Module 7

Maintenance and Security

Objectives

1. 1.7 Perform preventive maintenance procedures
2. 1.8 Basic OS security settings

PREVENTIVE MAINTENANCE

Safe Mode

1. A diagnostic mode of a Windows OS
2. Reduced functionality
3. Disables many non-core components
4. Intended to fix most, if not all problems within an operating system
5. Used to remove rogue security software
6. An installation that will only boot into its safe mode typically has a major problem
7. Accessed through `msconfig` or F8 at startup

Task Manager

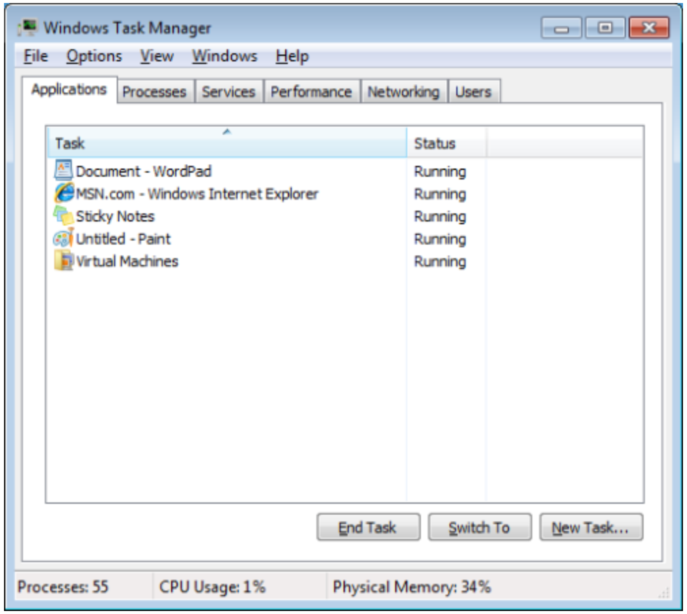
1. Ways to access:
   A. Right-click the Taskbar and select Task Manager
   B. [Ctrl]+[Shift]+[Esc]
   C. Click the Start button and type `taskmgr` in the Start Search box, and press [Enter].
   D. [Ctrl]+[Alt]+[Delete] and can click Start Task Manager.

For more information about the Task Manager

Task Manager

Applications tab

1. Operates exactly the same as it did in XP and Vista
2. Allows you to determine the status of a task as well as end, switch, or create a new task


Windows Task Manager
File Options View Windows Help
Applications Processes Services Performance Networking Users

Task	Status
Document - WordPad	Running
MSN.com - Windows Internet Explorer	Running
Sticky Notes	Running
Untitled - Paint	Running
Virtual Machines	Running

End Task
Switch To
New Task...

Processes: 55 CPU Usage: 1% Physical Memory: 34%

Task Manager

Processes tab

1. Provides detailed process information
2. More information available, just pull down the View menu and choose the Select Columns command:
   A. The Image Path Name setting shows the full path to the file behind the running process
   B. The Command Line setting shows the full command line, including the parameters or switches used to launch the process
3. Other useful information about a particular process can be viewed by right-clicking on a process and selecting the Open File Location or Properties commands

