running **Windows Update** or Automatic Update.

The exam focuses on Windows 7; WSUS only runs on server versions of Windows. Therefore, understanding the following configuration process should provide adequate WSUS information to pass the exam.
This task teaches you how to install WSUS on a server, approve updates, and configure a Windows 7 client to retrieve updates.

Use the following procedure to install WSUS:

1. Log on an administrator to a computer running Windows Server 2008 R2.
2. Click Start\ Tools**Server Manager**.
3. In the Details pane, click Roles node\ Add Roles to display the **Add Roles Wizard**.
4. On the **Before You Begin** page, click **Next**.
5. On the **Select Server Roles** page, select the **Windows Server Update Services role**. Add any required role services when prompted.
6. Click **Next** four times, and **Install**.
7. When the **Windows Server Update Services Setup Wizard** appears, click **Next**.
8. When you add the WSUS server role, Windows Server 2008 R2 downloads the latest version directly from Microsoft. The most recent version of WSUS is WSUS version 3.0 with Service Pack 2
9. Accept the terms on the Licensing Agreement page, and click **Next**.
10. On the **Required Components to Use Administration UI page**, click **Next**.
11. On the **Select Update Source page**, you would normally de-select the Store Updates Locally check box to **Prevent the WSUS** server from copying updates locally. However, in a production environment, leave this check box selected so clients can download updates from the LAN instead of Microsoft. from your WSUS (across your local area network) instead of directly from Microsoft.
12. Click Next.
13. On the **Database Options page**, click **Next**.
14. If the Connecting to SQL Server Instance page appears, click **Next**.
15. On the **Web Site Selection page**, click Next to use the default IIS Web site, or create a new WSUS site if in a production environment.
16. On the Ready **To Install page**, click Next.
17. On the **Completing the WSUS Setup Wizard page**, click Finish.
18. On the **Installation Results page**, click Close. If prompted, restart the computer.

Use this process to configure WSUS and install updates after approved.

1. From **Administrative Tools**, click Windows Server Update Services. The Windows **Server Update Services Configuration Wizard** appears.
2. On the **Before You Begin page**, click **Next**.
3. On the **Join the Microsoft Update Improvement Program page**, click **Next**.
4. On the **Choose Upstream Server page**, click **Next**.
5. On the **Specify Proxy Server page**, click **Next**.
6. On the **Connect to Upstream Server page**, click Start Connecting. The WSUS Configuration Wizard downloads information from Microsoft Update. Click Next.
7. On the **Choose Products page** only Office and Windows updates are downloaded by default. Browse through the other update types that are available to familiarize yourself, then accept these default settings by clicking **Next**.
8. On the **Choose Classifications page**, select the All Classifications check box. Click Next.
9. On the **Set Sync Schedule page**, click **Next**.
10. On the **Finish page**, click **Next**.
11. On the **What's Next** page, make note of other WSUS configuration steps. Click Finish.

