

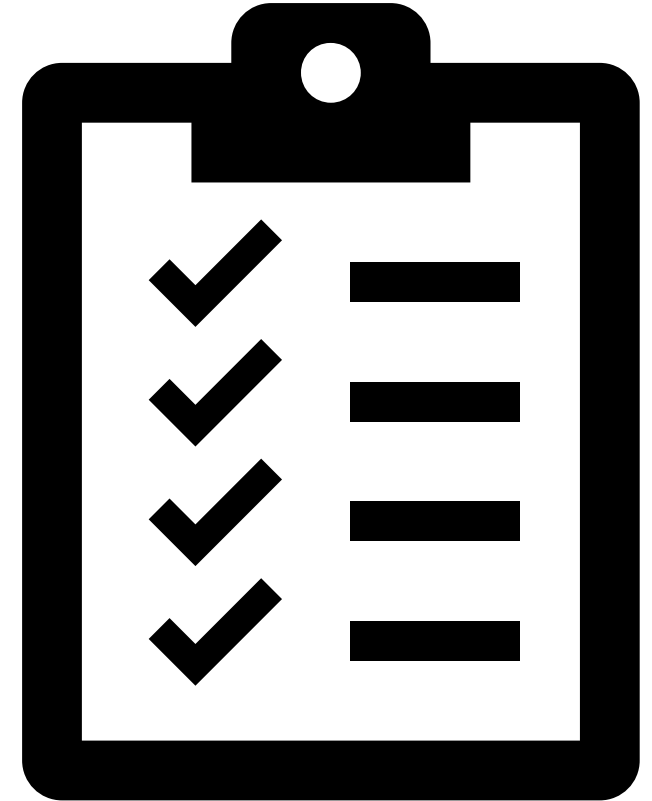


# Microsoft Windows Security Configuration

## Unit 6

# Learning Objectives

- Edit File-level permissions on Windows systems
  - Purpose, use, and types
  - Permission inheritance and parent/child relationships
  - Customization
- Backup function and best-practice backup strategies
  - Availability and integrity
  - Major backup techniques and types
  - Configuration
- Audit logging and system monitoring
  - Audit logging purpose and configuration
  - Performance monitoring purpose and configuration





# Windows File Protections

## Section 1



# 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**

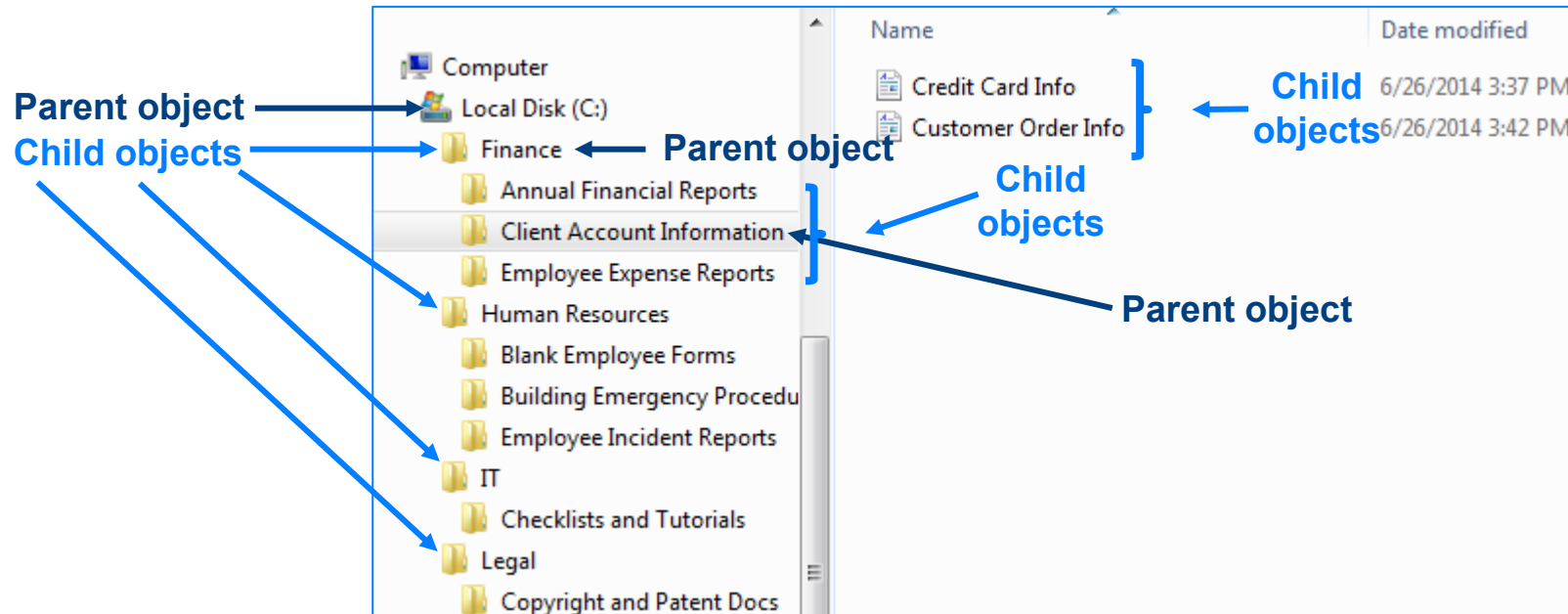
- Allows users to make changes to a file and overwrite existing content

- **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)



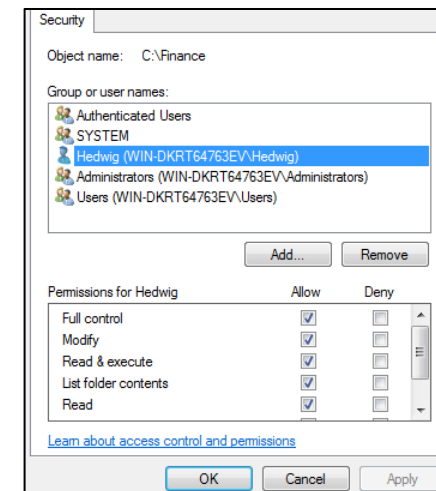
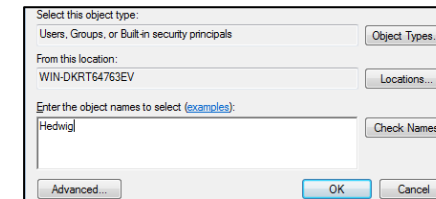
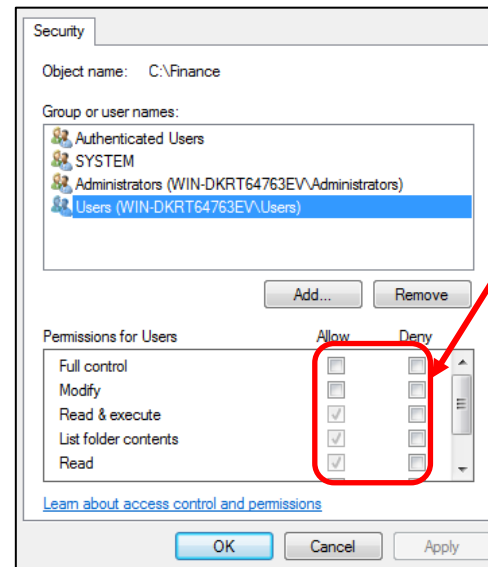
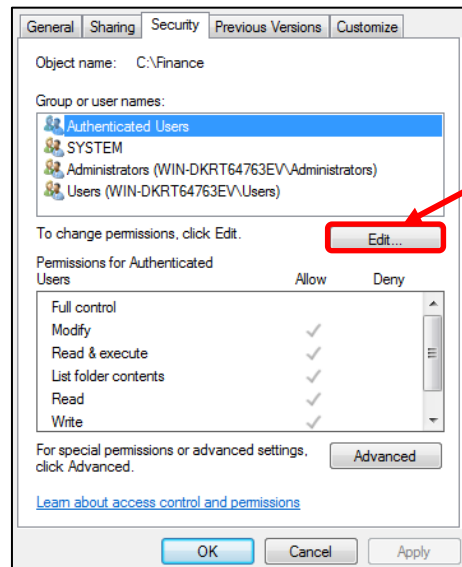


# Inheritable Permissions

- 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.

