AIR FORCE ASSOCIATION'S

CYBERPATRIOT

NATIONAL YOUTH CYBER EDUCATION PROGRAM

UNIT EIGHT

Microsoft Windows Security Configuration

www.uscyberpatriot.org

Learning Objectives

- Participants will learn how to implement proper file-level permissions on Windows systems
  - Purpose, use, and types
  - Permission inheritance and parent/child relationships
  - Customization
- Participants will understand how backups function and best-practice backup strategies
  - Availability and integrity
  - Major backup techniques and types
  - Configuration
- Participants will understand how audit logging and system monitoring are performed and configured
  - Audit logging purpose and configuration
  - Performance monitoring purpose and configuration

SECTION ONE

Windows File Protections

The CIA Triad (Review)

- 3 Goals of information security:
  - Maintain information **confidentiality**
    - Making sure only approved users have access to data
  - Maintain information **integrity**
    - Data Integrity: assurance that information has not been tampered with or corrupted between the source and the end user
    - Source Integrity: assurance that the sender of the information is who it is supposed to be
  - Maintain information **availability**
    - Ensuring data is accessible by approved users when needed

Source: http://www.techrepublic.com/blog/it-security/the-cia-triad/

File Permissions

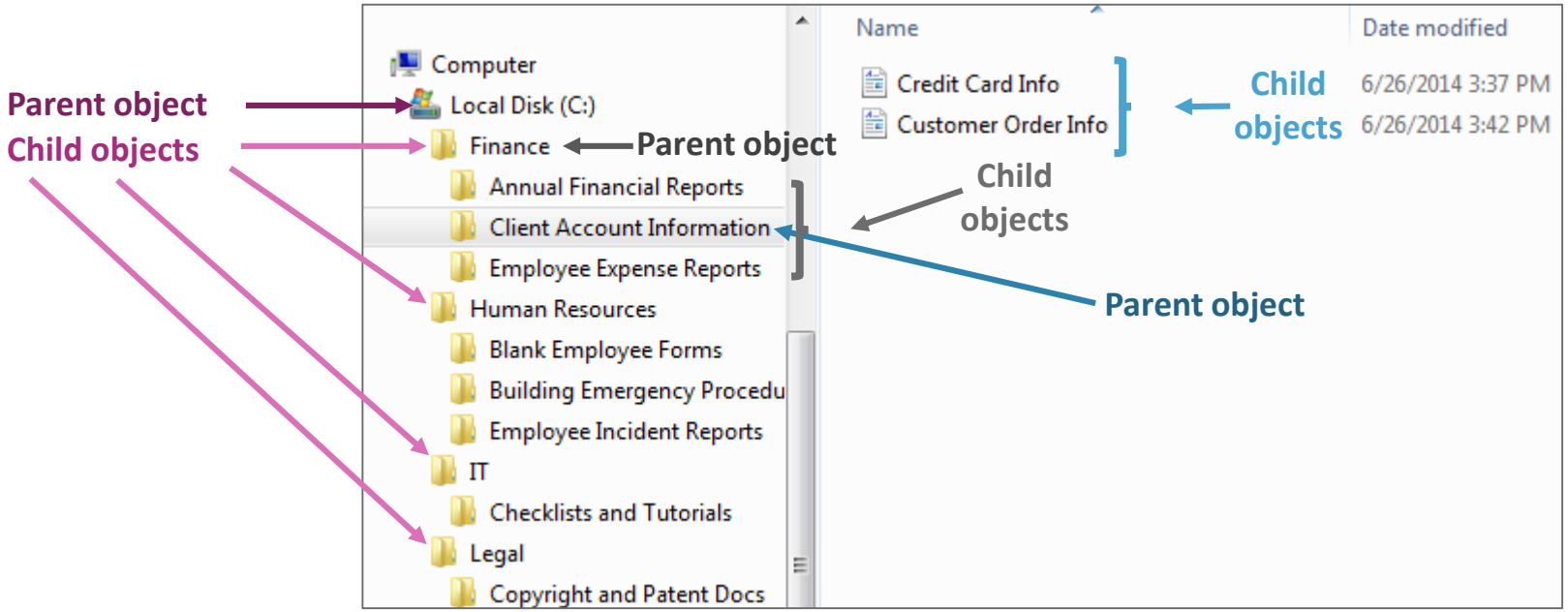
- Important tool for ensuring data integrity and confidentiality
- More customizable than the blanket set of permissions given to users by adding them to either the Users or Administrators group
- Use to restrict access or editing rights to specific data on shared resources
- Can be customized by individual user or by user group

Types of File Permissions

- Full Control
  - Administrator level access
  - Users can make every possible change to a selected file or the contents of a selected folder
- Modify
  - Allows users to change a file's content, but not its ownership
  - Users cannot delete the file
- Read & Execute
  - Allows users to open and run programs
- List Folder Contents
  - Allows users to view the names of files stored in the selected folder
- Write
  - Allows users to make changes to a file and overwrite existing content
- Read
  - Allows users to view the attributes of a file or folder, but not edit it

Parent and Child Objects

- Use inheritable permissions to apply the same security settings to all of the files (child objects) in a folder (parent object)



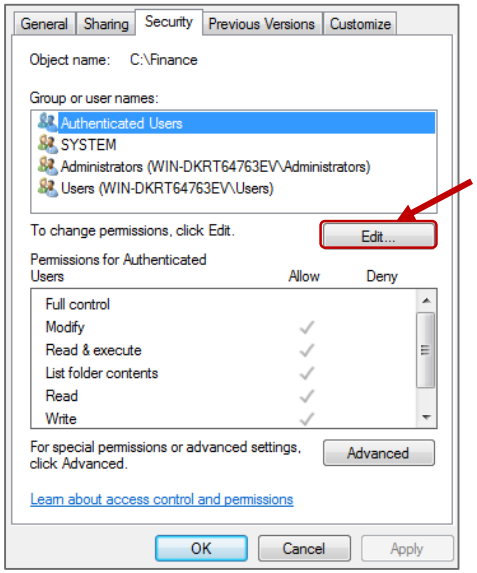
Inheritable Permissions

- By default, objects within a folder, known as child objects, inherit permission settings from their containing folder, known as the parent object
- You can turn off inheritable permissions and customize who gets what kind of access to certain folders, subfolders, or documents
- Depending on how many users need access to a sensitive file or folder and how many of the files in a folder need to be restricted, there are several ways to apply permissions
  - E.g. If you want certain users or groups to be denied access to *all but a few* files within a folder, it is quickest to apply a restrictive permission setting to the parent object (folder). Once you have denied those users' access to all of the files in the folder, you can go to the individual files you do want them to have access to and override the permissions those files inherited from the parent folder.