12. To configure **AD DS Group Policy** settings so that domain members synchronize with the WSUS server. On the computer running Windows Server 2008 R2, click **Start\Administrative Tools\Group Policy Management**.
13. In **the Group Policy Management console**, select the Group Policy Management\Forest\Domains\nwtraders.msft\Default Domain Policy node. Right-click Default Domain Policy, click Edit.
14. In the **Group Policy Management Editor**, select the Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update node. Double-click the Specify Intranet Microsoft Update Service Location setting. Click Enabled.
15. In the Set **The Intranet Update Service For Detecting updates box**, type **http://** and the name of your computer running Windows Server 2008 R2 (such as **http://DC 1**). Click OK.
16. In the **Group Policy Management Editor**, double-click the Configure Automatic Updates policy. Click Enabled. In the **Configure Automatic Updating** list, Select 3 – Auto Download and Notify for Install. Accept the default settings by clicking OK.
17. Double-click the **Turn on Recommended Updates via Automatic Updates policy**. Click Enabled. This enables Windows Update to install both recommended updates, which include driver updates, Windows features, and other updates. Click OK.
18. Open the **Windows Server Update Services** console from the Administrative Tools folder on the Start menu. If your server does not appear in the Update Services list In the Update Services console, click the Connect to Server link in the Actions pane, type the server name, and click Connect.
19. **Select the Update Services**\<*server_name*>\Computers\Synchronizations node. If synchronization is currently running, select it. Wait until the synchronization completes.
20. Select the Update Services\<*server_name*>\Updates\All Updates node. In the Approval, select Unapproved. In the Status list, select **Failed or Needed**. Then, click Refresh, and wait several minutes for the Update Services console to display the list of unapproved updates.
21. Right-click any updates that appear, and then click Approve. To select all updates, press Ctrl+A. If no updates appear, verify that your computer running Windows 7 appears when you select the Computers\All Computers node. If you still see no updates, verify that the WSUS server has downloaded available updates from Microsoft. If updates have been synchronized, you might need to wait until Windows Update on the client notifies the WSUS server of its current status.
22. In the **Approve Updates dialog box**, select the All Computers list and then click Approved for Install, and then click **OK**.
23. If prompted, accept the license terms.
24. In the **Approval Progress dialog box**, click Close.

Note: You must install WSUS on at least one server in your network. To deploy updates to computers running Windows 7, you must have WSUS 3.0 SP2 or later installed on the network server.

Practice Questions

Chapter 1

1. You are creating a GPO to deploy FireFox.msi to your Windows 7 clients. The MSI files are stored in a share named Apps on Server1. The permissions for the share provide read access to Everyone and Co-Owner to Domain Admins. You are working in the Computer Configuration section of the GPO and want to Publish the MSI file so that users can optionally install the application if they desire; however, the Publish option is disabled. How can you publish the MSI file instead of assigning it? Select the best answer.

○ A. Create the policy in the User Configuration section of the GPO

○ B. Recreate the MSI file with the publish flag enabled

○ C. Deploy an executable instead because MSI files do not support publishing

○ D. Right-click on the Software Settings node in the GPO and choose Enable Advanced Functions

2. You want to ensure that the Windows Gadget Platform is enabled for your Windows 7 clients. Though it is enabled by default, it was disabled during image creation. What Windows 7 tool can you use to install or remove the Windows Gadget Platform? Select the best answer.

○ A. The Programs and Features Control Panel

○ B. Windows Updates

○ C. Group Policies

○ D. Compatibility Administrator

3. You must configure a registry value on several hundred Windows 7 Enterprise desktops. You want to do this in the simplest way possible. The environment consists of a Windows Server 2008 R2 AD DS domain with seven domain controllers all running Windows Server 2008 R2 Enterprise Edition. You do not want to visit each machine, nor do you want to create batch file or script code. What is the best way to change the registry entry? Select the best answer.

○ A. Login script

○ B. Create a custom ADM file

○ C. Use Group Policy Preferences

○ D. Create a custom program that can make the change

4. You are using Windows Deployment Services from a Windows Server 2008 R2 server to deploy Windows 7. All Windows 7 desktops include PXE-compliant network adapters. All desktops can reach the WDS server on the network. You must reimage one of the desktops. How will you boot the computer to start the reimaging process? Select the best answer.

❍ A. Boot the computer from a Windows PE disc that can access the WDS server

❍ B. Boot the computer to Widnows 7 and then run reimage /wds:ip_address

❍ C. Boot the computer from the network using the NIC and start the reimaging process

❍ D. Boot the computer from a Windows PE USB flash drive that can access the WDS server

5. You have configured an HTTPS subscription for event forwarding; however, you receive errors that indicate the connection cannot be made. What should you verify to ensure that the HTTPS subscription can function properly? Select the best answer.