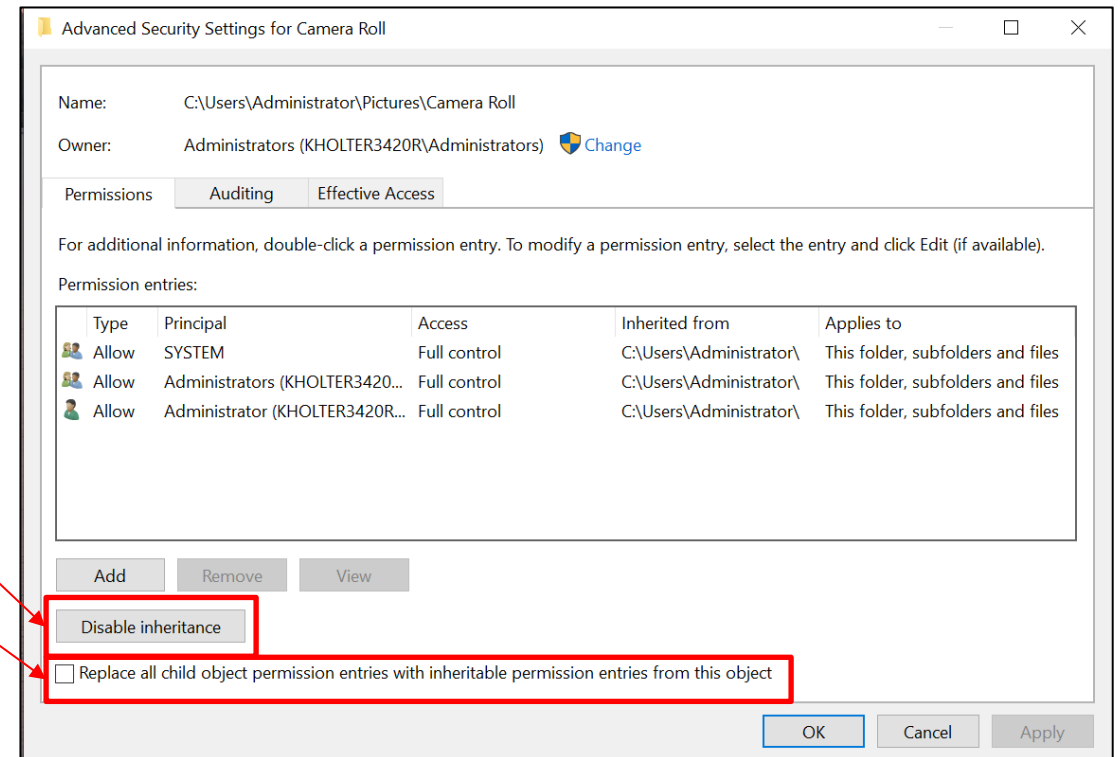
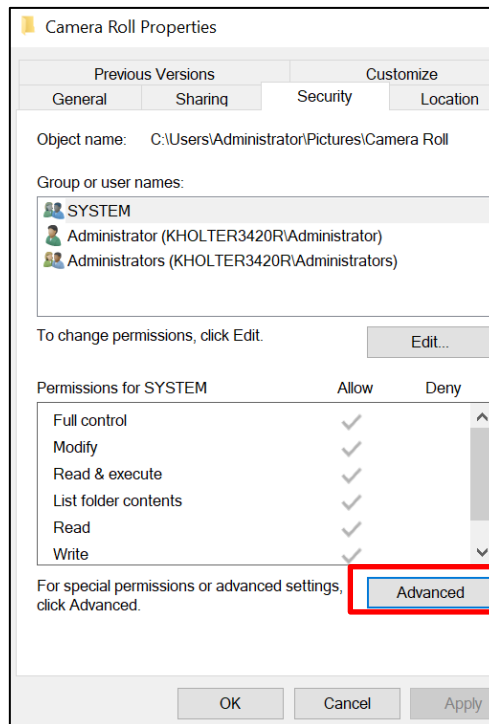
# Customizing Permissions

- 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



# 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

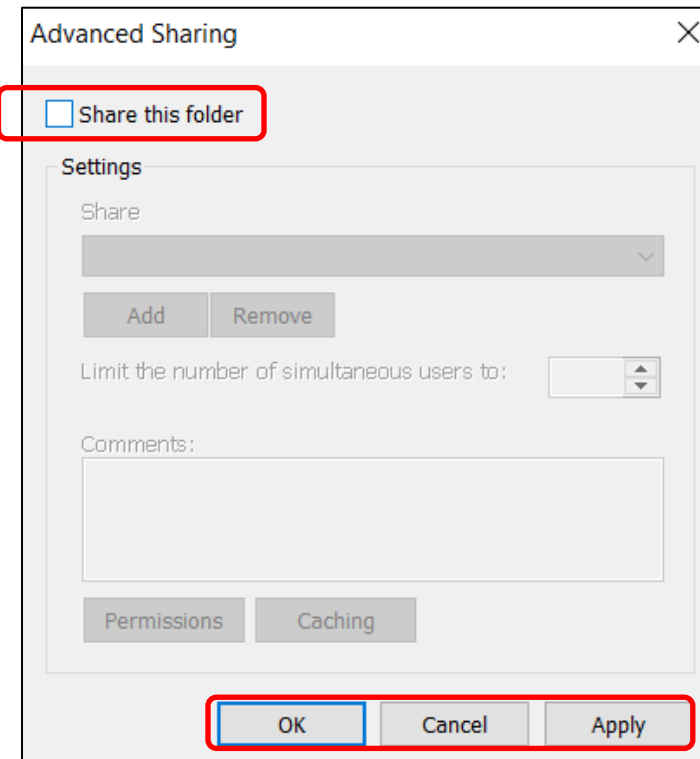
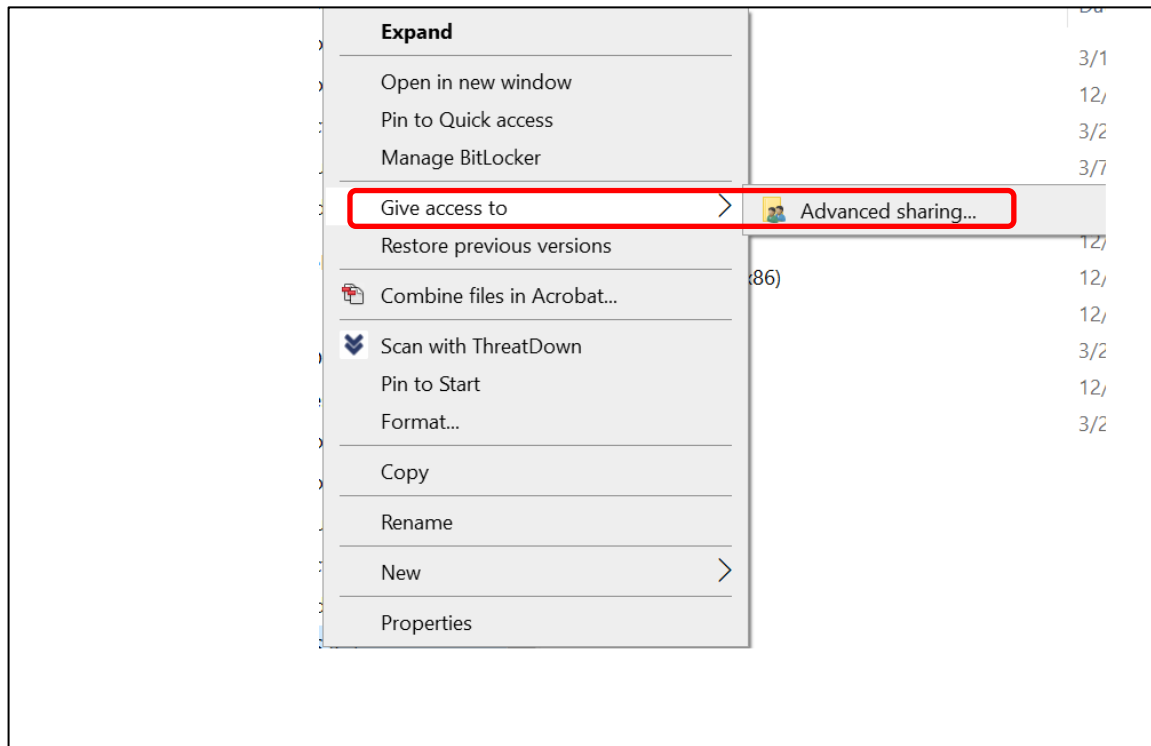


# File Permissions

- Restrict access or editing rights to data on shared resources
- Types of permissions:
  1. Full Control
  2. Modify
  3. Read & Execute
  4. List Folder Contents
  5. Write
  6. Read

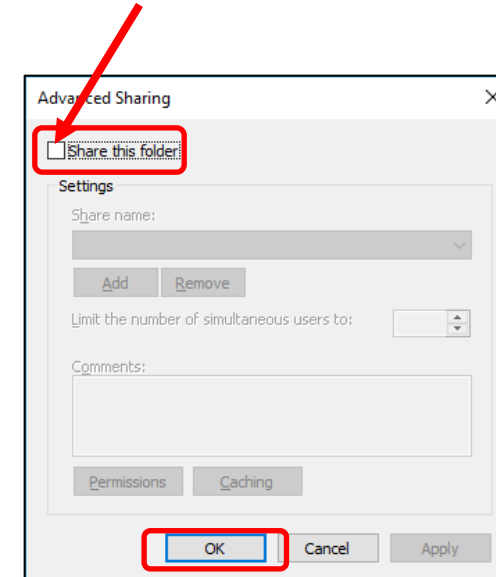
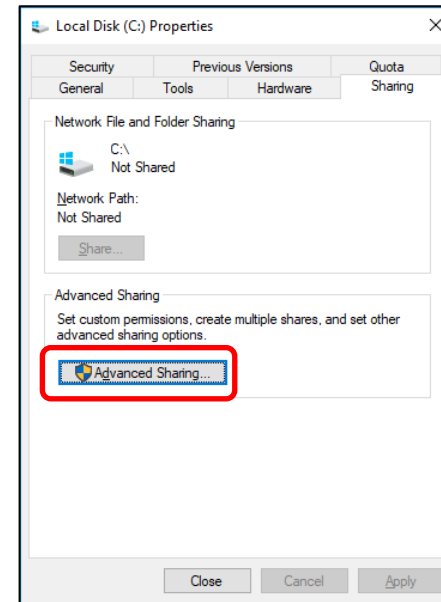
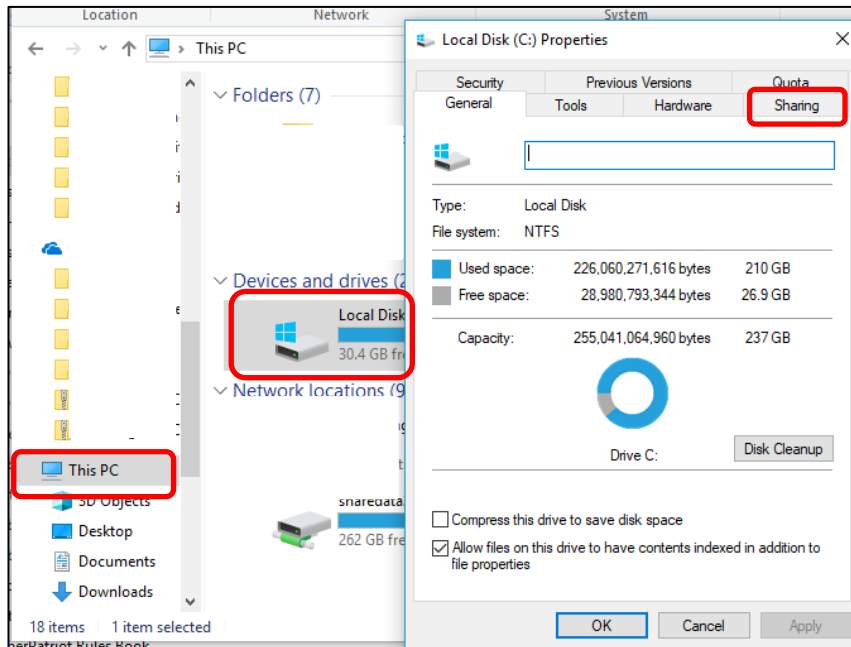
# Sharing Drives