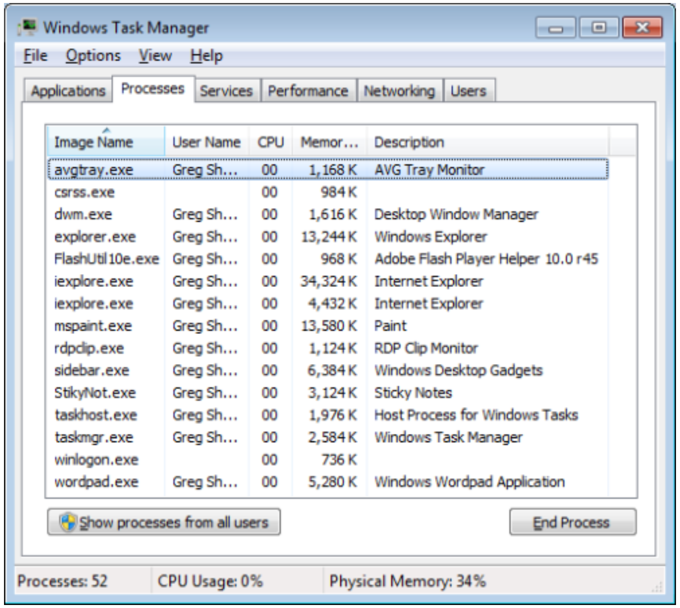


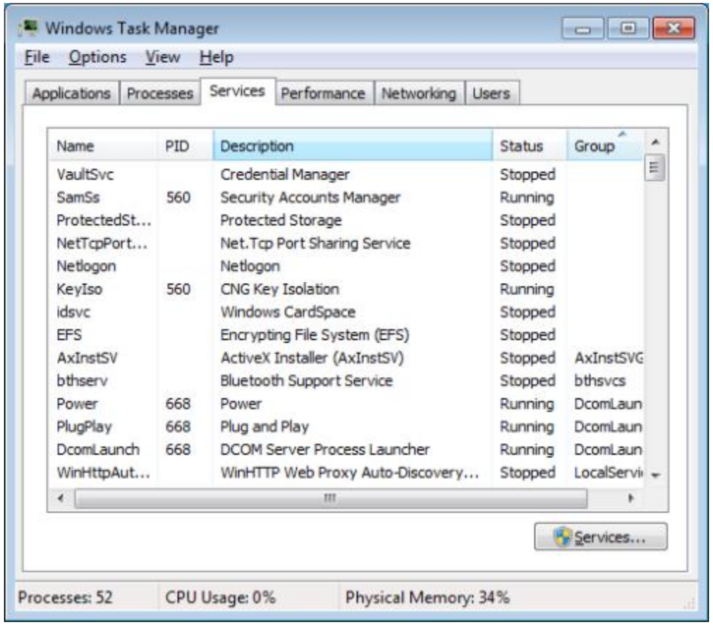
Image Name	User Name	CPU	Memor...	Description
avgtray.exe	Greg Sh...	00	1,168 K	AVG Tray Monitor
csrss.exe		00	984 K	
dwm.exe	Greg Sh...	00	1,616 K	Desktop Window Manager
explorer.exe	Greg Sh...	00	13,244 K	Windows Explorer
FlashUtil10e.exe	Greg Sh...	00	968 K	Adobe Flash Player Helper 10.0 r45
iexplore.exe	Greg Sh...	00	34,324 K	Internet Explorer
iexplore.exe	Greg Sh...	00	4,432 K	Internet Explorer
mspaint.exe	Greg Sh...	00	13,580 K	Paint
rdpclip.exe	Greg Sh...	00	1,124 K	RDP Clip Monitor
sidebar.exe	Greg Sh...	00	6,384 K	Windows Desktop Gadgets
StikyNot.exe	Greg Sh...	00	3,124 K	Sticky Notes
taskhost.exe	Greg Sh...	00	1,976 K	Host Process for Windows Tasks
taskmgr.exe	Greg Sh...	00	2,584 K	Windows Task Manager
winlogon.exe		00	736 K	
wordpad.exe	Greg Sh...	00	5,280 K	Windows Wordpad Application

Processes: 52 CPU Usage: 0% Physical Memory: 34%

Task Manager

Services tab

1. View the services that are running or available
2. If you want to investigate whether a running service is tied to a particular process, you can right-click on the service name and select the Go to Process command
3. If you need more control, click the Services button to launch the Services mmc


Windows Task Manager
File Options View Help
Applications Processes Services Performance Networking Users
Services...

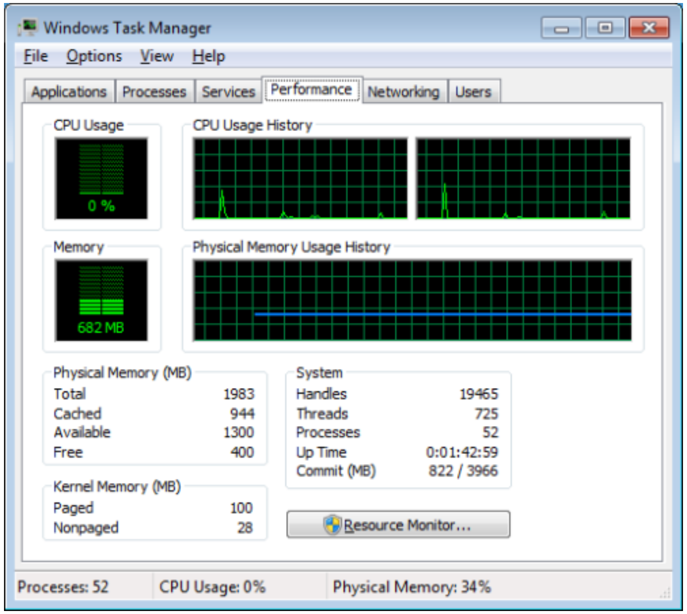
Name	PID	Description	Status	Group
VaultSvc		Credential Manager	Stopped	
SamSs	560	Security Accounts Manager	Running	
ProtectedSt...		Protected Storage	Stopped	
NetTcpPort...		Net.Tcp Port Sharing Service	Stopped	
Netlogon		Netlogon	Stopped	
KeyIso	560	CNG Key Isolation	Running	
idsvc		Windows CardSpace	Stopped	
EFS		Encrypting File System (EFS)	Stopped	
AxInstSV		ActiveX Installer (AxInstSV)	Stopped	AxInstSVG
bthserv		Bluetooth Support Service	Stopped	bthsvcs
Power	668	Power	Running	DcomLaun
PlugPlay	668	Plug and Play	Running	DcomLaun
DcomLaunch	668	DCOM Server Process Launcher	Running	DcomLaun
WinHttpAut...		WinHTTP Web Proxy Auto-Discovery...	Stopped	LocalServi

Processes: 52 CPU Usage: 0% Physical Memory: 34%

Task Manager

Performance tab

1. Shows the performance of the CPU and RAM
2. In the Physical Memory section:
   A. The Total entry shows the amount of RAM installed in the system
   B. The Cached entry shows the amount of physical memory used for system resources
   C. The Available entry shows the amount of physical memory not being used
3. In the Kernel Memory section:
   A. The Paged and Nonpaged entries show you how much of it is coming from virtual memory and how much is coming from physical memory



Physical Memory (MB)

Total	1983
Cached	944
Available	1300
Free	400

Kernel Memory (MB)