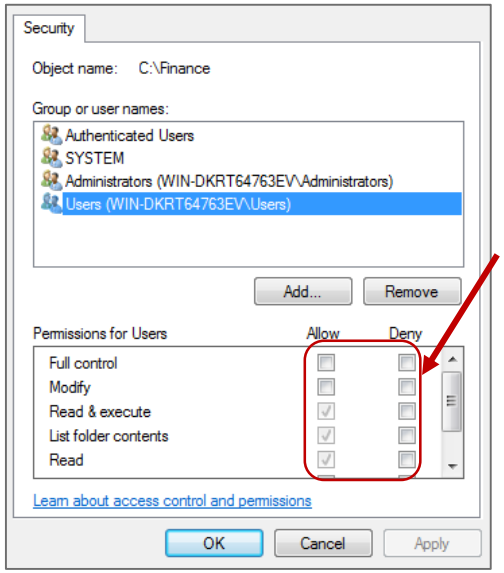
Customizing Permissions

- To apply the same permissions to all of the contents of a folder, Right-click the folder → Select Properties → Click the Security tab
- Edit the permissions of an entire group by highlighting it and checking the appropriate boxes
- Edit the permissions of a specific user (or subgroups you have created) by using the "Add…" button to add him/her to the Group or Usernames box and then checking the appropriate boxes

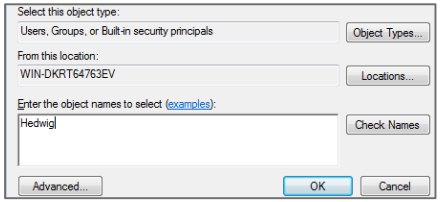
1.



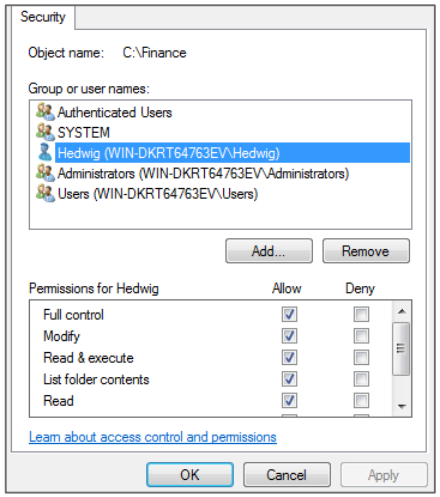
2.



3.



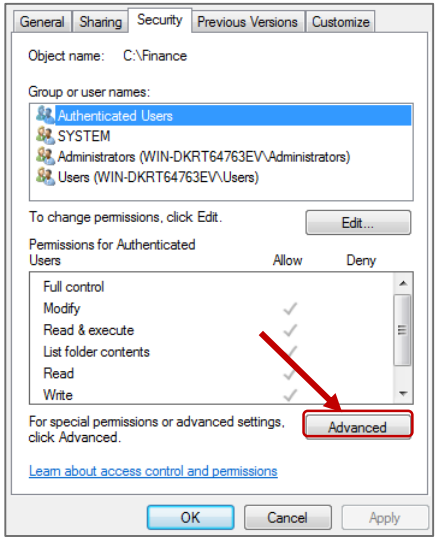
4.



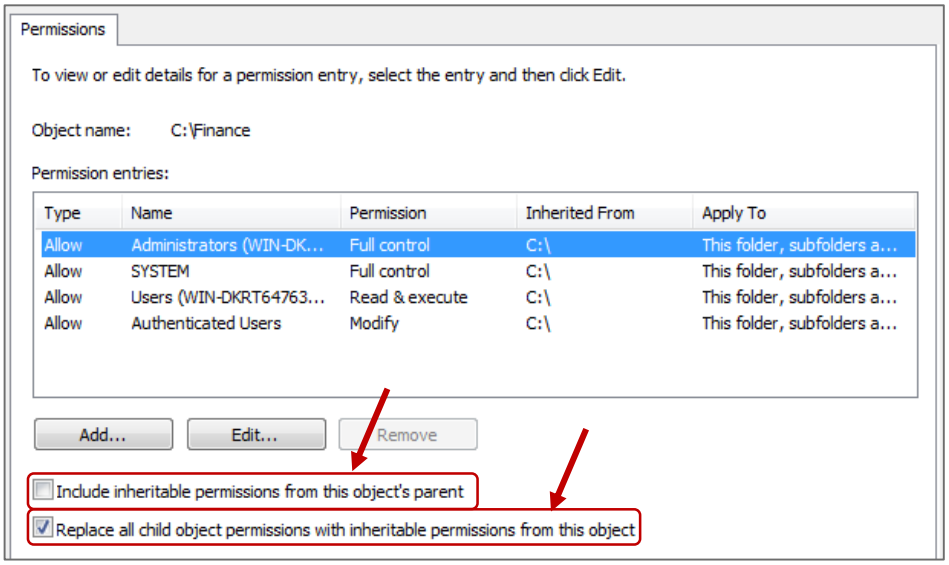
Customizing Permissions

- To remove permissions inherited from a parent and create custom settings, Click the "Advanced" button from the Security tab → Click Change Permissions → Uncheck the "Include inheritable permissions…" box
- Customize permissions for individual users and/or groups using the "Add…" button.
- To extend your new settings to all of the child object or to extend permissions to the child objects in a folder, check the "Replace all child objects…." button

1.

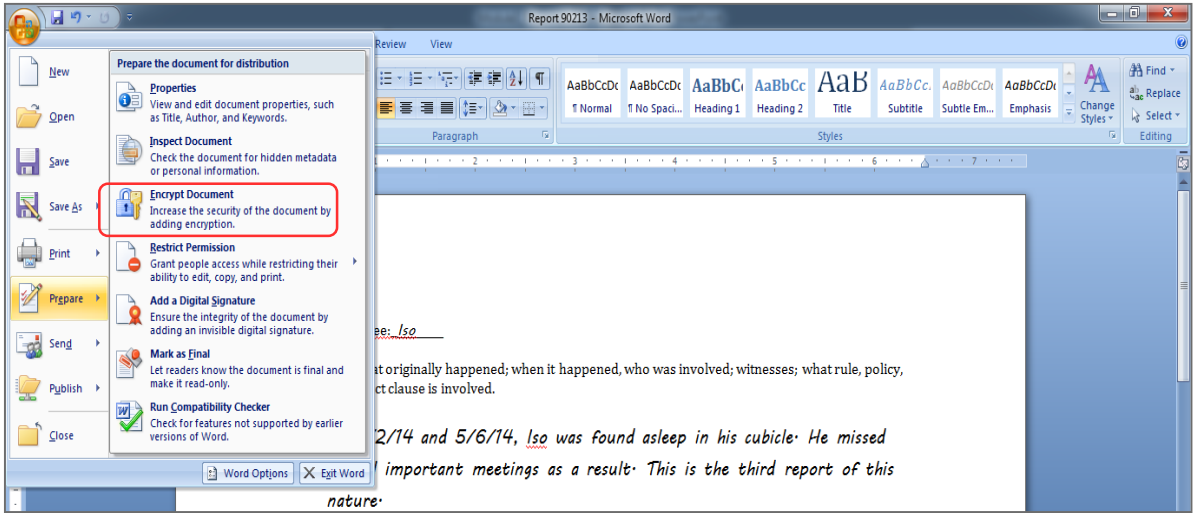


2.
3.