- You can share an entire network's files by sharing its drives
- Generally, not a good idea – Anyone could see or modify your files
- To turn off Sharing Drives: Open File Explorer → Click This PC → Right Click the Local Disk Drive → Share with → Advanced Sharing → Uncheck Share this folder → Click OK



# Sharing Drives

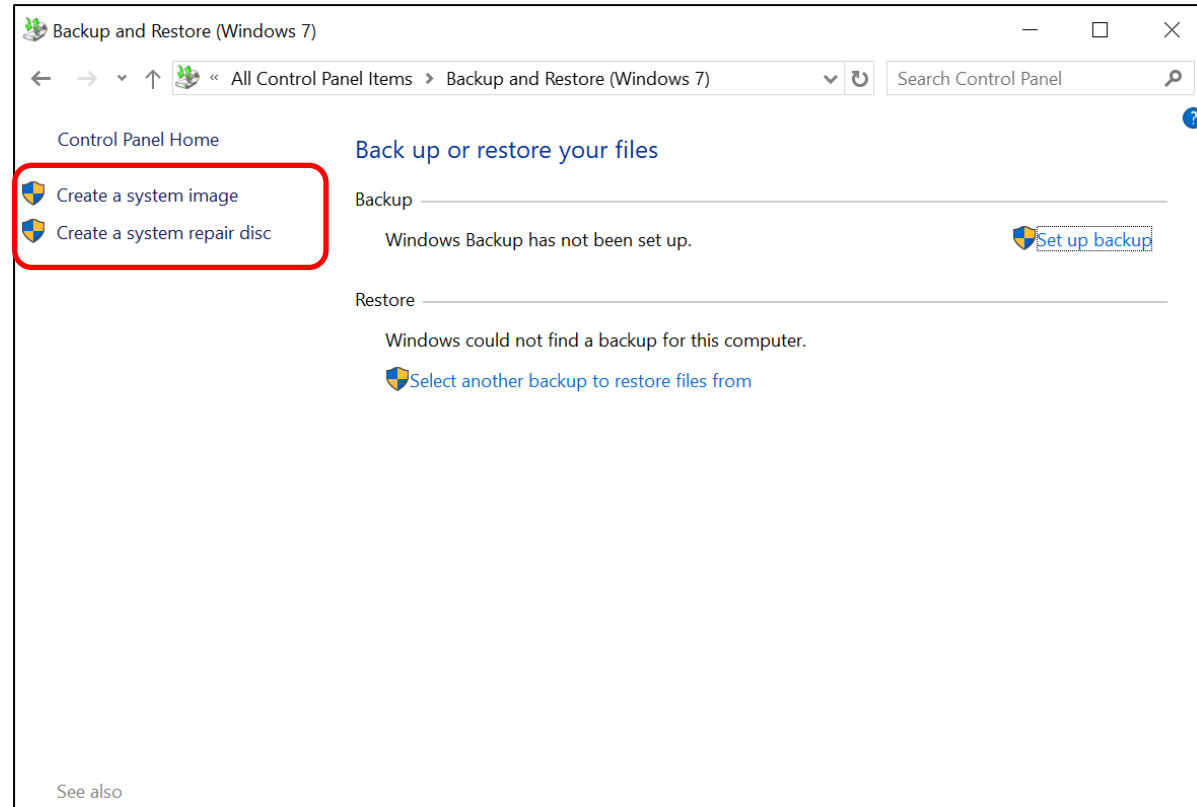
- Alternate Method
- To turn off Sharing Drives: Open File Explorer → Click This PC → Right Click the Local Disk Drive → Properties → Sharing → Advanced Sharing → Uncheck Share this folder → Click OK



# Creating Backups

- Control Panel → System and Security → Backup and restore

- System image:**  
Contains files, programs, system files, and settings
- Create a System repair disc:**  
Contains necessary system files





# Windows Auditing and Monitoring

## Section 2

# Event Viewer

- Displays logs of events occurring on the Windows operating system

## Windows 10

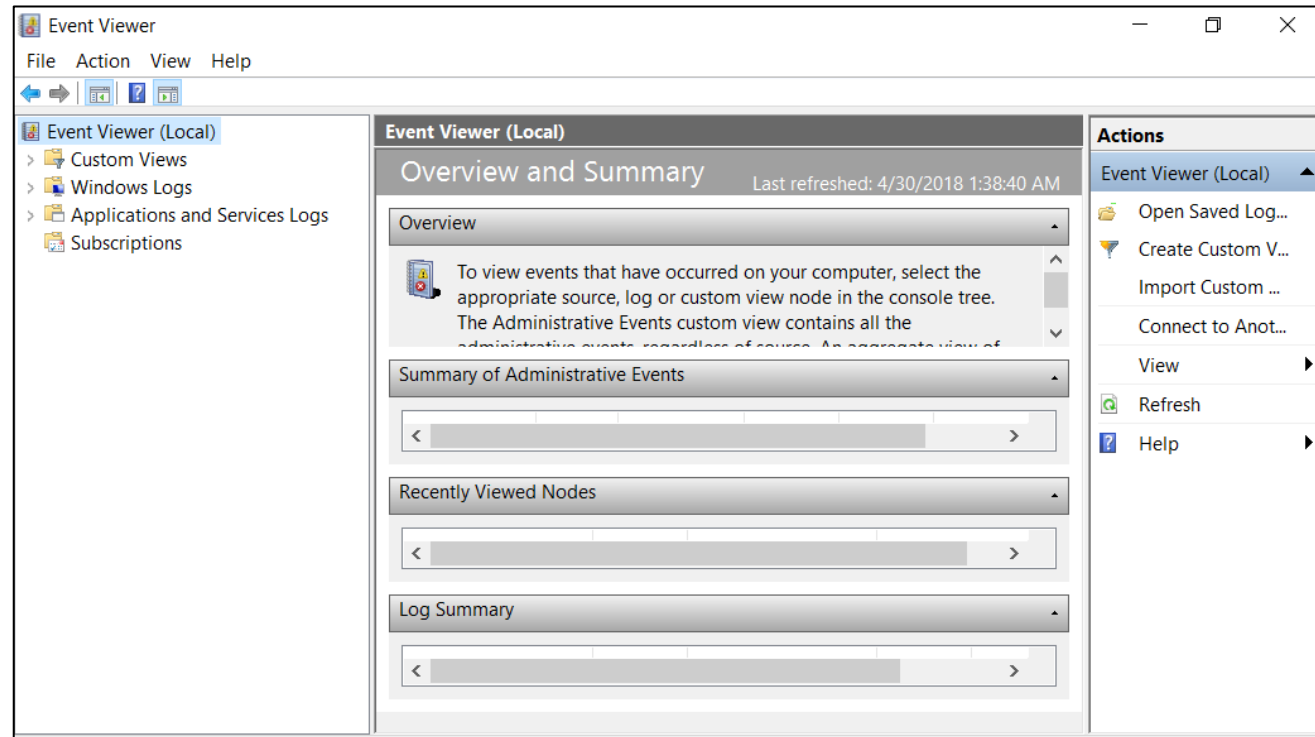
Control Panel → Administrative Tools → Event Viewer

OR Search → Event Viewer

## Windows 11

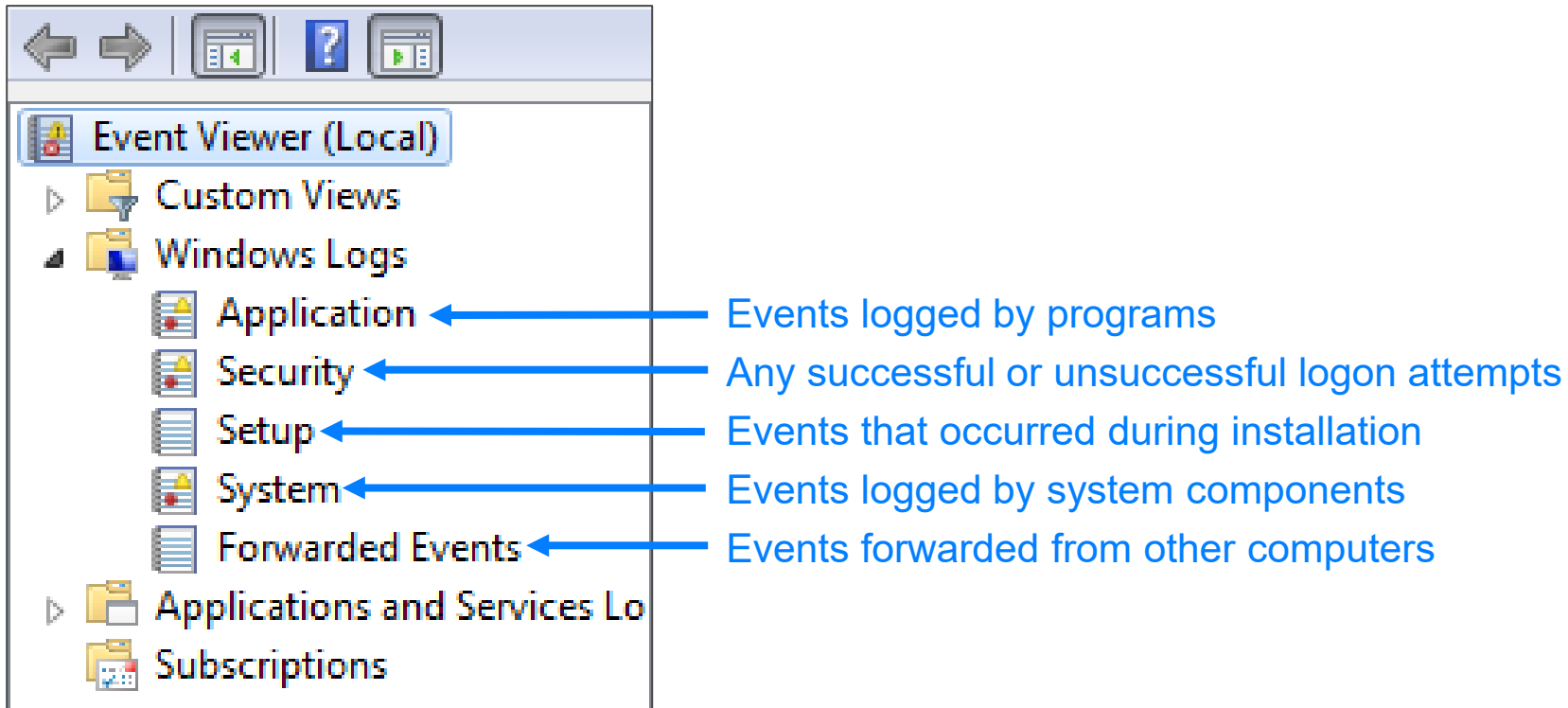
Control Panel → System and Security → Windows Tools → View event logs