Paged	100
Nonpaged	28

System

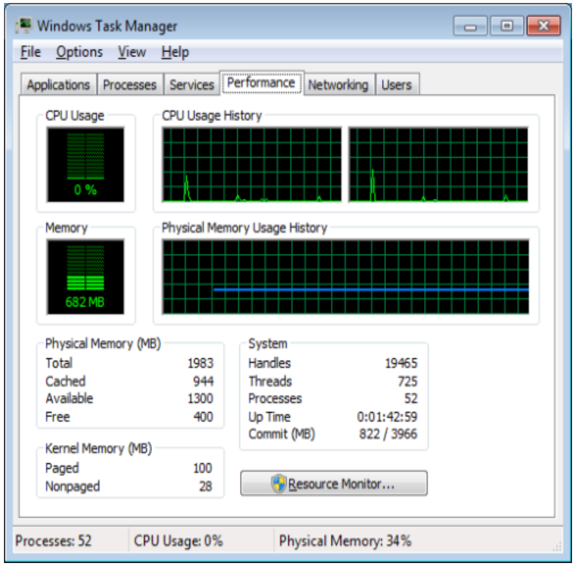
Handles	19465
Threads	725
Processes	52
Up Time	0:01:42:59
Commit (MB)	822 / 3966

Processes: 52 CPU Usage: 0% Physical Memory: 34%

Task Manager

Performance tab

4. In the System section:
   A. The Handles entry shows the number of object identifiers that are currently in use by all running processes
   B. The Threads entry refers to the number of sub-processes running inside of larger processes
   C. The Processes entry shows the number of currently running processes
   D. The Up Time entry shows the amount of time that has passed since the computer has been restarted
   E. The Commit entry shows Page File usage



Physical Memory (MB)	
Total	1983
Cached	944
Available	1300
Free	400

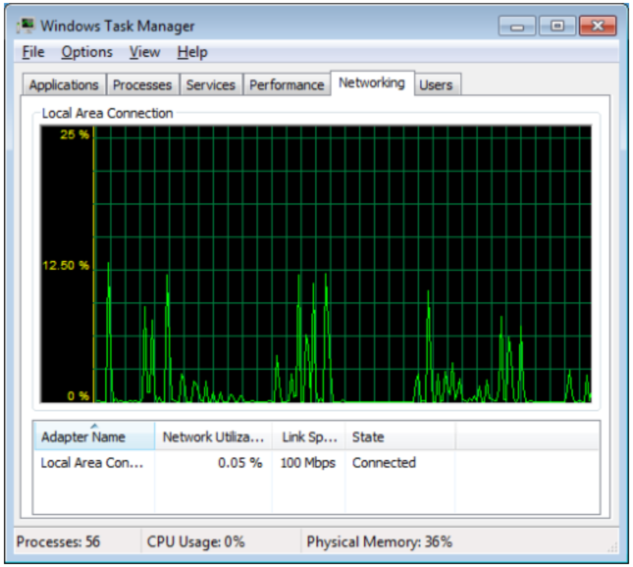
Kernel Memory (MB)	
Paged	100
Nonpaged	28

System	
Handles	19465
Threads	725
Processes	52
Up Time	0:01:42:59
Commit (MB)	822 / 3966

Processes: 52 CPU Usage: 0% Physical Memory: 34%

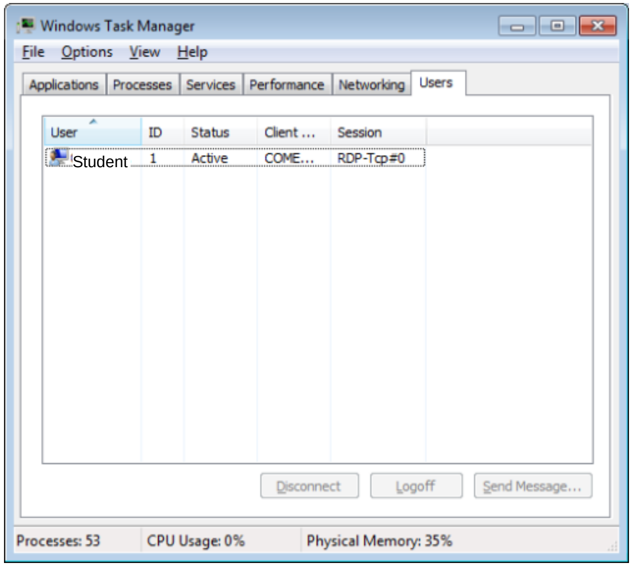
Task Manager

1. The **Networking tab** shows the network status and usage
2. The **Users tab** shows who is logged on to the system



Adapter Name	Network Utiliza...	Link Sp...	State
Local Area Con...	0.05 %	100 Mbps	Connected

