



Educate
Engage
Inspire



Presented by

**NORTHROP
GRUMMAN**

In partnership with



Module 6

Microsoft Windows security configuration

cybertairan.csiro.au



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*
- *Customisation*

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 1

Windows files protections

Review: The CIA Triad

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 customisable than the blanket set of permissions given to users by adding them to either the Users or Administrators group.

Used to restrict access or editing rights to specific data on shared resources.

Can be customised by individual user or by user group.

[Click the System Settings button in the menu bar.](#)

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 and 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.

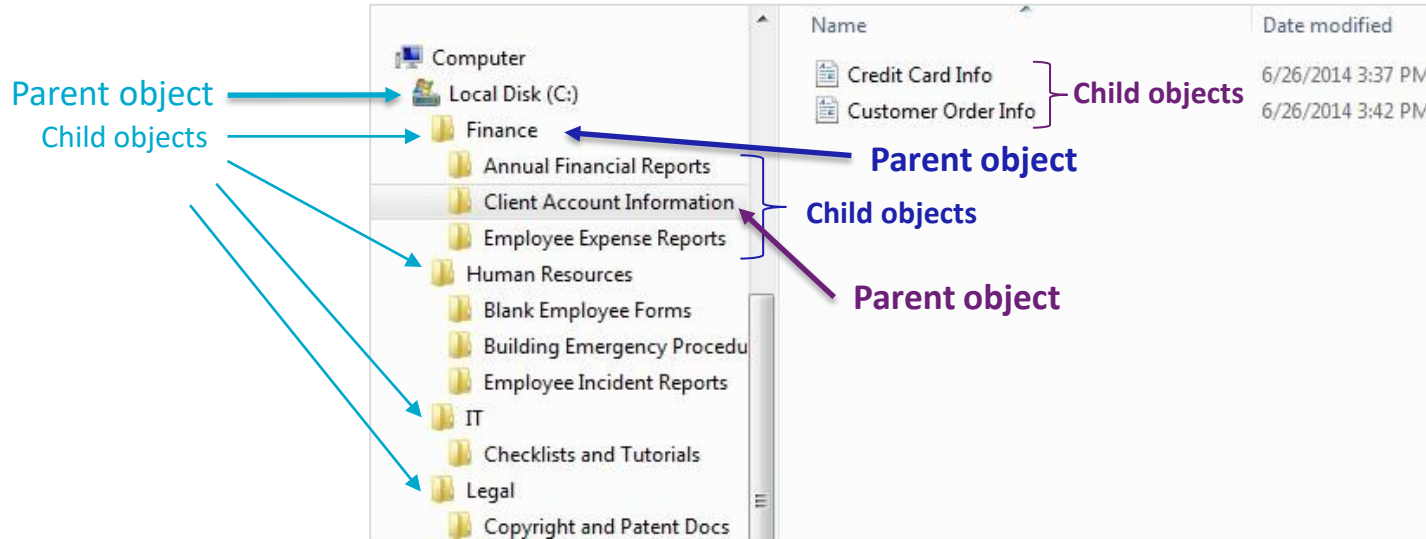
Read

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).



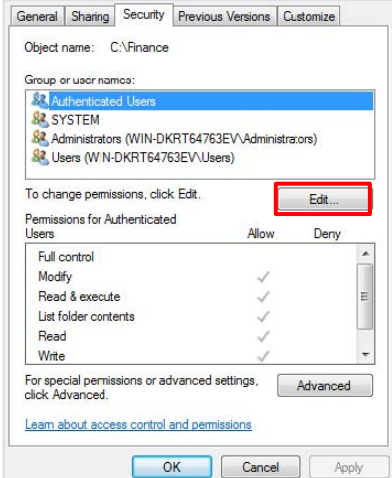
Inheritable permissions

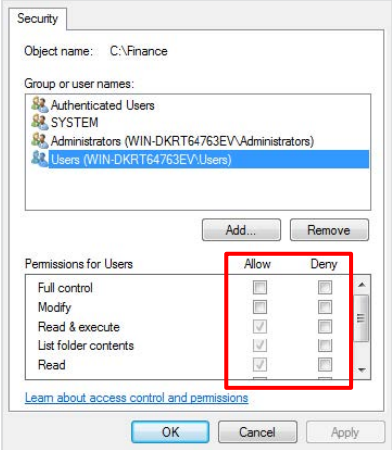
- By default, objects within a folder (known as child objects) inherit permission settings from their containing folder (known as the parent object).
- You can turn off inheritable permissions and customise who gets what kind of access to certain folders, subfolders, or documents.
- Depending on how 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.