❍ A. Windows Firewall exception for port 443

❍ B. Windows Firewall exception for port 80

❍ C. Windows Firewall exception for port 21

❍ D. Windows Firewall exception for port 25

Chapter 2

1. You are supporting both mobile and stationary users running Windows 7 on laptops and desktops. Several of the machines are used by more than one user. Users often attempt to logon only to notice that the user name is incorrect. What group policy setting would require the users to enter their logon name and password each time and would not allow the logon name to be retained between logons? Select the best answer.

❍ A. Interactive logon: Do not require CTRL+ALT+DEL

❍ B. Interactive logon: Do not display last user name

❍ C. Interactive logon: Do not remember last user name

❍ D. Network logon: Do not display last user name

2. You support a Windows 7 network environment that includes an AD DS domain. 438 users connect to the domain from Windows 7 client machines. All clients run Windows 7 Enterprise Edition and the domain runs all Windows Server 2008 R2 servers. Most users are required to reset their passwords every 30 days. Three users have never been prompted to reset their passwords, and they have used their accounts for more than four months. Their passwords have not expired. What is the likely cause? Select the best answer.

❍ A. The Password expires property is disabled for their user accounts

❍ B. The three users are local administrators on their machines

❍ C. The three users are Domain Admins in the domain

❍ D. The Password never expires setting is enabled for their user accounts

3. A user is attempting to logon to a Windows Server 2008 domain with a Windows 7 Enterprise client. He receives the following error:Windows could not log you in. The trust relationship between this computer and the primary domain failed.What can you do to allow the machine to logon to the domain again? Select the best answer.

○ A. Remove the machine from the domain and then join the domain again

○ B. Logon as a Domain Admin, immediately logoff, and then logon as the user again

○ C. Remove the machine from the domain and then logon

○ D. At a command prompt, execute the command trcreate /domain

4. A user attempts to logon to a Windows 7 Enterprise desktop with a domain account. The machine has a trust relationship with the domain. When the user attempts to logon, she received the following error message:Your account has time restrictions that prevent you from logging on at this time. Please try again later.What must be modified to allow this user to logon? Select the best answer.

○ A. Modify the allows logon times for all domain users in a GPO

○ B. Modify the Logon Hours for this user in the domain user account

○ C. Modify the local machine's Allowed hours of operation setting in the Computer Properties dialog

○ D. Modify the Logon Hours for this user in the local machine user account

5. You support Windows 7 clients in a large Windows Server 2008 R2 domain with more than 2300 clients and 112 servers. Thirteen DNS servers are in use. You need to determine which DNS server is being used by default on a specific client. Which one of the following IPCONFIG commands is the appropriate command for viewing DNS configuration settings? Select the best answer.

○ A. IPCONFIG /FLUSHDNS

○ B. IPCONFIG

○ C. IPCONFIG /ALL

○ D. IPCONFIG /DISPLAYDNS

6. You are troubleshooting a name resolution problem. When a specific Windows 7 client attempts to access the server named Server13.AHG.local, the connection fails. You can PING the IP address of the server from the client and it works. You've verified that the DNS entry in the DNS server used by the client is correct. What else should you check? Select the best answer.

○ A. The hosts file on the client

○ B. The IPv6 settings on the client

○ C. The DNS server's resolution cache

○ D. The network routes

Chapter 3

1. You work as a Windows 7 Enterprise desktop administrator. You want to configure the system's Security log so that the maximum log size is 10240, but you want to automatically archive the Security log file when it is full rather than overwriting the file. What steps should you take in the Event Viewer in order to establish this configuration? Choose all that apply.

   ○ A. Check the Archive the log when full, do not overwrite events option on the General tab of the Security Log Properties dialog

   ○ B. Right-click on the Security log in the Event Viewer > Windows Logs section and select Properties

   ○ C. Click the Clear Log button in the Log Properties dialog

   ○ D. Set the Maximum log size (KB) value to 10240

2. You are troubleshooting a laptop computer that runs Windows 7 Enterprise Edition. The computer has a built-in wireless network adapter that has failed. The adapter is integrated and cannot be replaced. The laptop has four USB 2.0 ports, one ExpressCard port and an Ethernet adapter. The user needs a wireless connection and would like the device to work in her home computer as well. What hardware should the user acquire? Select the best answer.