OR Search → Event Viewer



# Windows Logs

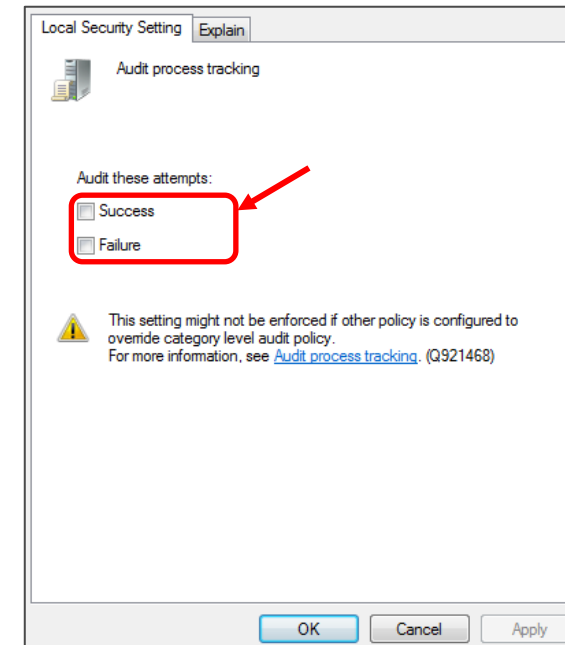
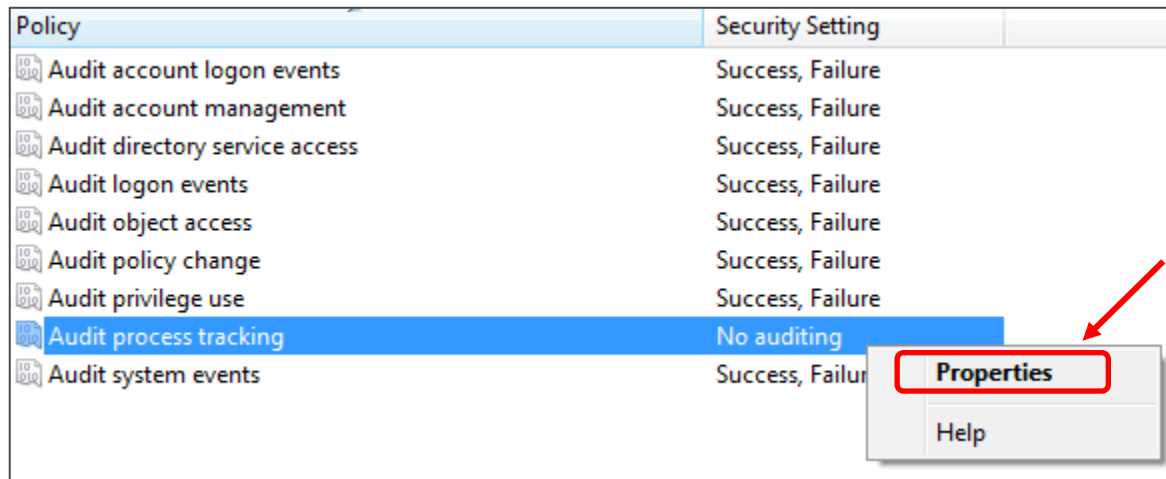
- Customize what security logs are kept by setting **Audit Policies**
- Security logs can be a useful last defense against attacks and a tool for forensics investigations into the source of a past attack or unauthorized entry



# Audit Policy Settings

- **Windows 10:** Control Panel → Administrative Tools → Local Security Policy → Local Policies → Audit Policy
- **Windows 11:** Control Panel → System and Security → Windows 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

Policy	Security Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Success, Failure
Audit logon events	Success, Failure
Audit object access	Success, Failure
Audit policy change	Success, Failure
Audit privilege use	Success, Failure
Audit process tracking	No auditing
Audit system events	Success, Failure



# Audit Policy

- Must be set and enabled for logs to be available in the Event Viewer

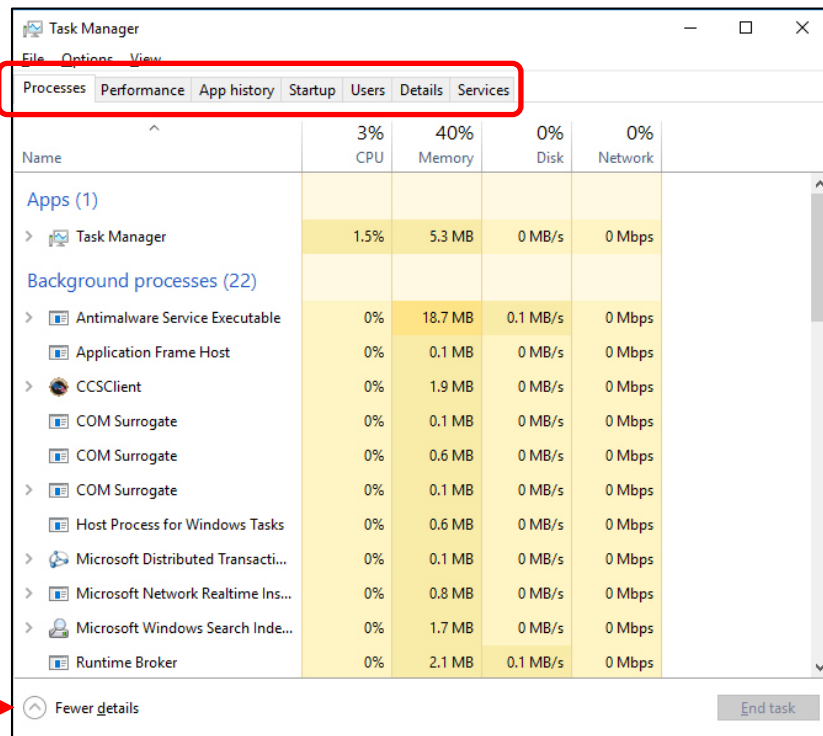
Policy	Security Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Success, Failure
Audit logon events	Success, Failure
Audit object access	Success, Failure
Audit policy change	Success, Failure
Audit privilege use	Success, Failure
Audit process tracking	Success, Failure
Audit system events	Success, Failure

Recommended for Windows 10 users

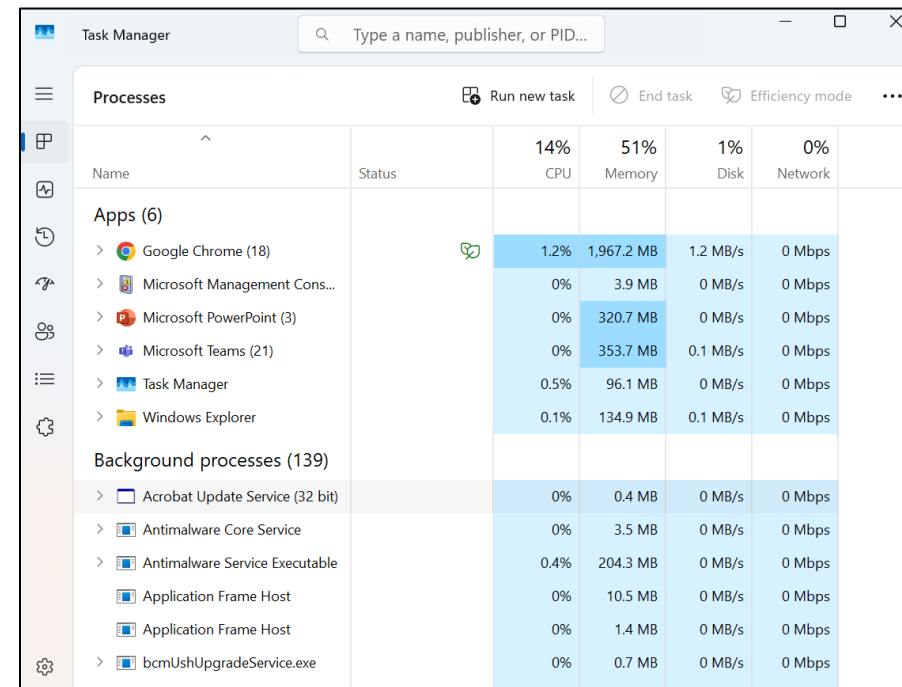
# Task Manager

- Shows programs, services, and processes currently running
- Shows network activity and resource utilization
- Search → Task Manager