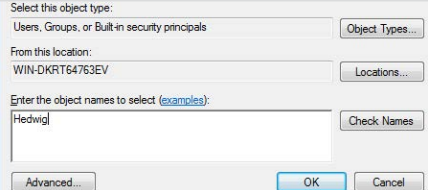
E.g. If you want certain users or groups to be denied access to all but a few files within a folder, it is quickest to apply a restrictive permission setting to the parent object (folder). Once you have denied those users' access to all of the files in the folder, you can go to the individual files you do want them to have access to and override the permissions those files inherited from the parent folder.

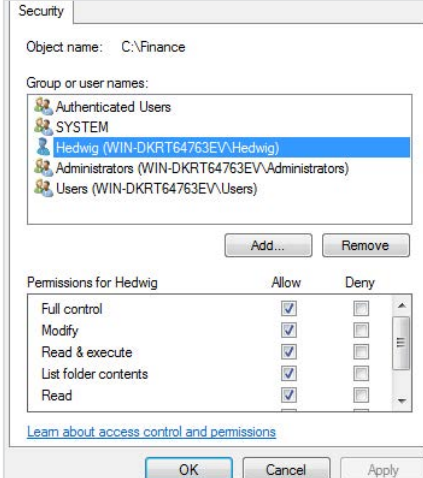
Customising permissions

- 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 them to the Group or Usernames box and then checking the appropriate boxes.

1. 

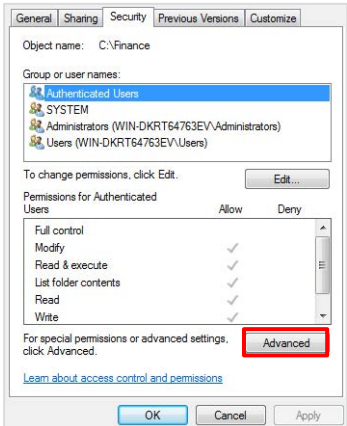
2. 

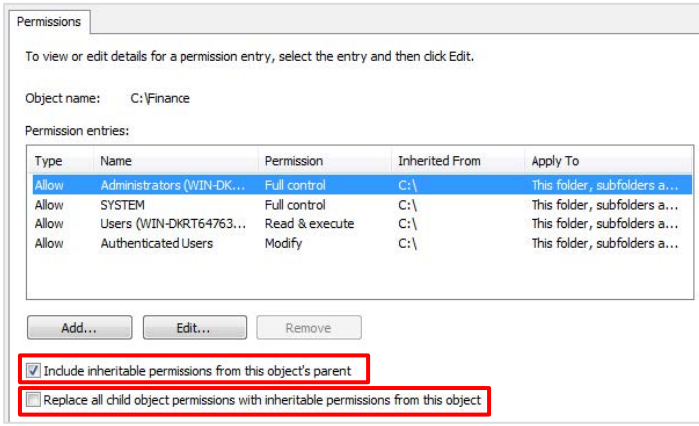
3. 

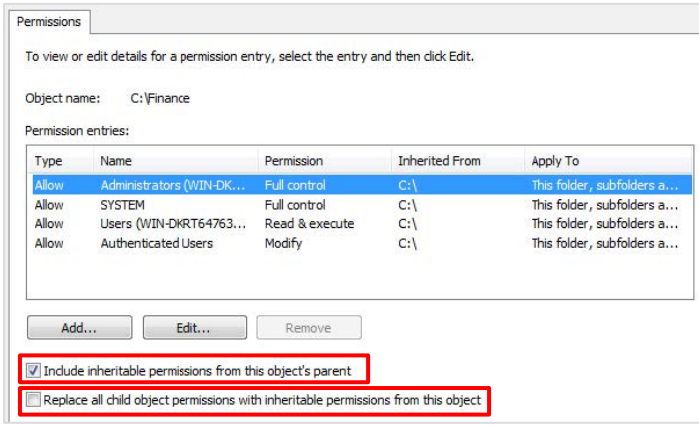
4. 

Customising 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.
- Customise permissions for individual users and/or groups using the 'Add...' button.
- To extend your new settings to all of the child objects or to extend permissions to the child objects in a folder, check the 'Replace all child objects....' button.