Processes: 56 CPU Usage: 0% Physical Memory: 36%

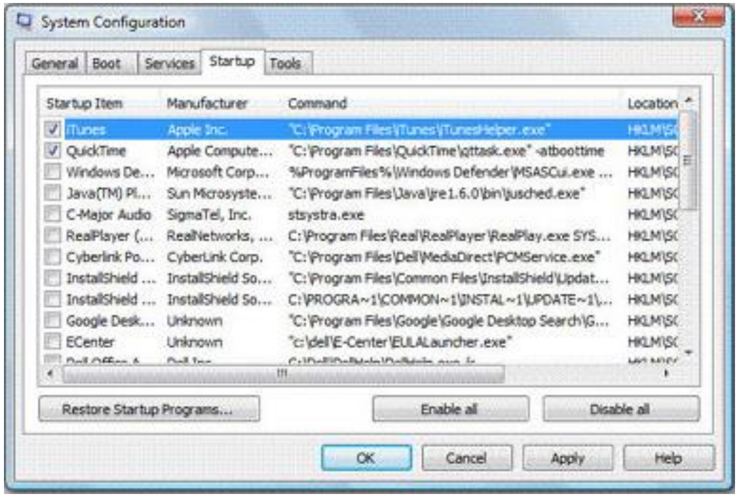


User	ID	Status	Client ...	Session
Student	1	Active	COME...	RDP-Tcp#0

Processes: 53 CPU Usage: 0% Physical Memory: 35%

System Configuration Tool

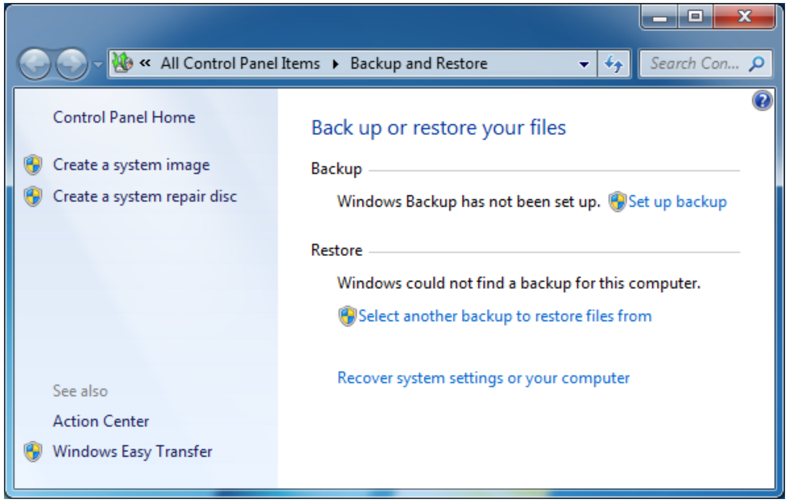
1. **`msconfig`**
2. Can help identify problems that might prevent Windows from starting correctly
3. Tabs include:
   - A. General
   - B. Boot
   - C. Services
   - D. Startup
   - E. Tools



	Startup Item	Manufacturer	Command	Location
☑	iTunes	Apple Inc.	"C:\Program Files\iTunes\iTunesHelper.exe"	HKLM\SO
☑	QuickTime	Apple Compute...	"C:\Program Files\QuickTime\qttask.exe" -atboottime	HKLM\SO
□	Windows De...	Microsoft Corp...	%ProgramFiles%\Windows Defender\MSASCui.exe ...	HKLM\SO
□	Java(TM) Pl...	Sun Microsyste...	"C:\Program Files\Java\jre1.6.0\bin\jusched.exe"	HKLM\SO
□	C-Major Audio	SigmaTel, Inc.	stsystra.exe	HKLM\SO
□	RealPlayer (...	RealNetworks, ...	C:\Program Files\Real\RealPlayer\RealPlay.exe SYS...	HKLM\SO
□	Cyberlink Po...	CyberLink Corp.	"C:\Program Files\Dell\MediaDirect\PCMService.exe"	HKLM\SO
□	InstallShield ...	InstallShield So...	"C:\Program Files\Common Files\InstallShield\Updat...	HKLM\SO
□	InstallShield ...	InstallShield So...	C:\PROGRA~1\COMMON~1\INSTAL~1\UPDATE~1\...	HKLM\SO
□	Google Desk...	Unknown	"C:\Program Files\Google\Google Desktop Search\G...	HKLM\SO
□	ECenter	Unknown	"c:\dell\E-Center\EULALauncher.exe"	HKLM\SO

Scheduling Backups

1. Found under Control Panel, System and Maintenance, Backup and Restore
2. You can:
   A. Click backup or restore and then follow the wizard
   B. Create a system image
   C. Create a system repair disc
3. Recommendations:
   A. Don't back up your files to the same hard disk that Windows is installed on
   B. Always store backup media in a secure and fireproof place offsite
   C. Create a regular schedule



Back up or restore your files

Backup

Windows Backup has not been set up. Set up backup

Restore

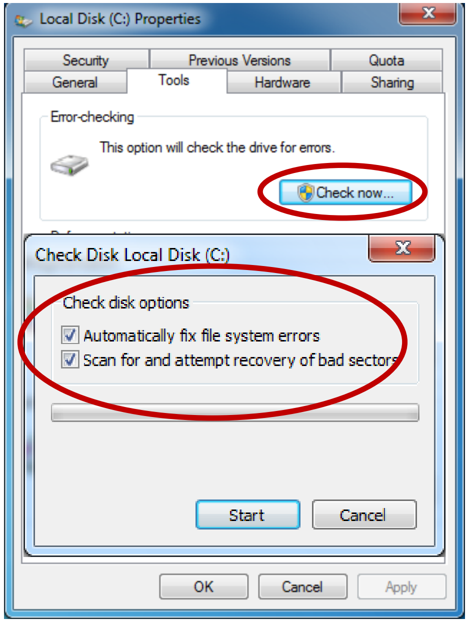
Windows could not find a backup for this computer.

Select another backup to restore files from

Recover system settings or your computer

Scheduling Check Disks

1. Can help solve some computer problems and improve the performance of your computer by making sure that your hard disk has no errors
2. Open Computer > right-click the hard disk drive that you want to check > Properties > Tools tab > under Error-checking click Check Now
3. To automatically repair problems with files and folders that the scan detects, select Automatically fix file system errors
4. To perform a thorough disk check, select both Automatically fix file system errors and Scan for and attempt recovery of bad sectors


Local Disk (C:) Properties

Error-checking

This option will check the drive for errors.