Windows 10



Windows 11



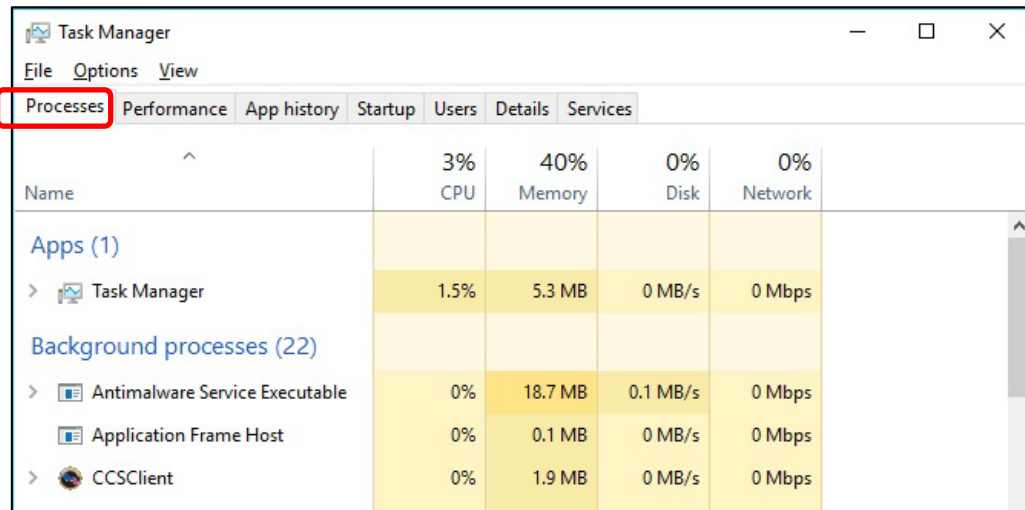
Note: If the Task Manager is showing few details, then click “More details” here



# Task Manager: Processes

- Three tasks:
  - Close programs that are not responding
  - Determine if an unnecessary piece of software is running
  - Find the process that is associated with certain software

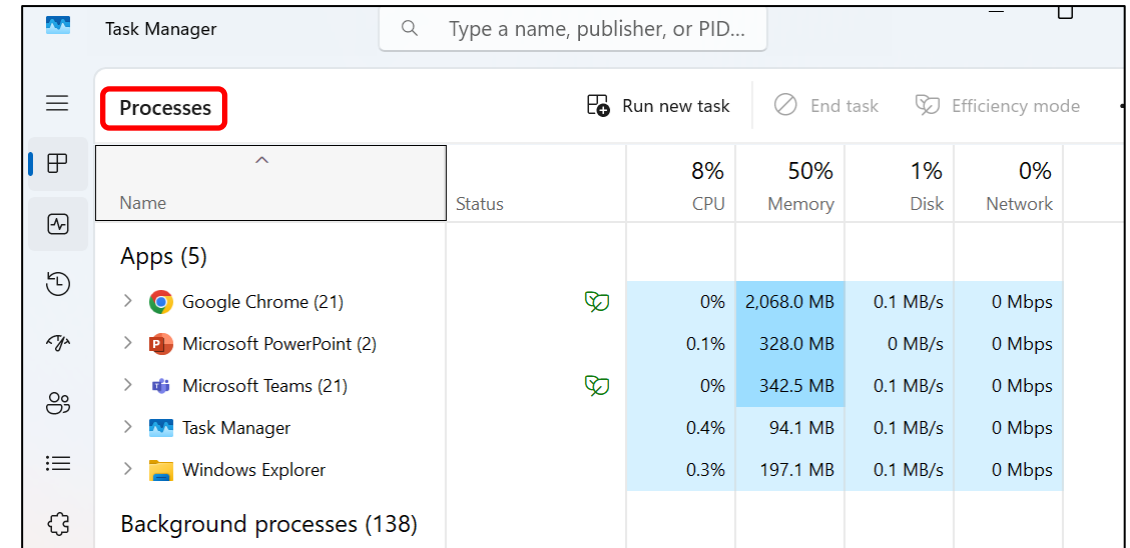
Windows 10



The screenshot shows the Windows 10 Task Manager window with the 'Processes' tab selected. The 'Processes' tab is highlighted with a red box. The window displays a table of running processes, categorized into 'Apps (1)' and 'Background processes (22)'. The table columns are Name, CPU, Memory, Disk, and Network.

Name	CPU	Memory	Disk	Network
<b>Apps (1)</b>				
Task Manager	1.5%	5.3 MB	0 MB/s	0 Mbps
<b>Background processes (22)</b>				
Antimalware Service Executable	0%	18.7 MB	0.1 MB/s	0 Mbps
Application Frame Host	0%	0.1 MB	0 MB/s	0 Mbps
CCSCClient	0%	1.9 MB	0 MB/s	0 Mbps

Windows 11



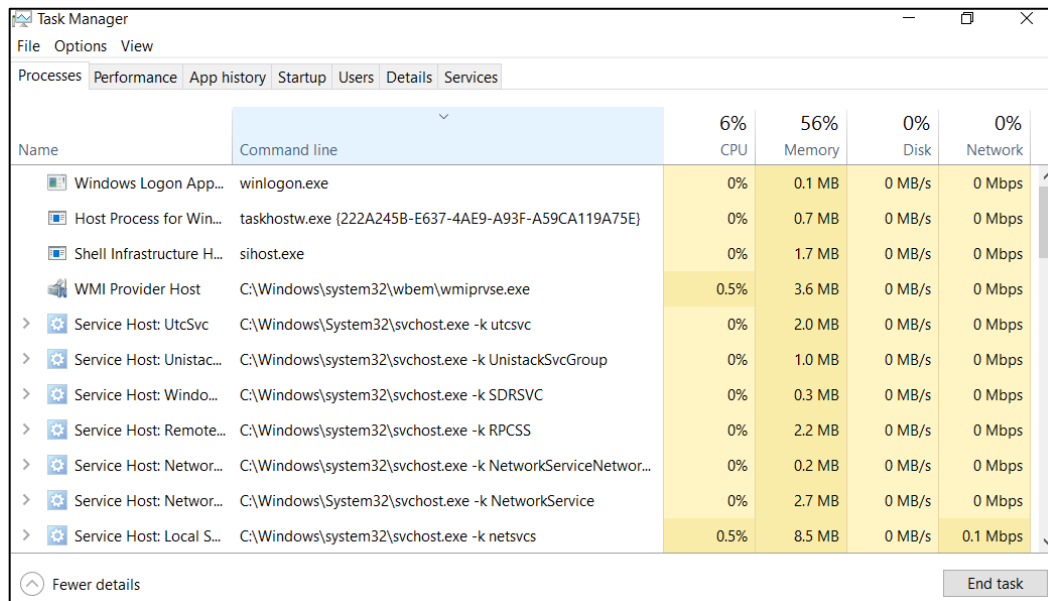
The screenshot shows the Windows 11 Task Manager window with the 'Processes' tab selected. The 'Processes' tab is highlighted with a red box. The window displays a table of running processes, categorized into 'Apps (5)' and 'Background processes (138)'. The table columns are Name, Status, CPU, Memory, Disk, and Network.

Name	Status	CPU	Memory	Disk	Network
<b>Apps (5)</b>					
Google Chrome (21)	Running	0%	2,068.0 MB	0.1 MB/s	0 Mbps
Microsoft PowerPoint (2)	Running	0.1%	328.0 MB	0 MB/s	0 Mbps
Microsoft Teams (21)	Running	0%	342.5 MB	0.1 MB/s	0 Mbps
Task Manager	Running	0.4%	94.1 MB	0.1 MB/s	0 Mbps
Windows Explorer	Running	0.3%	197.1 MB	0.1 MB/s	0 Mbps
<b>Background processes (138)</b>					

# Task Manager: Processes

- Some processes are essential for Windows
- Some malware can only be ended here

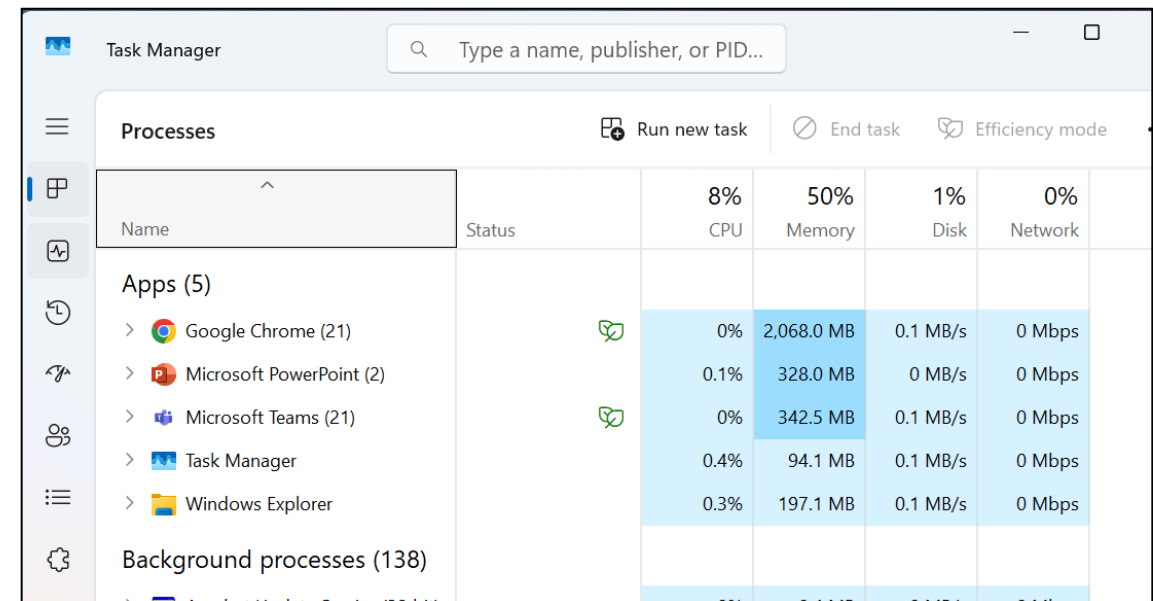
## Windows 10



The screenshot shows the Windows 10 Task Manager interface with the 'Processes' tab selected. The window title is 'Task Manager' and the menu bar includes 'File', 'Options', and 'View'. The 'Processes' tab is active, showing a list of running processes with columns for Name, Command line, CPU usage, Memory usage, Disk usage, and Network usage. The 'Host Process for Windows Explorer' (taskhostw.exe) is highlighted in yellow, indicating it is the active process. Other processes include 'Windows Logon Application' (winlogon.exe), 'Shell Infrastructure Host' (sihost.exe), 'WMI Provider Host', and several 'Service Host' instances.