MS Office File Encryption

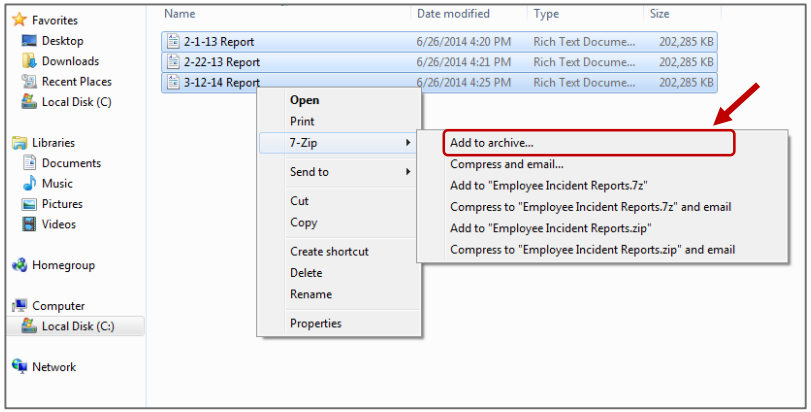
- Another method of protecting information confidentiality and integrity
- Much quicker than setting file permissions and can be used to control access to documents shared with people outside your network
- Open a Microsoft Word document → Click the Window button → Prepare → Encrypt Document



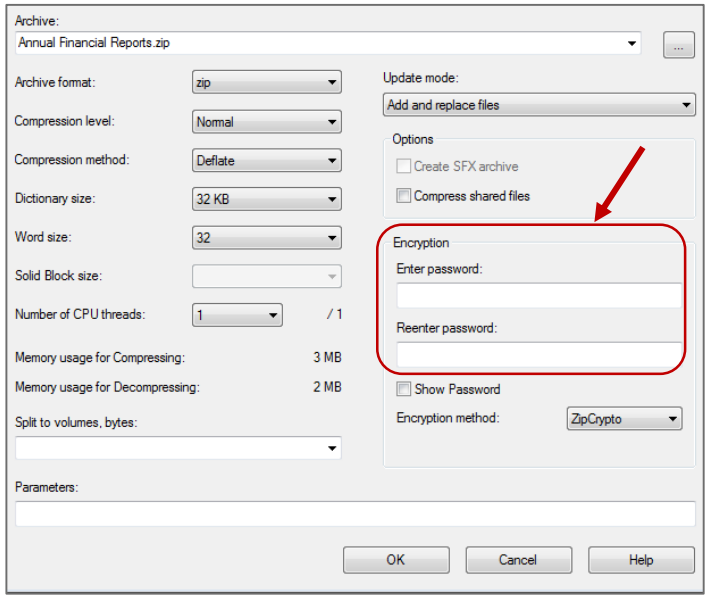
7-Zip Zipped File Encryption

- Encrypt multiple files and files of different types (.doc, .mp4, etc.) at once by zipping (compressing) them in 7-Zip or another zipping program
- To install 7-zip, go to: www.7-zip.org
- Zipping also condenses the size of files, making them easier to transfer across the Internet or fit on a USB drive
- Open your Documents→ Select Files → Right-Click → 7-Zip → Add to Archive → Use the Encryption section to add a password to the .zip file

1.



2.



Windows Backup Options

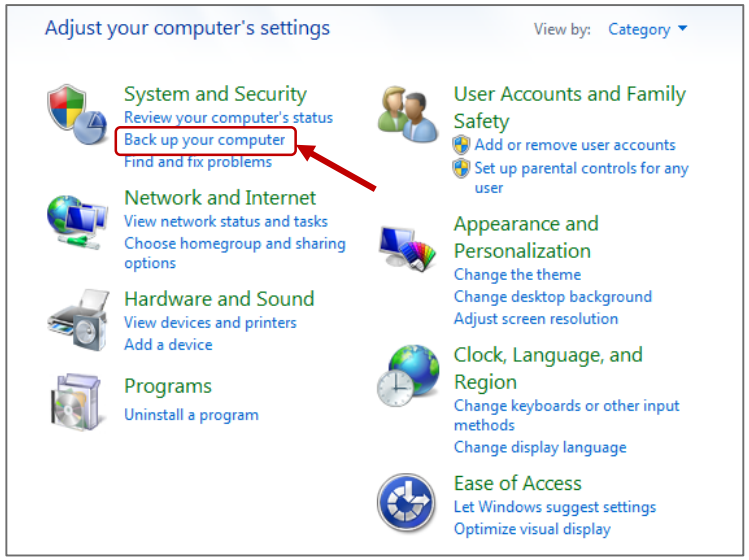
- Ensure data remain available to users during and after a natural disaster, power outage, hardware failure or hacking attack
- If your system is breached and files lose their integrity, backups can be restored to allow users to work with the latest untampered versions of files
- Windows allows you to create three types of backups:
  - System Repair Disc:
    - Contains only the system files needed to install/restore Windows to a computer without a functioning OS
    - Can be followed with a system image to restore everything else
  - System image:
    - Contains files and programs on your system and Windows system files and settings
    - When you boot a computer with a functioning OS from a system image, the entire system will be automatically restored
  - "Full" Backup
    - Saves the program files, folders, and documents you have selected to back up, so they can be later restored to a machine with a functioning OS
    - Much smaller file size than system repair discs, so can be run more frequently

Sources: http://windows.microsoft.com/en-us/windows7/what-is-a-system-image, http://windows.microsoft.com/en-us/windows7/create-a-system-repair-disc, http://windows.microsoft.com/en-us/windows/back-up-files#1TC=windows-7

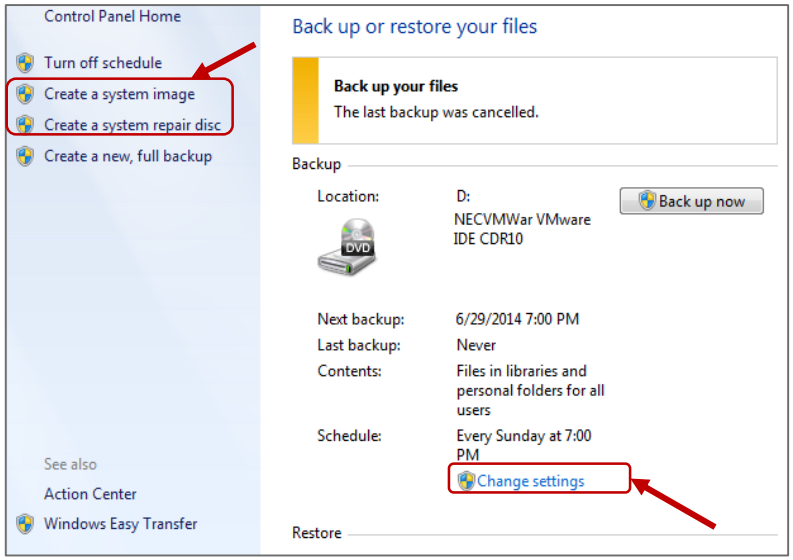
Creating Backups

- Control Panel → System and Security → Backup your computer
- Use the buttons on the left to launch the setup wizards for system images and system repair disc
- Use the change settings button to set-up regular, automatic “full backups”

1.