Check Disk Local Disk (C:)

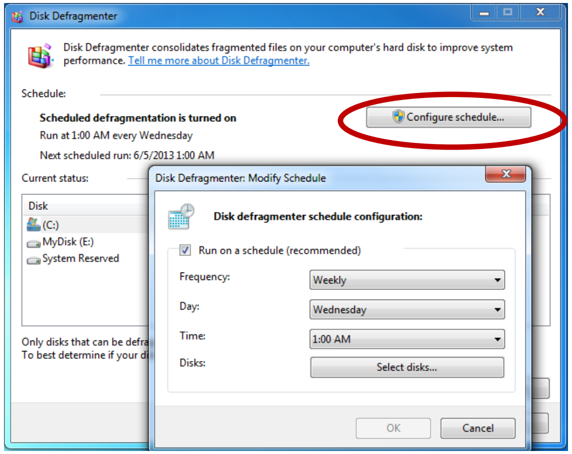
Check disk options

☑ Automatically fix file system errors

☑ Scan for and attempt recovery of bad sectors

Scheduling Disk Defragmenter

1. Rearranges fragmented data on a volume so it will work more efficiently
2. Scheduling makes it run at regular intervals when your computer is turned on
3. It is scheduled to run once a week by default
4. Can be changed
5. Open Computer > right-click the hard disk drive that you want to check > click Properties > Tools tab > under Defragmentation, click Defragment Now
6. Can't be scheduled for solid-state drives (SSD), as well as some types of virtual hard disks (VHD)
7. You can defragment manually



Disk Defragmenter

Disk Defragmenter consolidates fragmented files on your computer's hard disk to improve system performance. Tell me more about Disk Defragmenter.

Schedule:

Scheduled defragmentation is turned on

Run at 1:00 AM every Wednesday

Next scheduled run: 6/5/2013 1:00 AM

Current status:

Only disks that can be defra

To best determine if your di

Disk Defragmenter: Modify Schedule

Disk defragmenter schedule configuration:

☑ Run on a schedule (recommended)

Frequency: Weekly

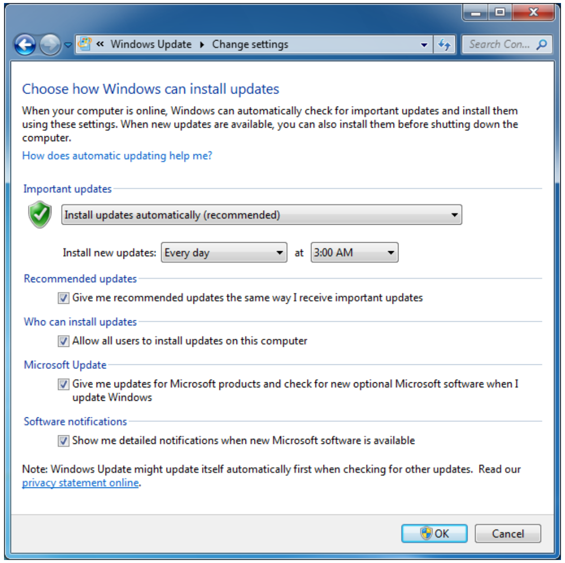
Day: Wednesday

Time: 1:00 AM

Disks:

Windows Updates

1. Helps keep your PC safer and your software current
2. Automatic updating
   - A. Important updates provide significant benefits, such as improved security and reliability
   - B. Recommended updates address noncritical problems
3. Optional updates are installed manually
4. Open Windows Update by clicking the Start button > All Programs > Windows Updates
   - A. To change what gets updated click Change settings in the left pane > choose the option that you want
   - B. Under Recommended updates, select the Give me recommended updates the same way I receive important updates check box



Choose how Windows can install updates

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

How does automatic updating help me?

Important updates

Install updates automatically (recommended)

Install new updates: Every day at 3:00 AM

Recommended updates

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

Who can install updates

☑ Allow all users to install updates on this computer

Microsoft Update

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

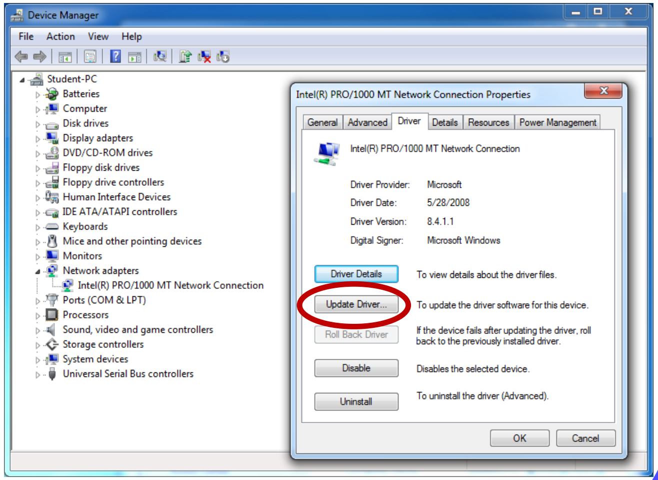
Software notifications

☑ Show me detailed notifications when new Microsoft software is available

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

Driver Updates

1. A driver is software that allows your computer to communicate with hardware devices
2. Windows can automatically check if there are drivers available for new devices that you connect to your computer
3. For older hardware, updated drivers might become available but aren't installed automatically
4. To install these optional updates, go to Windows Update > check for updates > then view and install driver updates that are available
5. You can manually install drivers