Name	Command line	CPU	Memory	Disk	Network
Windows Logon App...	winlogon.exe	0%	0.1 MB	0 MB/s	0 Mbps
Host Process for Win...	taskhostw.exe (222A245B-E637-4AE9-A93F-A59CA119A75E)	0%	0.7 MB	0 MB/s	0 Mbps
Shell Infrastructure H...	sihost.exe	0%	1.7 MB	0 MB/s	0 Mbps
WMI Provider Host	C:\Windows\system32\wbem\wmiprvse.exe	0.5%	3.6 MB	0 MB/s	0 Mbps
Service Host: UtcSvc	C:\Windows\System32\svchost.exe -k utcsvc	0%	2.0 MB	0 MB/s	0 Mbps
Service Host: Unistac...	C:\Windows\system32\svchost.exe -k UnistackSvcGroup	0%	1.0 MB	0 MB/s	0 Mbps
Service Host: Windo...	C:\Windows\system32\svchost.exe -k SDRSVC	0%	0.3 MB	0 MB/s	0 Mbps
Service Host: Remote...	C:\Windows\system32\svchost.exe -k RPCSS	0%	2.2 MB	0 MB/s	0 Mbps
Service Host: Networ...	C:\Windows\system32\svchost.exe -k NetworkServiceNetwor...	0%	0.2 MB	0 MB/s	0 Mbps
Service Host: Networ...	C:\Windows\System32\svchost.exe -k NetworkService	0%	2.7 MB	0 MB/s	0 Mbps
Service Host: Local S...	C:\Windows\system32\svchost.exe -k netsvcs	0.5%	8.5 MB	0 MB/s	0.1 Mbps

## Windows 11



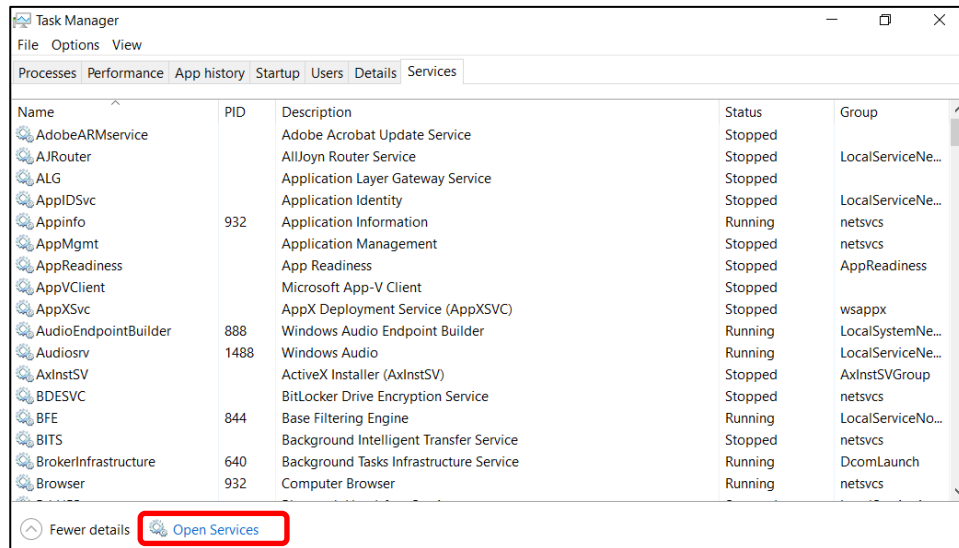
The screenshot shows the Windows 11 Task Manager interface with the 'Processes' tab selected. The window title is 'Task Manager' and the search bar contains 'Type a name, publisher, or PID...'. The 'Processes' tab is active, showing a list of running processes with columns for Name, Status, CPU usage, Memory usage, Disk usage, and Network usage. The 'Host Process for Windows Explorer' (taskhostw.exe) is highlighted in yellow, indicating it is the active process. Other processes include 'Google Chrome (21)', 'Microsoft PowerPoint (2)', 'Microsoft Teams (21)', 'Task Manager', and 'Windows Explorer'.

Name	Status	CPU	Memory	Disk	Network
Google Chrome (21)		0%	2,068.0 MB	0.1 MB/s	0 Mbps
Microsoft PowerPoint (2)		0.1%	328.0 MB	0 MB/s	0 Mbps
Microsoft Teams (21)		0%	342.5 MB	0.1 MB/s	0 Mbps
Task Manager		0.4%	94.1 MB	0.1 MB/s	0 Mbps
Windows Explorer		0.3%	197.1 MB	0.1 MB/s	0 Mbps

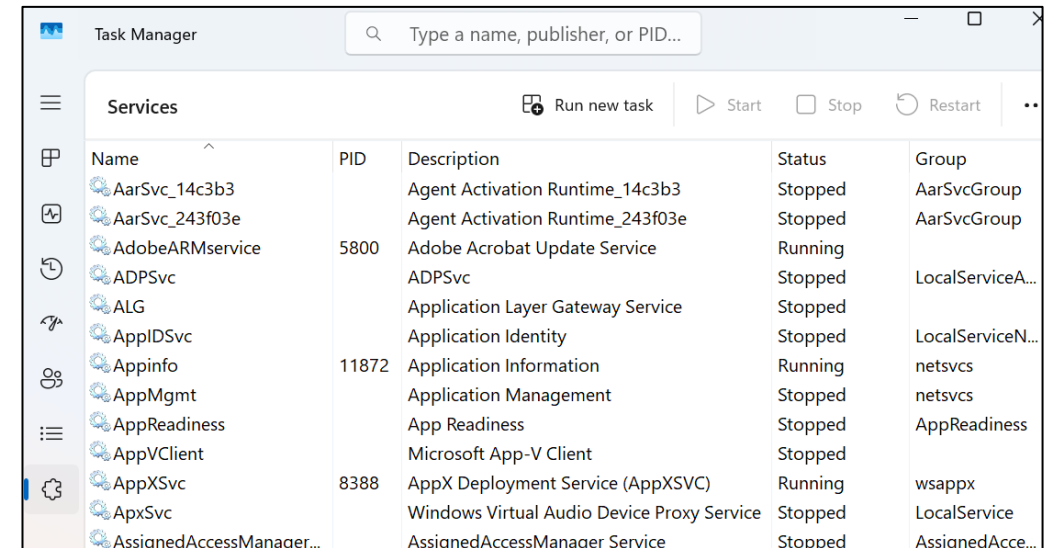
# Task Manager: Services

- List of processes running in the background
- If a service is suspect, details may be found on the internet
- To Stop an unwanted service: **Click Open Services → Right Click the service → Click Stop**

Windows 10



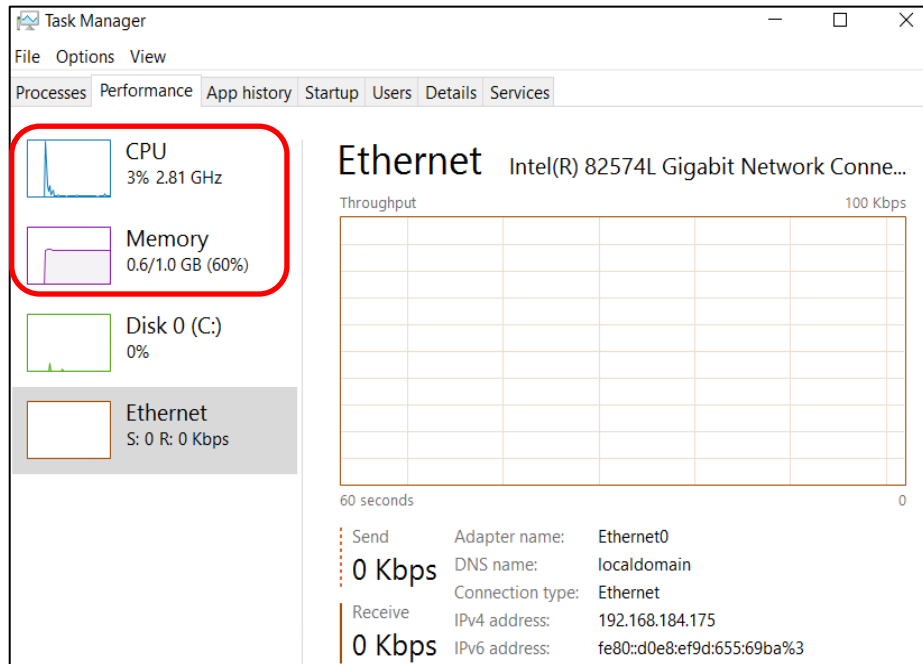
Windows 11



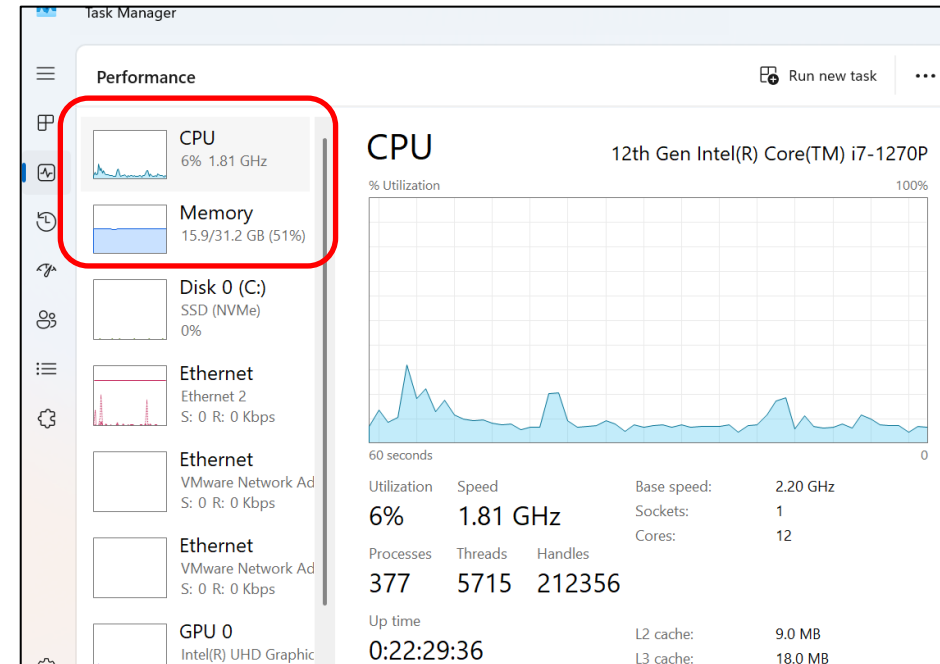
# Task Manager: Performance

- CPU: Monitors current and past resource use
- CPU usage by core
- Multi-core Processors