2.



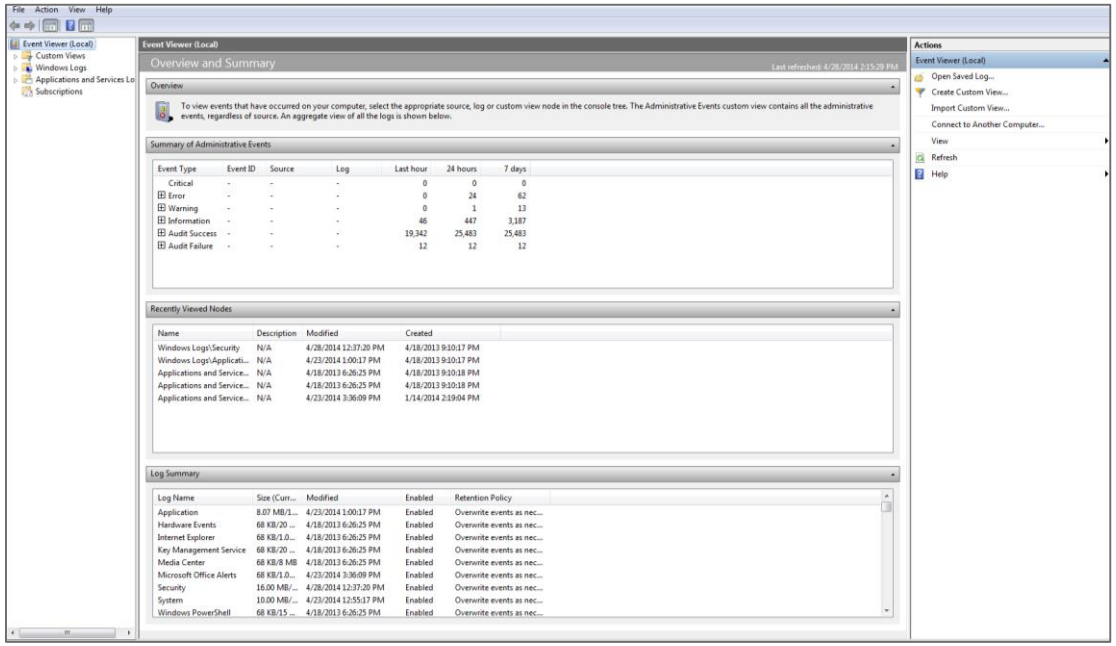
Sources: http://windows.microsoft.com/en-us/windows7/what-is-a-system-image, http://windows.microsoft.com/en-us/windows7/create-a-system-repair-disc, http://windows.microsoft.com/en-us/windows/back-up-files#1TC=windows-7

SECTION TWO

Windows Auditing

Event Viewer

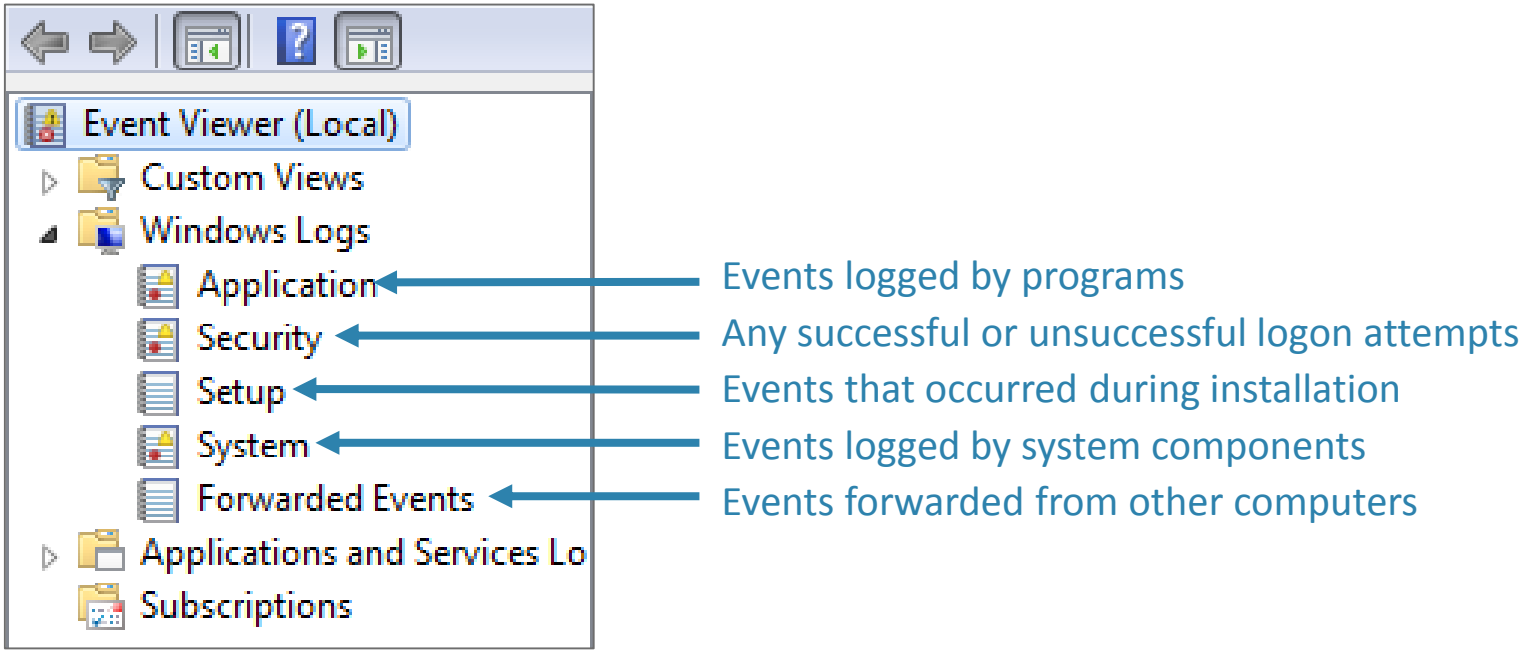
- Security tool that allows you to view records of changes and other events that have happened on a computer
- Used by cybersecurity professionals to monitor system changes and the inner workings and less visible processes run by a computer
- Control Panel → System and Security → Administrative Tools → Event Viewer



Source: http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/sag_seconceptsimpaudbp.mspx?mfr=true

Windows Logs

- Security logs can be a useful last defense against attacks and a tool for forensics investigations into the source of a past attack or unauthorized entry
- Customize what security logs are kept by setting **Audit Policies**