- Student-PC
  - Batteries
  - Computer
  - Disk drives
  - Display adapters
  - DVD/CD-ROM drives
  - Floppy disk drives
  - Floppy drive controllers
  - Human Interface Devices
  - IDE ATA/ATAPI controllers
  - Keyboards
  - Mice and other pointing devices
  - Monitors
  - Network adapters
    - Intel(R) PRO/1000 MT Network Connection
  - Ports (COM & LPT)
  - Processors
  - Sound, video and game controllers
  - Storage controllers
  - System devices
  - Universal Serial Bus controllers

Intel(R) PRO/1000 MT Network Connection

Driver Provider: Microsoft

Driver Date: 5/28/2008

Driver Version: 8.4.1.1

Digital Signer: Microsoft Windows

Driver Details: To view details about the driver files.

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

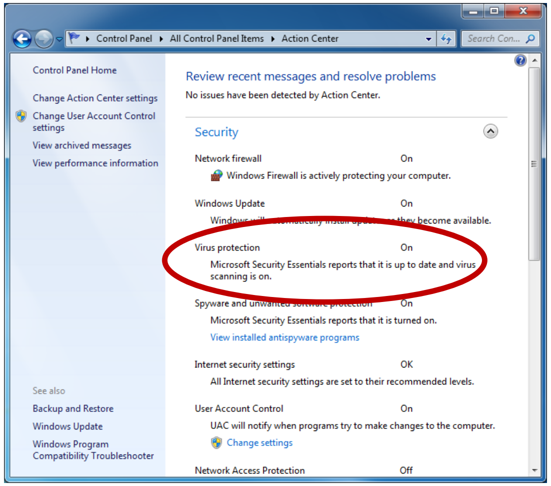
Roll Back Driver: If the device fails after updating the driver, roll back to the previously installed driver.

Disable: Disables the selected device.

Uninstall: To uninstall the driver (Advanced).

Antivirus Updates

1. Must be updated regularly to stay effective against new viruses
2. Most is designed to update automatically, but you can update your software manually
3. Windows does not come with antivirus software, but can often detect and monitor antivirus software installed
4. Status is displayed in Action Center
5. Open Action Center by clicking the Start button > Control Panel > Action Center > in the Security section look for Virus Protection


Control Panel ▸ All Control Panel Items ▸ Action Center
Search Con...
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

No issues have been detected by Action Center.

Security

Network firewall On

Windows Firewall is actively protecting your computer.

Windows Update On

Windows will automatically install updates as they become available.

Virus protection On

Microsoft Security Essentials reports that it is up to date and virus scanning is on.

Spyware and unwanted software protection On

Microsoft Security Essentials reports that it is turned on.

View installed antispyware programs

Internet security settings OK

All Internet security settings are set to their recommended levels.

User Account Control On

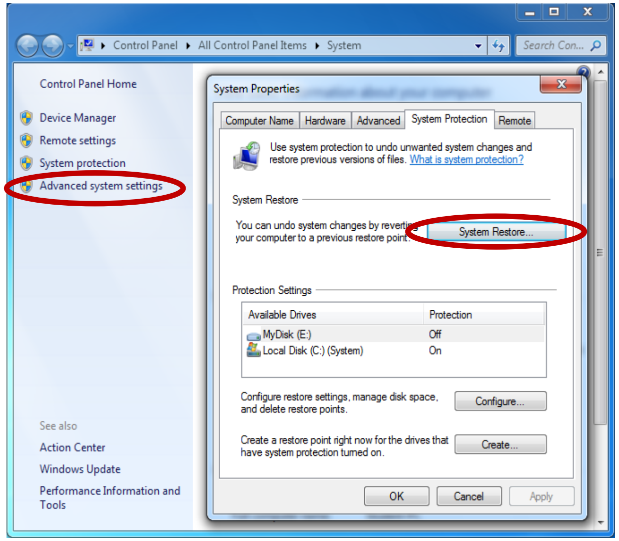
UAC will notify when programs try to make changes to the computer.

Change settings

Network Access Protection Off

System Restore

1. Can return your PC's system files and programs to a time when everything was working fine
2. It won't affect your documents, pictures, or other data
3. Open System Restore by clicking the Start button > Control Panel > System > click Advanced system settings on the left > System Protection tab > System Restore
4. Before you start System Restore, save any open files and close all programs



Use system protection to undo unwanted system changes and restore previous versions of files. What is system protection?

System Restore

You can undo system changes by reverti your computer to a previous restore point.

Protection Settings

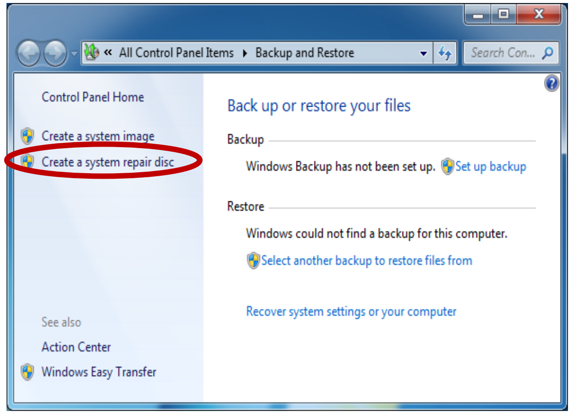
Available Drives	Protection
MyDisk (E:)	Off
Local Disk (C:) (System)	On

Configure restore settings, manage disk space, and delete restore points.