## Windows 10



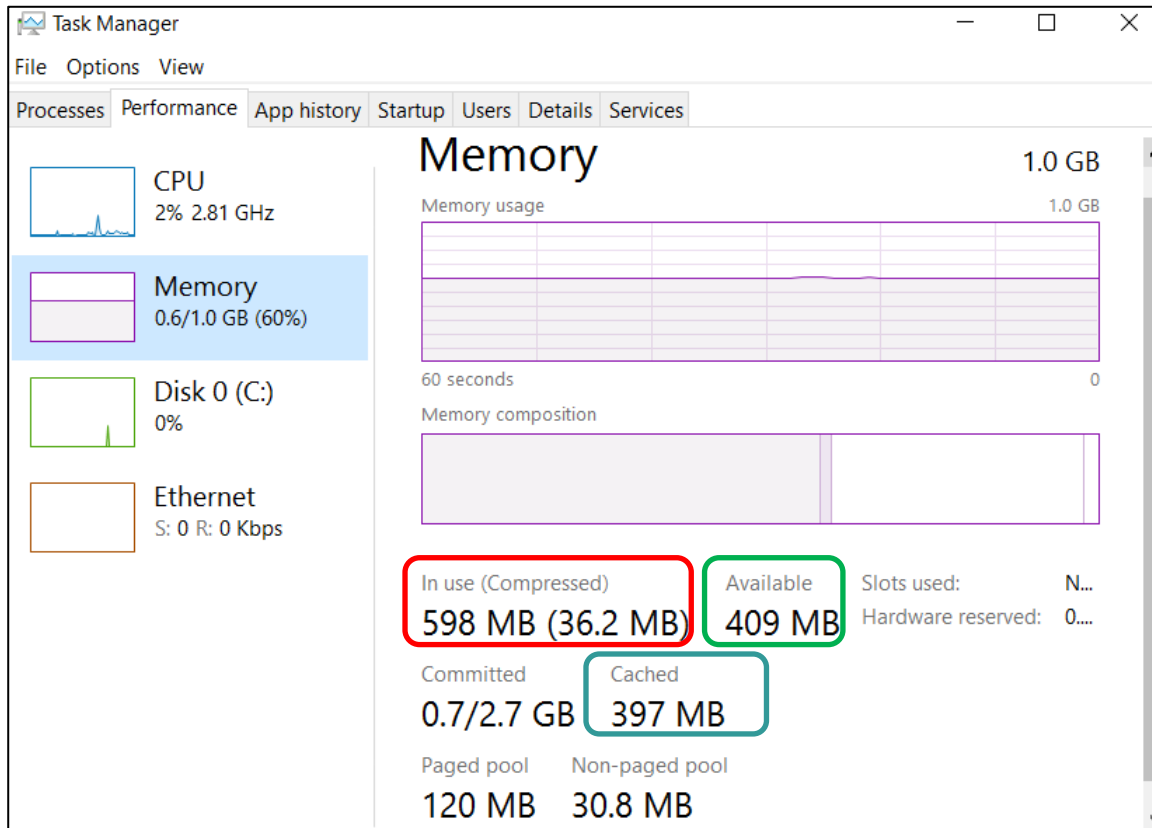
## Windows 11



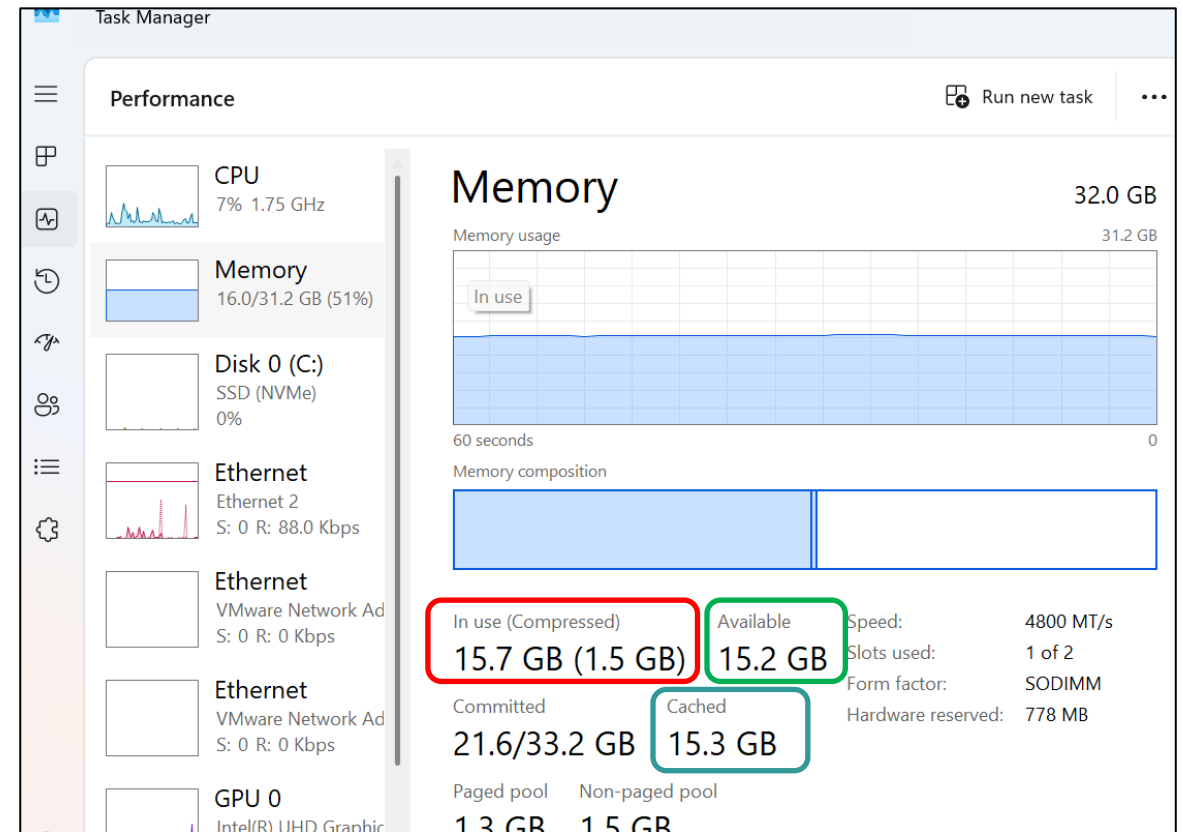
# Task Manager: Performance (cont.)