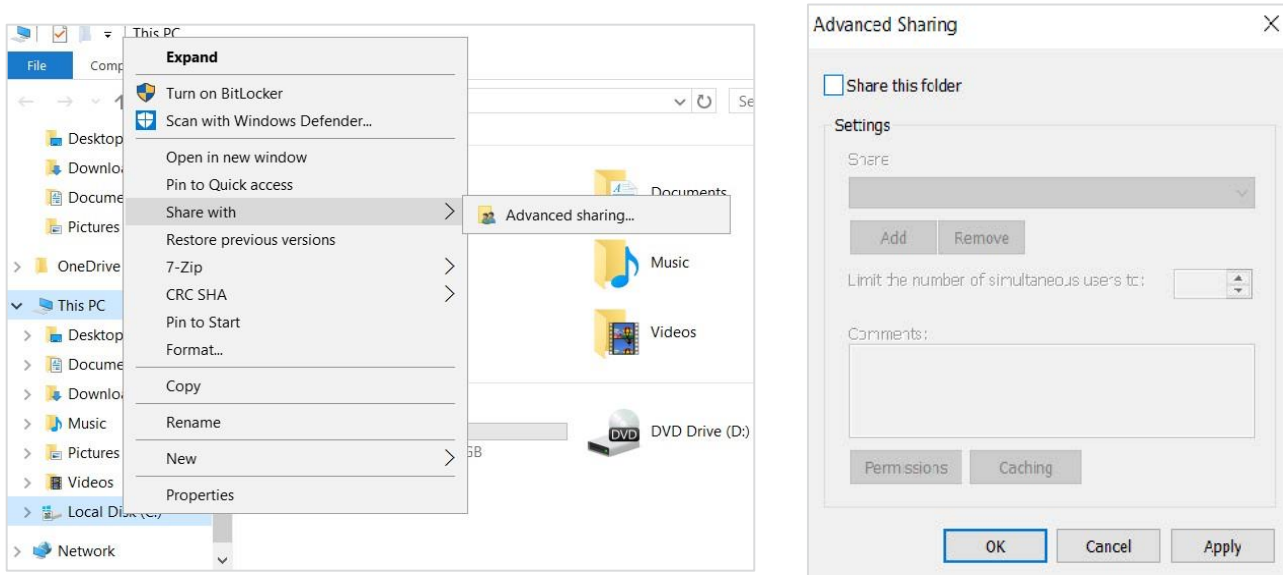
1. 

2. 

3. 

Sharing drives

- You can share an entire network's files by sharing its drives.
- Generally not a good idea.
- Anyone would be able to see or modify your files.



File permissions

Restrict access or editing rights to data on shared resources.

Types of permissions:

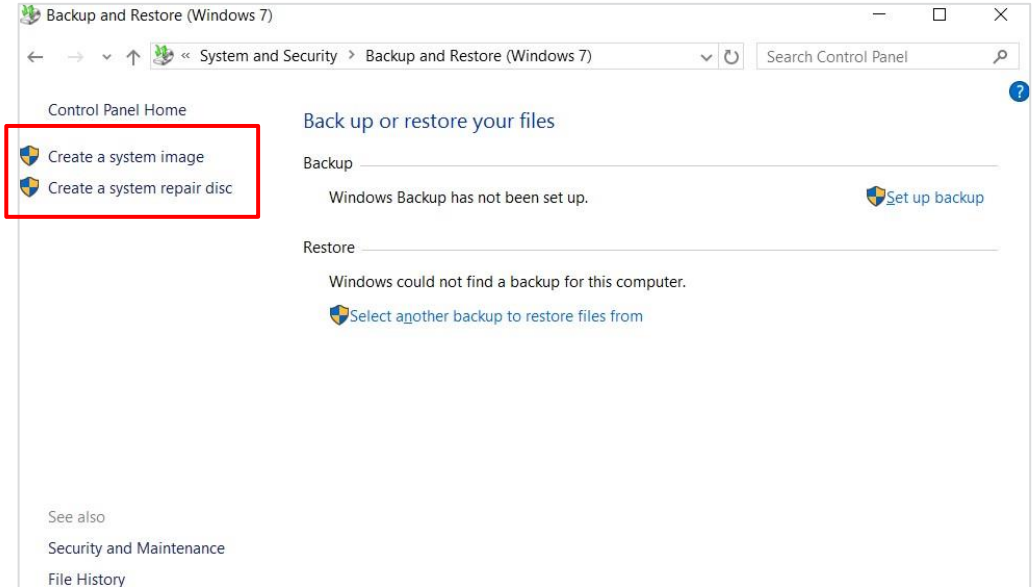
1. Full Control
2. Modify
3. Read and Execute
4. List Folder Contents
5. Write
6. Read

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.