   ○ A. A USB wireless adapter

   ○ B. An ExpressCard adapter

   ○ C. Add nothing; use the Ethernet port for wireless access

   ○ D. A firewire adapter

3. Which one of the following chkdsk commands will automatically attempt to repair discovered errors on a hard disk volume? Select the best answer.

   ○ A. chkdsk d: /f

   ○ B. chkdsk c: /b

   ○ C. chkdsk c: /i

   ○ D. chkdsk c: /v

4. You have several USB devices plugged into your Windows 7 system. When you add an additional USB device it is not installed correctly. If you first remove one of the other devices and then add the new device, it installs fine. What is the likely problem? Select the best answer.

   ○ A. The new device is a USB 1.1 device

   ○ B. The new device is a USB 3.0 device

   ○ C. The new device must always be externally powered

   ○ D. The USB bus is unable to power all the devices at the same time

Chapter 4

1. You must implement a wireless link for a Windows 7 user. The user runs Windows 7 Enterprise on a laptop computer. The user requires a data rate of 70 Mbps or greater. Which one of the following 802.11 technologies will meet the user's needs? Select the best answer.

○ A. 802.11a

○ B. 802.11b

○ C. 802.11g

○ D. 802.11n

2. You support laptop users running Windows 7 Enterprise. The users often connect to public hotspots to check their email messages while traveling. One user, Amy, has called complaining that her wireless connection is not working. She indicates that no wireless networks are displayed in the view available networks system tray tool; however, a coworker located in the same area can see three different networks. What is the likely problem? Select the best answer.

○ A. The wireless adapter is turned off on the laptop

○ B. Amy has a laptop with 802.11n, which is not compatible with older 802.11 networks

○ C. The DHCP client is not running on Amy's laptop

○ D. Amy's computer has less than 2 GB RAM

3. You are the desktop administrator for Windows 7 clients. You are assisting in a wireless network implementation project. You must select a security solution that will prevent eavesdropping on the wireless LAN. Which one of the following security solutions will accomplish your objective? Select the best answer.

○ A. Firewall

○ B. WPA2

○ C. Authentication

○ D. 802.11n

4. You must select a security solution for the Windows 7 laptops that connects to the wireless network. What is the primary difference between the Personal and Enterprise editions of WPA and WPA2? Select the best answer.

○ A. Personal uses EAP with an authentication server and Enterprise uses pre-shared keys

○ B. Personal uses 802.11b and Enterprise uses 802.11n

○ C. Personal uses pre-shared keys and Enterprise uses EAP with an authentication server

○ D. Personal uses 802.11b and Enterprise uses 802.11g

Chapter 5

1. You are the desktop administrator in your organization. Twenty desktop computers have been upgraded to Windows 7 Enterprise edition. The users are using the Internet Explorer 8.0 browser to access Internet websites. They are contacting you stating that certain components of websites are not working properly. On the Programs tab of the Internet Options dialog, what button should you click to ensure that all needed plug-ins are installed? Select the best answer.

   ○ A. Manage Add-ons

   ○ B. Manage Plug-ins

   ○ C. Set Programs

   ○ D. Settings

2. You are experiencing problems with a specific website in Internet Explorer 8.0. You suspect that the problem is related to a plug-in. Without the plug-in, the website should work but some graphics elements will not be displayed. What can you do to access the site without the plug-in without uninstalling the plug-in? Select the best answer.

   ○ A. Right-click the plug-in in the Manage Add-ons dialog and select More Information and then click Remove

   ○ B. Uninstall and reinstall Internet Explorer 8.0

   ○ C. Use the Manage Add-ons dialog to temporarily disable the plug-in

   ○ D. Visit the plug-in vendor's website and reinstall the plug-in

3. You are working with Internet Explorer 8.0 on Windows 7 Enterprise desktops. Several Internet Explorer features seem to be disabled. You want to determine if a Group Policy is causing the features to be disabled. What MMC snap-in can be used to determine if Group Policies are impacting the Internet Explorer configuration? Select the best answer.