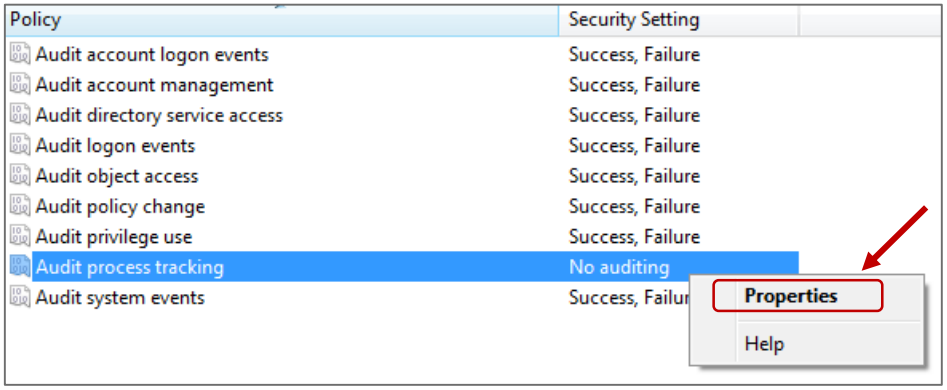


Source: http://technet.microsoft.com/en-us/library/hh824819.aspx

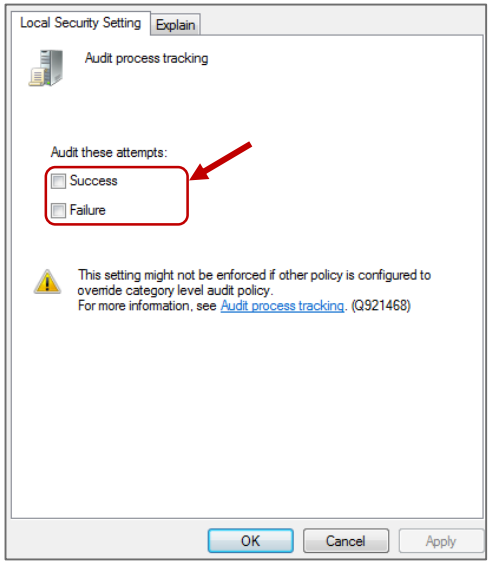
Audit Policy Settings

- Control Panel →System and Security → Administrative Tools → Local Security Policy → Local Policies → Audit Policy
  - Success: generates an event when the requested action succeeds
  - Failure: generates an event when the requested action fails
  - No Auditing: does not generate an event for the action
- Right click the Security Setting column → Properties → Success, Failure

1.



2.



Audit Policy Settings

- Must be set and enabled for logs to be available in the Event Viewer
  - Account logon events: Attempts to log into system accounts
  - Account management: Account creation or deletion, password changes, user group changes
  - Directory service access: Changes to shared resources on a network
  - Logon events: Attempts to log into a specific shared computer
  - Object access: Access to sensitive, restricted files
  - Policy change: Attempts to change local security policies, user rights, and auditing policies
  - Privilege use: Attempts to execute restricted system changes
  - Process tracking: Attempts to modify program files, which have rewritten or disrupted program processes (*key to detecting virus outbreaks)
  - System events: Computer shutdowns or restarts

*Recommended for Windows 7 users and Windows Server 2008 users
*Recommended only for Windows Server 2008 users

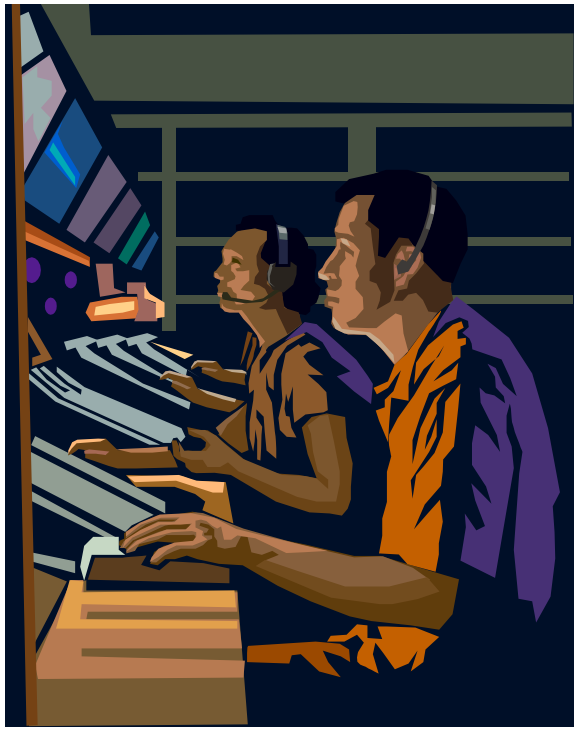
Sources: http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/sag_seconceptsimpaudbp.mspx?mfr=true , http://technet.microsoft.com/en-us/library/dd277311.aspx , http://technet.microsoft.com/en-us/library/dn487457.aspx

SECTION THREE

Performance Monitoring

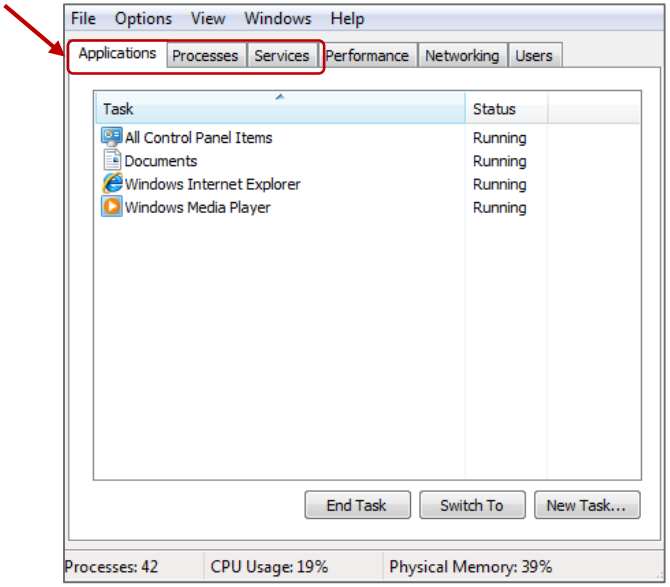
Performance Monitoring

- Allows you to track the use and performance of hardware and software resources on a system
- Allows you to view real-time and historical data
  - Stop problems as they're happening
  - Predict future problems
  - Conduct forensics to close vulnerabilities and stop intrusions of the same type from happening again
- Allows you to decide if hardware or software needs updating
- Allows you to determine if unknown programs and/or malware are running
- Allows you to monitor and restrict user access



Task Manager

- Shows programs, services, and processes currently running
- Shows network activity and resource utilization
- Right Click on the Menu Bar → Task Manager *or* press Ctrl + Alt + Del and Select "Start Task Manager"