Create a restore point right now for the drives that have system protection turned on.

Automated System Recovery (ASR)

1. Create an ASR disk as part of an overall plan for system recovery in case of system failure
2. Use as a last resort in system recovery
3. You can access the Automated System Recovery Preparation Wizard from Backup
4. This backs up the System State data, system services, and all disks associated with the operating system components
5. Does not include data files
6. To restore select Start > Control Panel > Backup and Restore > create a system repair disc on the left > select a drive > then click create disc


« All Control Panel Items ▸ Backup and Restore
Search Con...
Control Panel Home
Create a system image
Create a system repair disc
See also
Action Center
Windows Easy Transfer
Back up or restore your files
Backup
Set up backup
Restore
Select another backup to restore files from
Recover system settings or your computer

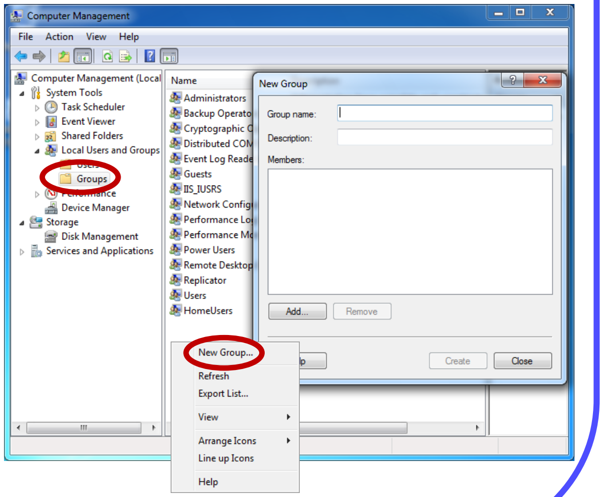
Windows Backup has not been set up.

Windows could not find a backup for this computer.

BASIC SECURITY

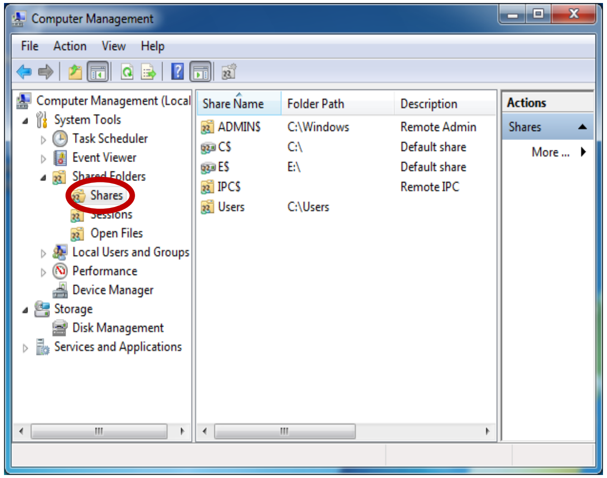
Users and Groups

1. A user group or security group is a collection of user accounts that all have the same security rights
2. A user account can be a member of more than one group
3. The two most common user groups are the standard user group and the administrator group
4. An administrator account can create custom user groups, move accounts from one group to another, and add or remove accounts from different groups
5. When you create a custom user group, you can choose which rights to assign
6. Cannot be completed on Windows 7 Starter, Windows 7 Home Basic, and Windows 7 Home Premium
7. To open select Start > Control Panel > Administrative Tools > Computer Management > Local Users and Groups in the left pane



Administrative Shares

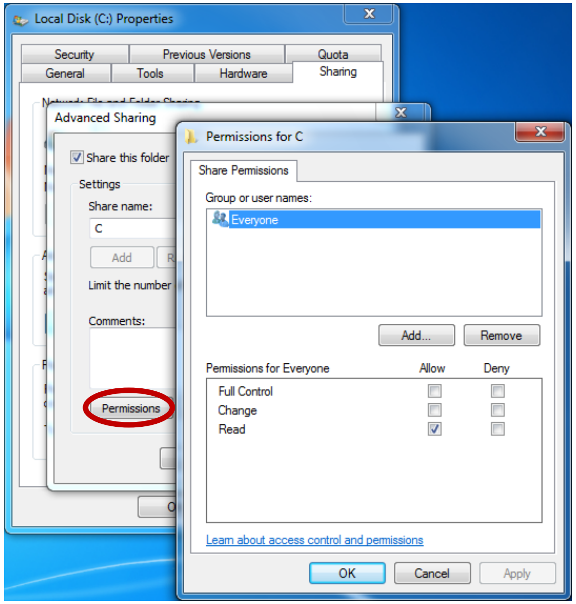
1. The default network shares
2. These default shares share every hard drive partition in the system
3. These shares will allow anyone who can authenticate as any member of the local Administrators group access to the root directory of every hard drive on the system
4. Are not accessible by default on home editions of XP, Vista or Windows 7
5. The "$" appended to the end of the share name means that it's a hidden share
   A. `\\MyComputer\C$`
   B. `\\MyComputer\ADMIN$` (shares access to %SYSTEMROOT%)
6. To view shares select Start > Control Panel > Administrative Tools > Computer Management > click Shard Folders in the left pane > Shares



Share Name	Folder Path	Description
ADMIN$	C:\Windows	Remote Admin
C$	C:\	Default share
E$	E:\	Default share
IPC$		Remote IPC
Users	C:\Users	