   ○ A. TPM Management

   ○ B. Security Templates

   ○ C. Event Viewer

   ○ D. Resultant Set of Policy

4. What application, included with Windows 7, must be periodically updated to detect and prevent the most recent malware from penetrating your machine? Select the best answer.

   ○ A. BitLocker

   ○ B. Microsoft Security Essentials

   ○ C. Avast Anti-virus

   ○ D. Windows Defender

5. Which of the following actions will require BitLocker recovery should they occur? Choose all that apply.

○ A. Adding a second hard drive

○ B. An attacker modifies the computer

○ C. Turning off the TPM

○ D. Forgetting the PIN

6. When you wish to implement BitLocker encryption for the internal hard drive on a system that does not include a TPM 1.2 module, what must the system BIOS support? Select the best answer.

○ A. Hot-swappable memory

○ B. Intel-VT

○ C. Reading from a USB flash device before OS load

○ D. Memory diagnostics

Answers & Explanations

Chapter 1

1. Answer: A

Explanation A. Correct. You can only Publish software to users and not to computers. If a user selects to install the software, it will only be available for that user's profile on the machine.

Explanation B. Incorrect. No such option exists in MSI files.

Explanation C. Incorrect. MSI files do support publishing, but only in the User Configuration section of the GPOs.

Explanation D. Incorrect. No such menu option exists. You must create published packages in the User Configuration section of the GPO.

2. Answer: A

Explanation A. Correct. The Programs and Features applet can be used to add or remove features. The Windows Gadget Platform is a feature.

Explanation B. Incorrect. Windows Updates is not required. Programs and Features allow you to add features and the Windows Gadget Platform is a feature.

Explanation C. Incorrect. You can disable the Programs and Features Control Panel to prevent users from working with this, but you must use Programs and features to enable it.

Explanation D. Incorrect. The Compatibility Administrator is used to create shim databases.

3. Answer: C

Explanation A. Incorrect. The login script would require batch file or script code.

Explanation B. Incorrect. In a Windows Server 2008 R2 domain it is better to use Preferences than to create a custom ADM file.

Explanation C. Correct. The Registry Group Policy Preference can be used to configure registry values in HKEY_CURRENT_USER, HKEY_CLASSES_ROOT, HKEY_LOCAL_MACHINE, HKEY_CURRENT_CONFIG, or HKEY_USERS.

Explanation D. Incorrect. This solution does not meet the requirement of least effort.

4. Answer: C

Explanation A. Incorrect. The WDS server can be located automatically with the PXE NIC adapter.

Explanation B. Incorrect. No such command exists.

Explanation C. Correct. PXE-compliant computers can automatically locate the WDS server and begin the imaging process.

Explanation D. Incorrect. The WDS server can be located automatically with the PXE NIC adapter.

5. Answer: A

Explanation A. Correct. HTTPS required port 443 to allow for communications.

Explanation B. Incorrect. Port 80 is used for HTTP; port 443 is used for HTTPS.

Explanation C. Incorrect. Port 21 is used for FTP; port 443 is used for HTTPS.

Explanation D. Incorrect. Port 25 is used for SMTP; port 443 is used for HTTPS.

Chapter 2

1. Answer: B

Explanation A. Incorrect. This policy will show the logon fields automatically, but it will still allow for the retaining of the last logon name.

Explanation B. Correct. When this policy is enabled, the last user name is not displayed. Users will be required to enter the user name and the password at each logon.

Explanation C. Incorrect. The proper policy name is Interactive logon: Do not display last user name.

Explanation D. Incorrect. The proper policy name is Interactive logon: Do not display last user name.

2. Answer: D

Explanation A. Incorrect. The property that impacts this behavior is the Password never expires property, and it is likely enabled for these three users.

Explanation B. Incorrect. Even local administrators are required to reset their domain passwords by default.