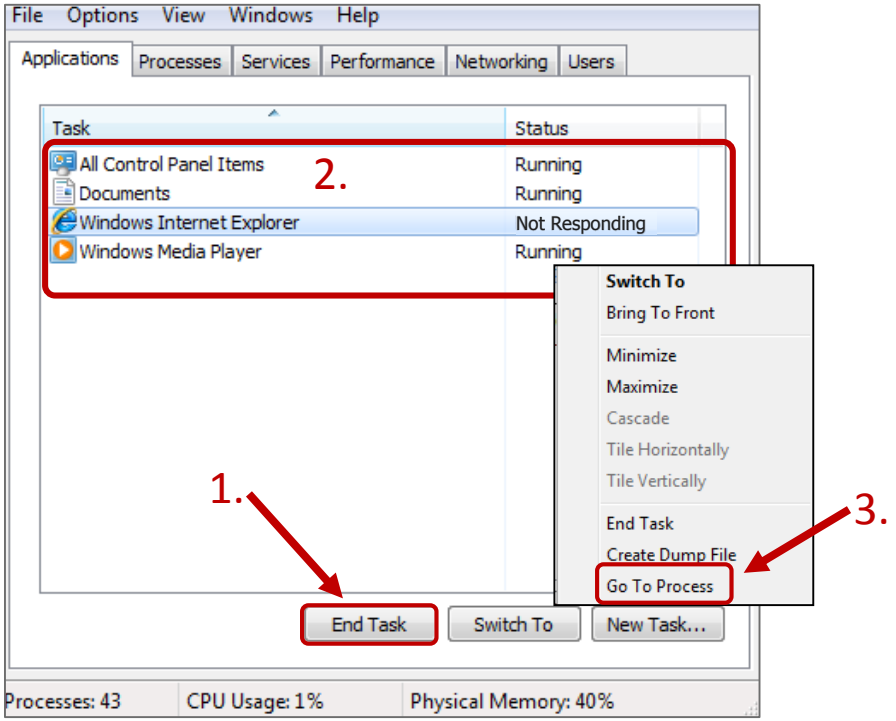


- Applications: programs you interact with on the desktop
- Processes: Files (.exe) that control applications
- Services: processes that do not interact with the desktop (e.g. hardware drivers)

Source: http://superuser.com/questions/209654/whats-the-difference-between-an-application-process-and-services

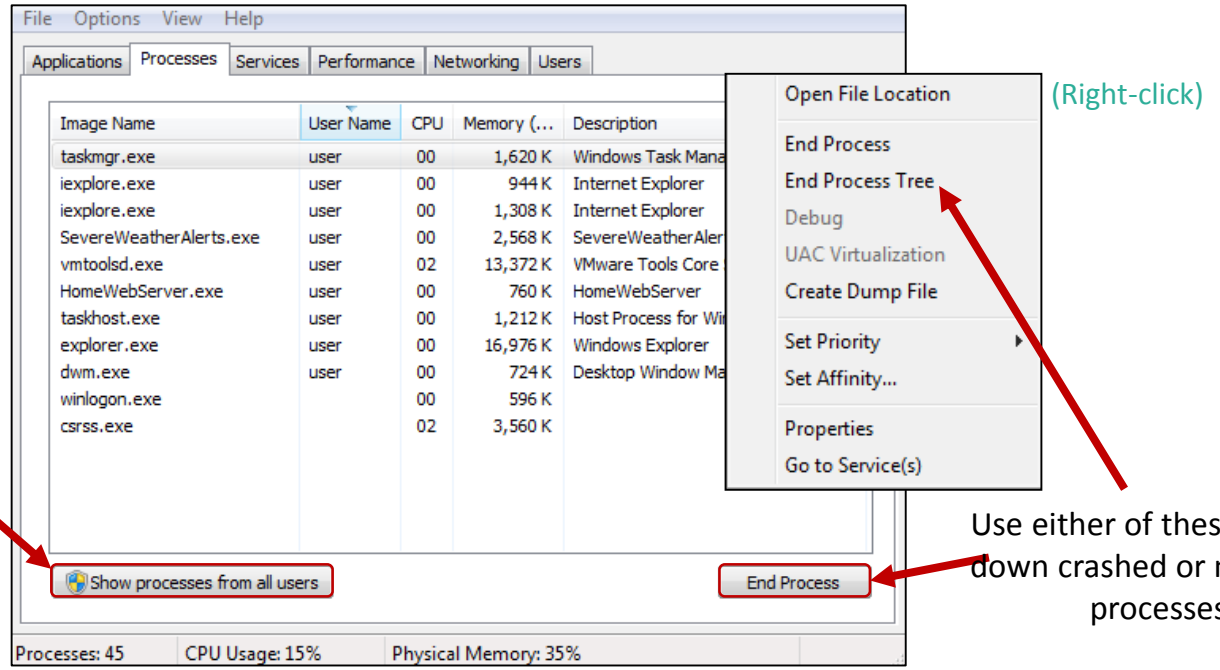
Task Manager – Applications Tab

- Three tasks:
  1. Close programs that are not responding
  2. Check if an unnecessary piece of software is running
  3. Find the process that is associated with certain software, so you do not shut it down when looking for illegitimate services



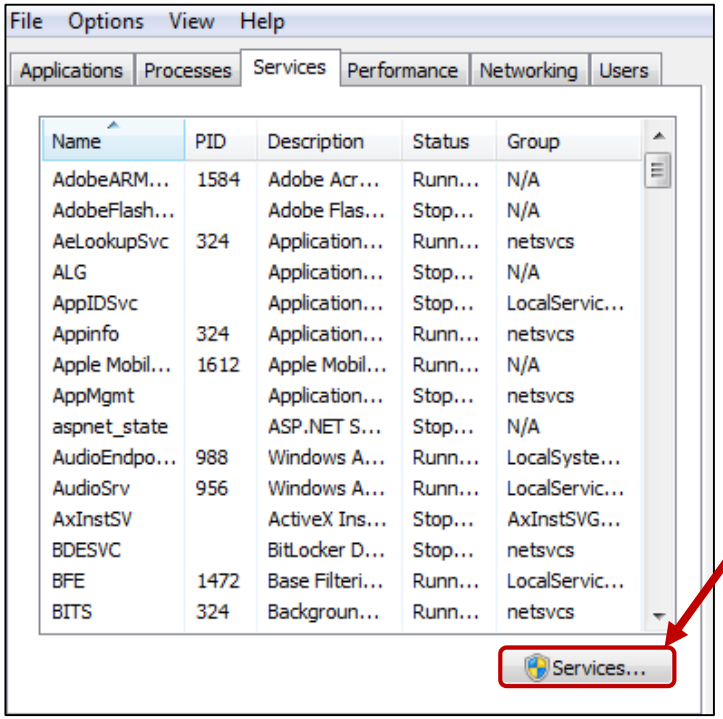
Task Manager – Processes Tab

- Some processes are essential for Windows and should not be shut down
- Some malware are not visible as applications and can only be ended by shutting down associated services
- Lookup processes to determine whether they are legitimate: www.processlibrary.com



Task Manager – Services Tab

- List of programs running in the background
- Click the "Services" button to manage services in advanced window