## Memory usage

### Windows 10



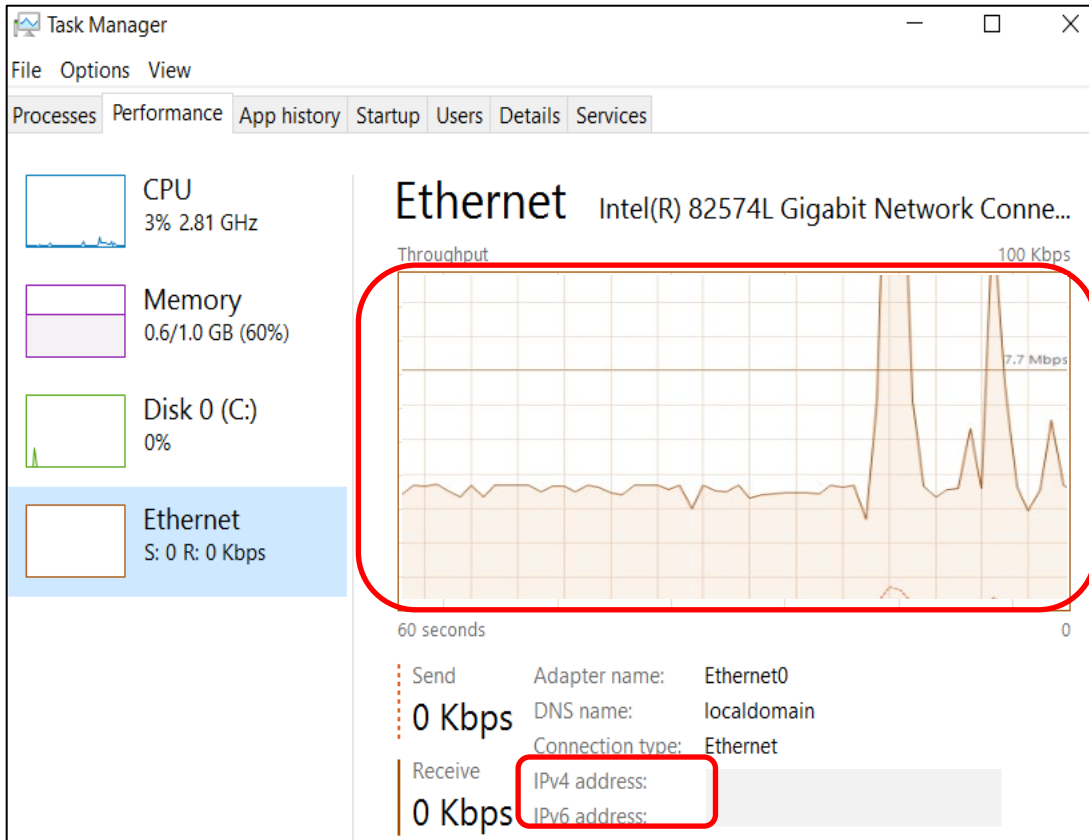
### Windows 11



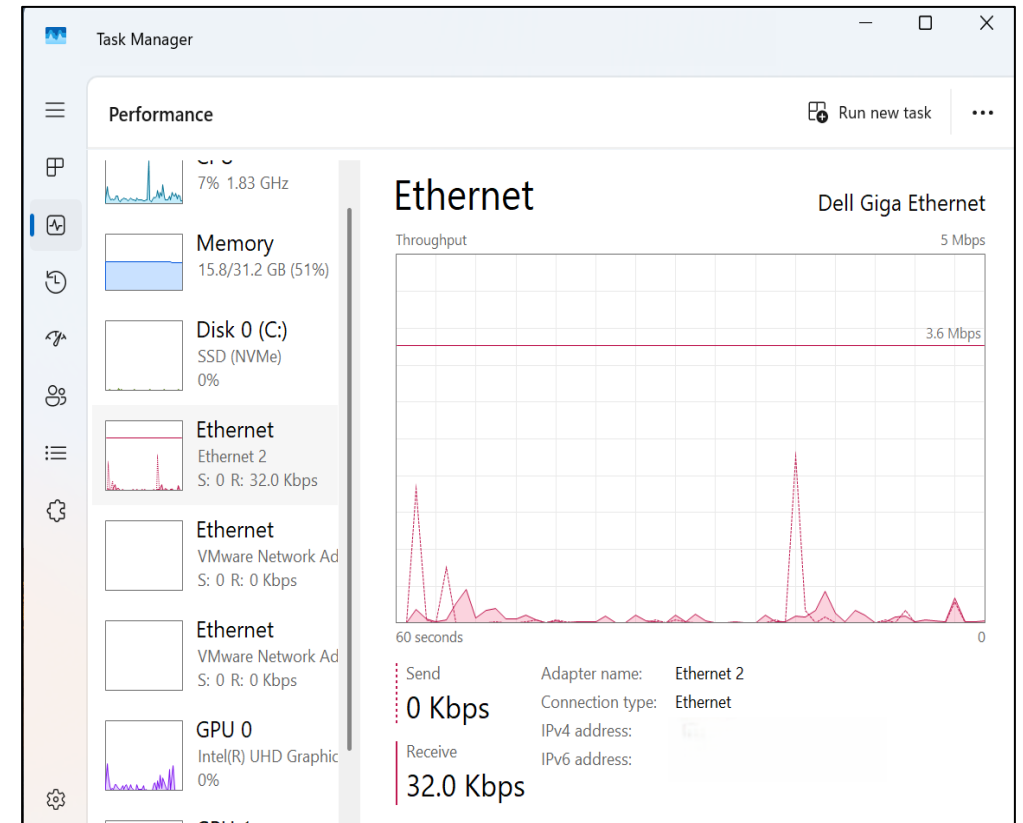
# Task Manager: Ethernet

## Graph of network usage

### Windows 10



### Windows 11





# Task Manager: Performance Tab

- Performance problems can arise from a broken router, switch, or cable, or from the computer itself
- To see resource utilization details: [Click Open Resource Monitor](#)

The image shows two screenshots from Windows. The left screenshot is the Task Manager Performance tab, displaying CPU usage at 14% on a 3.40 GHz processor. A red box highlights the 'Open Resource Monitor' button at the bottom. A red arrow points from this button to the right screenshot, which is the Resource Monitor Network tab. This tab shows a table of processes with network activity, including svchost.exe (NetworkService) and svchost.exe (LocalServiceNet...). Below the table are sections for Network Activity, TCP Connections, and Listening Ports. On the right side of the Resource Monitor window, there are three graphs: Network (10 Kbps), TCP Connections (10), and Ethernet0 (100%).

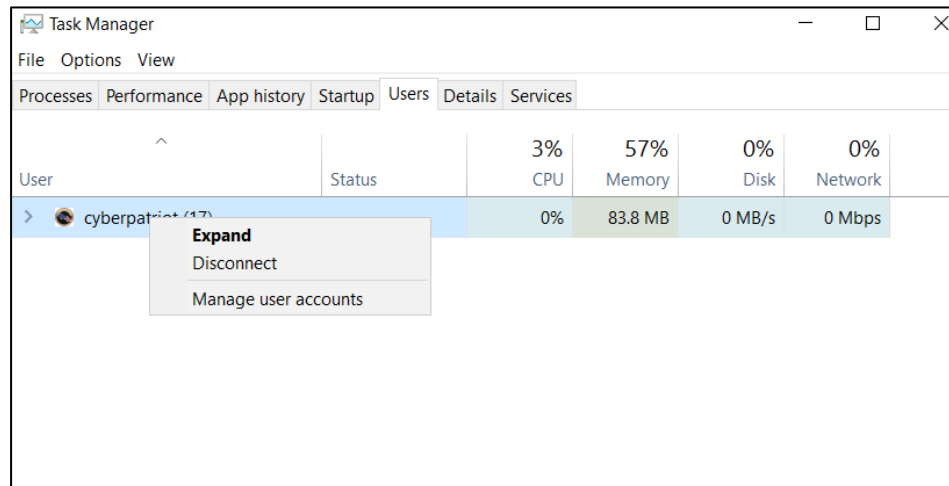
Process	PID	Send (B/sec)	Receive (B/sec)	Total (B/sec)
Image				
CCSCClient.exe	1868	35	28	63
svchost.exe (NetworkService)	1148	10	5	15
System	4	5	0	5
svchost.exe (LocalServiceNet...)	896	3	0	3
svchost.exe (netsvc)	856	1	0	1

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

# Task Manager: Users

- List of logged-in users
  - Disconnect
  - Logoff

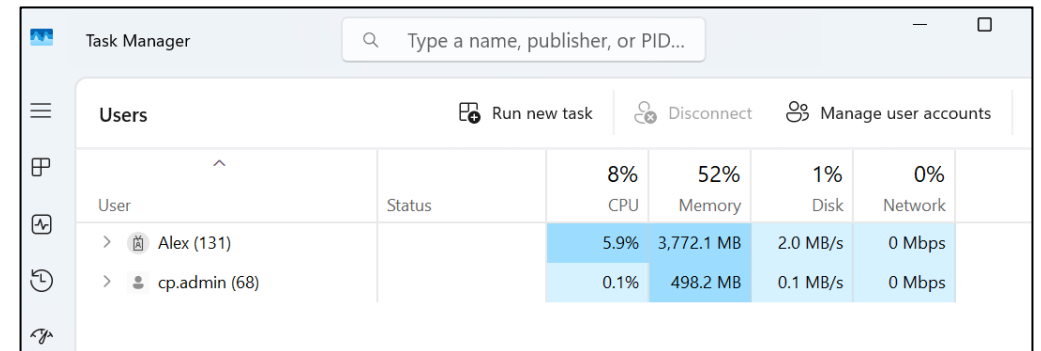
## Windows 10



The screenshot shows the Windows 10 Task Manager window with the 'Users' tab selected. A context menu is open over the 'cyberpatriot (17)' user entry, showing options: 'Expand', 'Disconnect', and 'Manage user accounts'. The table below shows the resource usage for the logged-in user.

User	Status	3% CPU	57% Memory	0% Disk	0% Network
> cyberpatriot (17)		0%	83.8 MB	0 MB/s	0 Mbps

## Windows 11

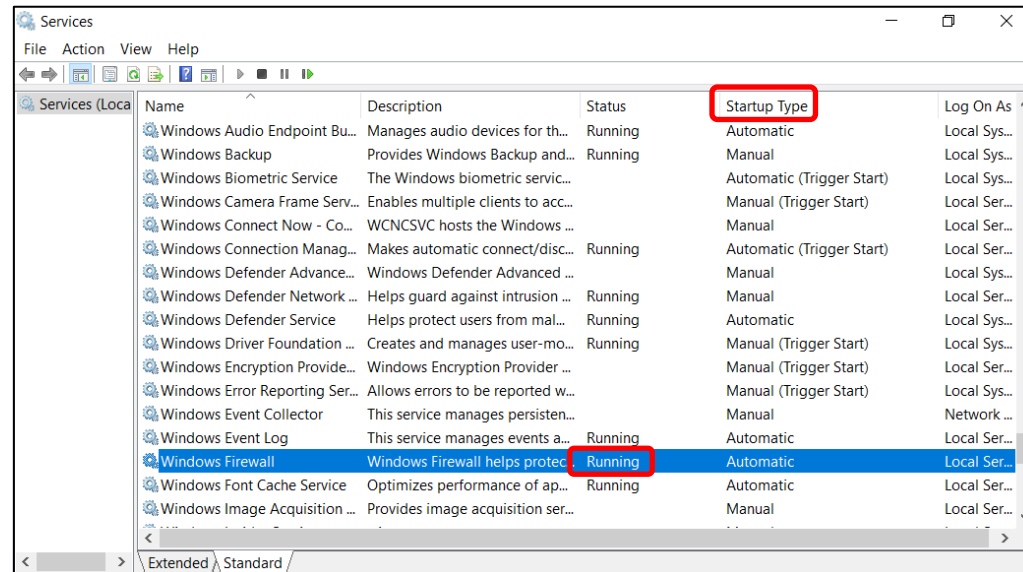


The screenshot shows the Windows 11 Task Manager window with the 'Users' tab selected. The interface includes a search bar at the top and buttons for 'Run new task', 'Disconnect', and 'Manage user accounts'. The table below shows the resource usage for two logged-in users.

User	Status	8% CPU	52% Memory	1% Disk	0% Network
> Alex (131)		5.9%	3,772.1 MB	2.0 MB/s	0 Mbps
> cp.admin (68)		0.1%	498.2 MB	0.1 MB/s	0 Mbps

# Services – Not In Task Manager

- Search → Services.msc
- Programs that run invisibly and automatically in the background
- Running vs. Stopped Services
- Startup Type:
  - Automatic
  - Manual
  - Disabled



# Services – Not In Task Manager

- Two reasons to disable services:
  - Unnecessary for your organization
  - Insecure
- The most insecure services are those that allow remote connections
- Example: Remote Desktop Protocol

Search → Services.msc