Explanation C. Incorrect. Even Domain Admins are required to reset their passwords by default.

Explanation D. Correct. When the Password never expires checkbox is checked for the user account, the user will not be prompted to reset the password and the password will never expire.

3. Answer: A

Explanation A. Correct. This process will recreate the trust relationship between the machine and the domain and regenerate the machine or computer account in the domain.

Explanation B. Incorrect. The Domain Admin logon will fail too if the trust relationship is broken.

Explanation C. Incorrect. This will allow you to logon to the local machine, but it will not enable you to logon to the domain again.

Explanation D. Incorrect. No such command exists.

4. Answer: B

Explanation A. Incorrect. You should modify the Logon Hours for this user not for all users.

Explanation B. Correct. The domain user account imposes these logon hour limits and it must be modified to allow the user to logon.

Explanation C. Incorrect. No such setting exists in the Computer Properties dialog.

Explanation D. Incorrect. Because the user is logging on with a domain account, all changes should be made to the domain account.

5. Answer: C

Explanation A. Incorrect. This command will empty the DNS cache. It will not display the default DNS server.

Explanation B. Incorrect. This command will only show the IP address, subnet mask, and default gateway. It will not show the DNS configuration.

Explanation C. Correct. This command will display the DNS configuration as well as the basic IP configuration.

Explanation D. Incorrect. This command will display the DNS cache. It will not show the DNS server used by default.

6. Answer: A

Explanation A. Correct. Because the hosts file is used before the DNS server, it can override settings in the server.

Explanation B. Incorrect. The IPv6 settings will have no impact on this name resolution scenario.

Explanation C. Incorrect. The DNS server will resolve from its local database when the entry is in that database.

Explanation D. Incorrect. The DNS server can be reached as demonstrated by the PING command.

Chapter 3

1. Answers: A, B, D

Explanation A. Correct. This option will ensure that the log is backed up whenever it reaches the Maximum log size (KB) setting. The archive is stored in the same directory as the active log.

Explanation B. Correct. This action will open the Security Log Properties dialog for modification.

Explanation C. Incorrect. This will empty the active log and is not required to meet the scenario's demands.

Explanation D. Correct. The Security log defaults to a size of 20480 in Windows 7. You will have to change this value to meet the demands of the scenario.

2. Answer: A

Explanation A. Correct. A USB adapter will work in the laptop and the home computer.

Explanation B. Incorrect. The ExpressCard adapter would not work with most home computers without adding a PCI ExpressCard reader to the machine.

Explanation C. Incorrect. Ethernet is a wired medium and will not provide direct wireless access.

Explanation D. Incorrect. Firewire wireless network adapters do not exist.

3. Answer: A

Explanation A. Correct. The /f switch indicates that errors on the disk should be fixed.

Explanation B. Incorrect. The /b switch is used to re-evaluate clusters previously marked as bad.

Explanation C. Incorrect. The /I switch indicates that a less vigorous check should be made of index entries.

Explanation D. Incorrect. The /v switch indicates that a verbose listing of file names should be output during processing.

4. Answer: D

Explanation A. Incorrect. USB 1.1 devices can coexist with USB 2.0 devices.

Explanation B. Incorrect. Windows 7 does not support the incomplete USB 3.0 specification at this time.

Explanation C. Incorrect. If the device always required external power, it wouldn't work when another device is removed.

Explanation D. Correct. You may have to attach an externally powered USB hub if you want to continue using all of the USB devices at the same time.

Chapter 4

1. Answer: D

Explanation A. Incorrect. The 802.11a amendment provided up to 54 Mbps data rates.

Explanation B. Incorrect. The 802.11b amendment provided up to 11 Mbps data rates.

Explanation C. Incorrect. The 802.11g amendment provided up to 54 Mbps data rates.

Explanation D. Correct. The 802.11n amendment provides for data rates up to 600 Mbps and is the only standard amendment that provides data rates above 54 Mbps at the time of Windows 7's release.