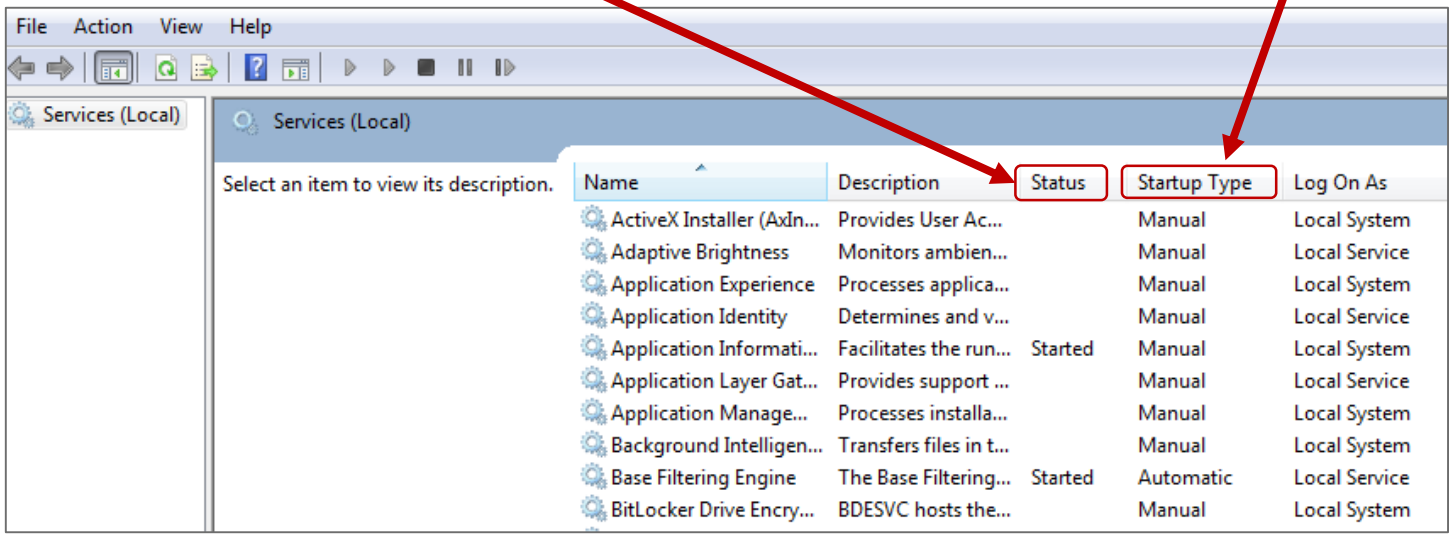


Monitoring Services

- Services are programs that run invisibly and automatically in the background
  - E.g. Windows Defender and Windows Firewall

Status:
- Started: Currently running
- Blank: Not running

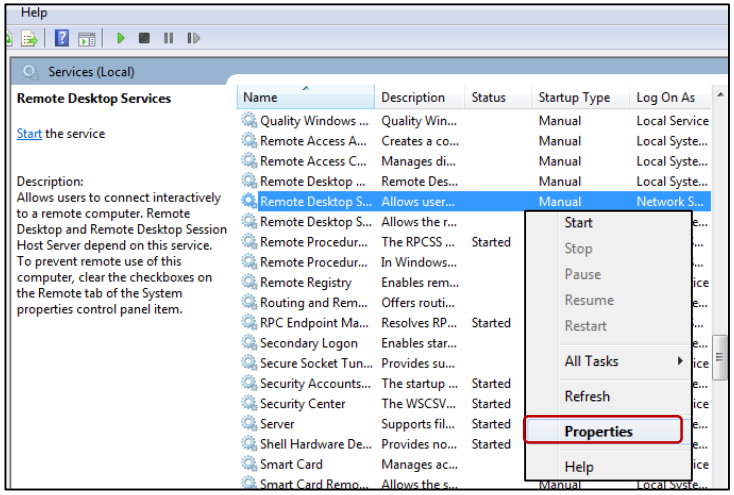
Startup Type (how services start when the computer is booted up):
- Automatic: Starts when computer is booted up
- Manual: Starts when prompted to by user
- Disabled: Cannot be re-enabled automatically or manually by regular users (only Admins)



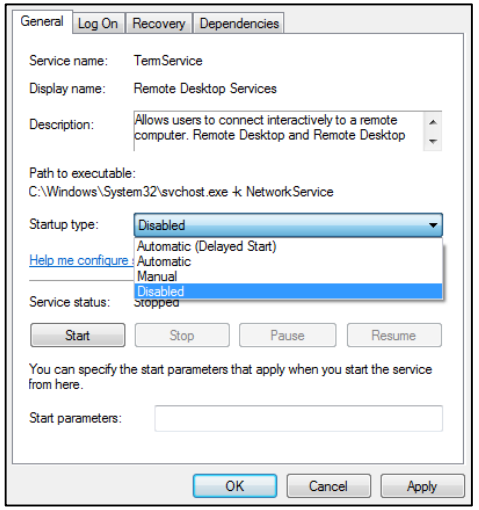
Disabling Services

- Two reasons to disable services:
  1. Unnecessary
     - E.g. Spotify or other programs that decrease student/worker efficiency
  2. Insecure
     - E.g. Remote Desktop Services or others than allow people to access your file systems from outside the organization's networks
- To disable a service or otherwise change its startup type, right-click it and select "Properties"

1.



2.

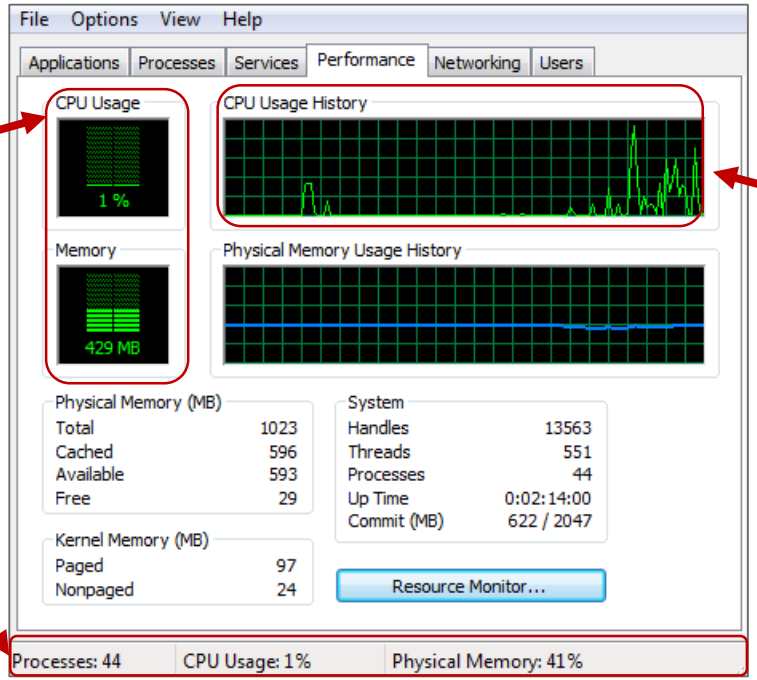


Source: http://www.techrepublic.com/blog/10-things/10-plus-windows-7-services-you-may-not-need/

Task Manager: Performance Tab

- Monitors current and past resource use
- Shows CPU usage by core
  - -If your computer has multiple cores, you will see multiple CPU graphs
  - -The more cores your computer has, the higher its processing power

Show the current usage of your CPU and memory out of the total available on your computer.