Share Permissions

1. Only apply to users who access the resource over the network
2. When you share a folder by default the “Everyone” group is given the read permission
3. It applies to all files and folders in the shared resource
4. Does not apply if you use terminal services, mapped drives, the Run command, or local user
5. Use Security Permissions to secure these
6. Security permissions are not available on FAT or FAT32 file systems



☑ Share this folder

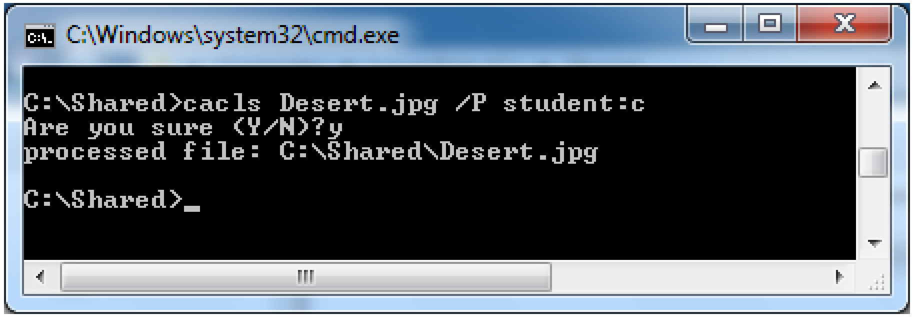
Share name: C

Group or user names: Everyone

Permissions for Everyone	Allow	Deny
Full Control	□	□
Change	□	□
Read	☑	□

Share Permissions

1. Command line:
   A. `cacls` *`filename`* `/G` *`user:permission`* (grant access to user)
   B. `cacls` *`filename`* `/D` *`user:permission`* (deny access to user)
   C. `cacls` *`filename`* `/P` *`user:permission`* (replace user access)
   D. Permissions
      - N (None)
      - R (Read)
      - W (Write)
      - C (Change)
      - F (Full control)

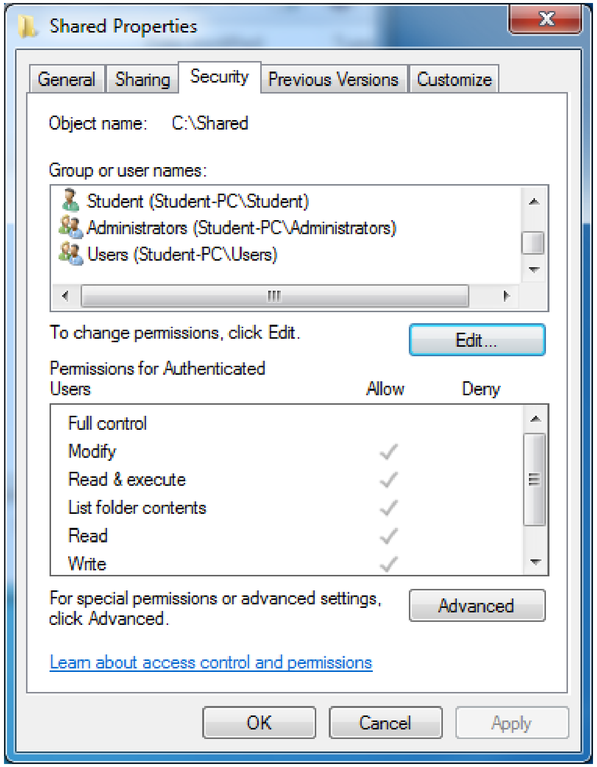


```
C:\Shared>cacls Desert.jpg /P student:c
Are you sure (Y/N)?y
processed file: C:\Shared\Desert.jpg

C:\Shared>_
```

Security Permissions

1. Applies to users logged on locally, terminal services, mapped drives, the Run command
2. Provides a more secure access
3. Can only be set on a volume that is formatted to the NTFS file system
4. Effective permissions are the result of combining the user's assigned permissions and the permissions of any groups the user belongs to
5. You should apply both shared and security permissions
6. Remove the "Everyone" access
7. Careful when using the "Administrators" group because anyone with "Administrator" privileges will have access



Object name: C:\Shared

Group or user names:

- Student (Student-PC\Student)
- Administrators (Student-PC\Administrators)
- Users (Student-PC\Users)

To change permissions, click Edit.

Permissions for Authenticated Users	Allow	Deny
Full control		
Modify	✓	
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write	✓	

For special permissions or advanced settings, click Advanced.

Summary

In this Module we discussed:

1. Safe Mode
2. Task Manager
3. Msconfig
4. Scheduling Backups
5. Scheduling Check Disk
6. Scheduling Defragmentation
7. Windows Updates
8. Driver Updates
9. Antivirus Updates
10. System Restore
11. Automated System Recovery
12. User and Group Permissions

Glossary and Terms

1. **Safe Mode –** A diagnostic mode of Windows
2. **msconfig** – Microsoft System Configuration
3. **Task Manager** – System Monitor Application
4. **Kernel** – The basic windows OS application that manages the input/output between hardware and software.
5. **Paged memory** – Memory usage performed by the operating system that transfers data between main memory and a hard drive.
6. **Process –** An instance of a computer program being executed.
7. **Thread –** Code execution inside a process.
8. **SSD –** Solid State Drive
9. **VHD** – Virtual Hard Disk
10. **Fragment** – A non-contiguous data file.
11. **Driver** – Software that bridges a hardware device to the operating system.
12. **Action Center** – A component of Windows that provides users with the ability to view the status of computer security and maintenance.
13. **ASR** – Automated System Recovery