2. Answer: A

Explanation A. Correct. It is not uncommon for laptops to allow users to turn off the wireless adapter to save battery power and for use on airplanes. Ensure that the adapter is turned on.

Explanation B. Incorrect. 802.11n devices can connect to 802.11 a/b/g networks just fine.

Explanation C. Incorrect. The DHCP client only plays a role once the computer is connected to a network.

Explanation D. Incorrect. A computer with the minimum requirements for Windows 7 should display available wireless networks if the adapter is on.

3. Answer: B

Explanation A. Incorrect. A firewall is used to provide security at the ingress (entrance) and egress (exit) to your network. It will not help prevent wireless eavesdropping.

Explanation B. Correct. WPA2 will encrypt the wireless communication to prevent eavesdropping.

Explanation C. Incorrect. Authentication alone will not prevent eavesdropping. You must implement an encryption solution as well.

Explanation D. Incorrect. 802.11n does not automatically prevent eavesdropping, though it does support the 802.11i amendment which can indeed prevent eavesdropping.

4. Answer: C

Explanation A. Incorrect. The opposite is true. Personal uses pre-shared keys.

Explanation B. Incorrect. Personal and Enterprise can be used on 802.11b through 802.11n.

Explanation C. Correct. The Enterprise edition provides for central management of authentication credentials and processes with a RADIUS server.

Explanation D. Incorrect. Personal and Enterprise can be used on 802.11b through 802.11n.

Chapter 5

1. Answer: A

Explanation A. Correct. The Manage Add-ons button will allow you to manage plug-ins (extensions) as well as toolbars and search providers.

Explanation B. Incorrect. No such button exists on the Programs tab.

Explanation C. Incorrect. The Set Programs button allows you to determine what programs should be used to open different file types or to perform functions like sending email.

Explanation D. Incorrect. No such button exists on the Programs tab.

2. Answer: C

Explanation A. Incorrect. This will uninstall the plug-in. You should right-click and select Disable instead.

Explanation B. Incorrect. This action is unnecessary and unavailable. You can simply disable the plug-in.

Explanation C. Correct. If you right-click on an add-on (plug-in), you can select Disable. The add-on is not uninstalled, but it will be disabled until you choose to enable it again.

Explanation D. Incorrect. This will not result in a disabled plug-in.

3. Answer: D

Explanation A. Incorrect. The Trusted Platform Module (TPM) Management snap-in allows you to configure and manage the TPM security hardware.

Explanation B. Incorrect. The Security Templates snap-in provides editing capabilities for security template files.

Explanation C. Incorrect. The Event Viewer snap-in is used to view log files.

Explanation D. Correct. The RSOP snap-in is used to generate policy data and view the policies applied to the local computer.

4. Answer: D

Explanation A. Incorrect. BitLocker is used to enable volume level encryption.

Explanation B. Incorrect. MSE is an additional download available from Microsoft.

Explanation C. Incorrect. Avast is a third-party software provider.

Explanation D. Correct. Windows Defender is built-into Windows 7 and is an anti-spyware solution.

5. Answers: B, C, D

Explanation A. Incorrect. You can add a second hard drive without using BitLocker on that drive. No recovery will be required.

Explanation B. Correct. This is applicable for a computer with a Trusted Platform Module (TPM) because the TPM checks the integrity of boot components during startup.

Explanation C. Correct. If you turn off the TPM in the BIOS, the key will not be available to unlock the drive.

Explanation D. Correct. If PIN authentication is enabled and you lose or forget the PIN, BitLocker recovery will be initiated.

6. Answer: C

Explanation A. Incorrect. No requirement of hot-swappable hardware exists.

Explanation B. Incorrect. Intel-VT is hardware assisted virtualization and is not required for BitLocker.

Explanation C. Correct. The BIOS must be able to read the encryption keys from a USB flash drive before loading the operating system.

Explanation D. Incorrect. BitLocker has no BIOS requirement for memory diagnostics.