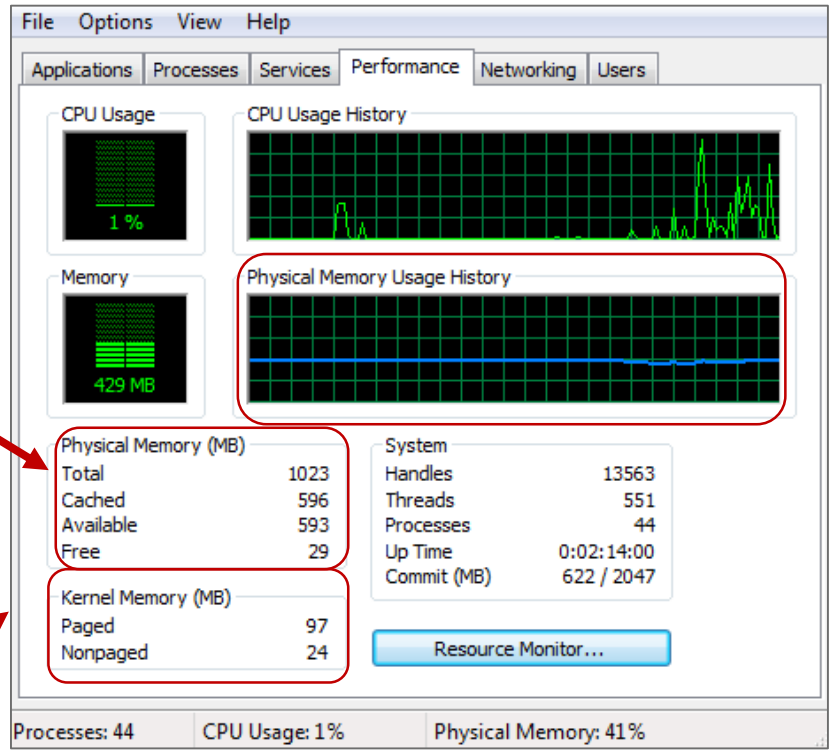
Shows CPU usage over time. A high percentage indicates a program or process might not be responding. Ending that process or program should improve performance.

Source: http://windows.microsoft.com/en-us/windows/see-details-computers-performance-task-manager#1TC=windows-7

Task Manager: Performance Tab (cont.)

Provides details on how RAM is being used. Cached RAM is used by system resources, available RAM is the amount immediately available for use by processes, drivers, or the OS, and free RAM is unused or does not contain useful information

Lists how much memory is being used by the OS as a whole. If these numbers are very high, Windows might be corrupt or there is a piece of malware that is hampering its ability to run effectively.



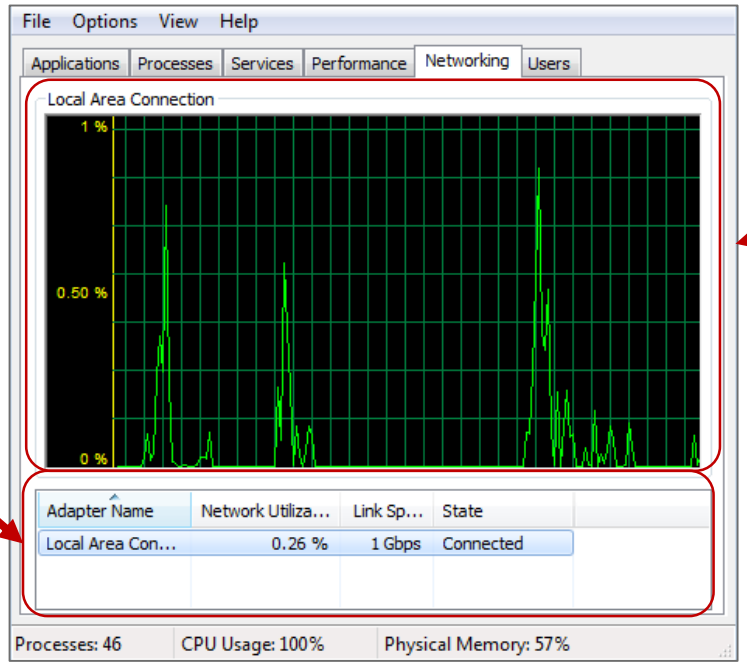
Displays the amount of RAM being used over time. Extremely high values could indicate hidden malware is operating on your system.

Source: http://windows.microsoft.com/en-us/windows/see-details-computers-performance-task-manager#1TC=windows-7

Task Manager: Networking Tab

- Network connectivity problems can arise from a broken router, switch, or cable, or from the computer itself
  - The Networking tab will allow you to check whether the computer is the origin of the problem

Lists the names of your connections and tells you the percentage of your overall network that each connection is utilizing, the speed of the link, and whether or not that link is fully connected.

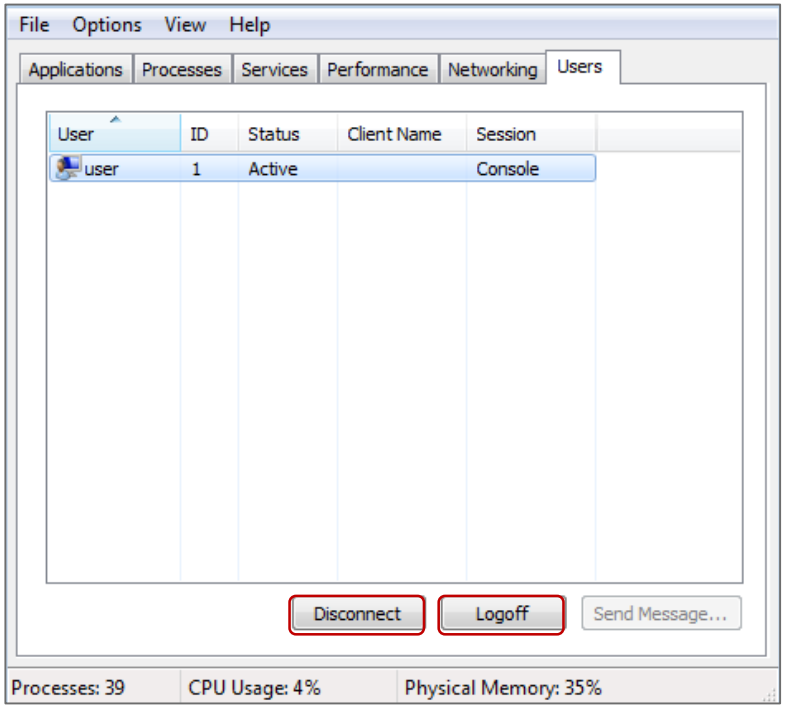


Shows network performance over time. If utilization is very high one or more programs on your may be eating up all of your available bandwidth. Or, if you are not currently using any programs connected to the Internet, a high number could indicate you have malware on your computer or that an intruder is accessing your computer remotely.

Source: http://www.bleepingcomputer.com/tutorials/how-to-use-the-windows-task-manager/#networking

Task Manager: Users Tab

- Shows you all of the users currently logged on to the system
- Allows you to “disconnect” users
  - Terminate the user’s connection without shutting down the programs they were running
- Allows you to “logoff” users
  - Log the user off the computer completely and terminate any running programs



Source: http://www.bleepingcomputer.com/tutorials/how-to-use-the-windows-task-manager/#networking