Section 2

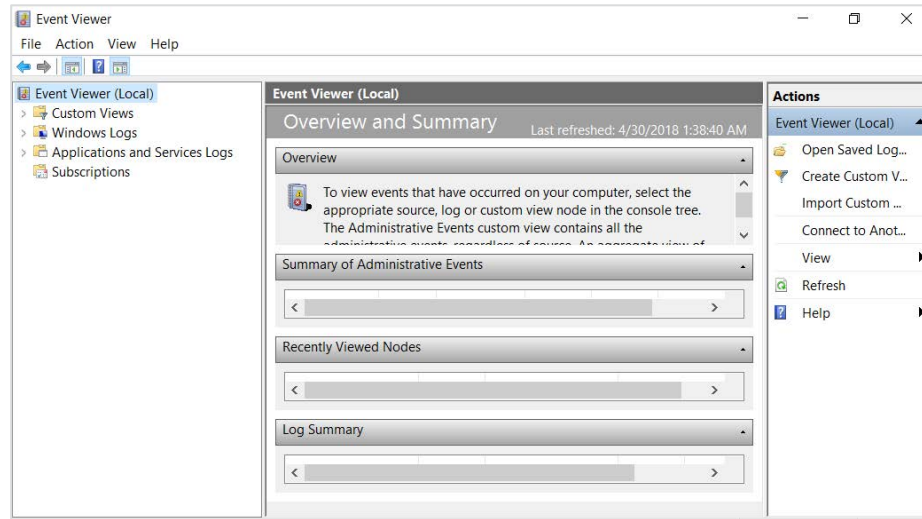
Windows auditing and monitoring

Event Viewer

Displays logs of events occurring on the Windows operating system.

Control Panel → System and Security → Administrative Tools → Event Viewer

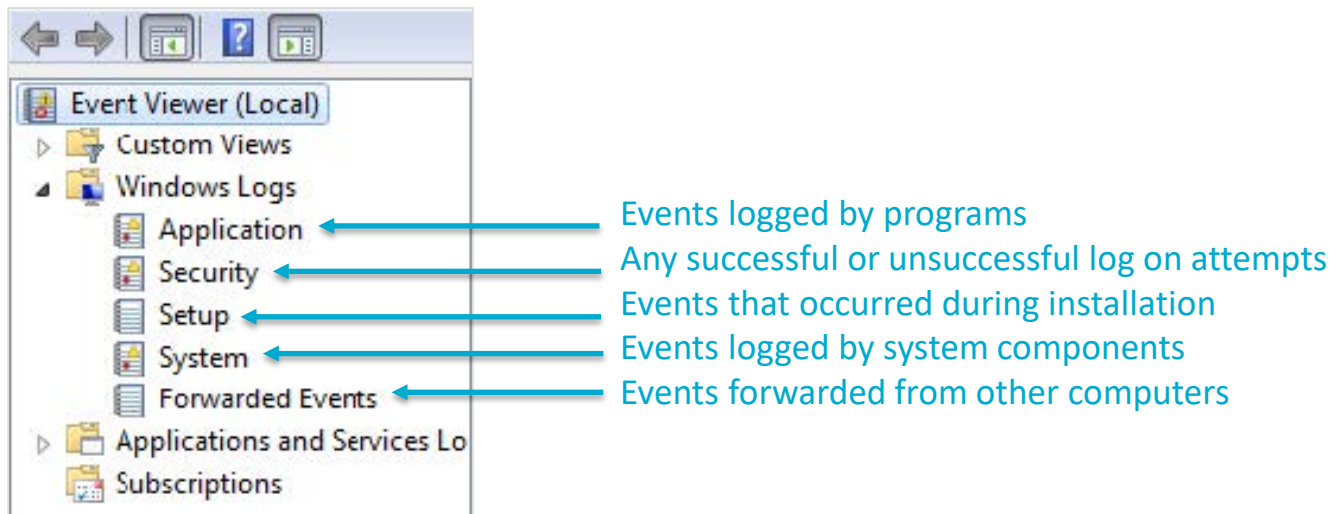
OR Search → Event Viewer



Windows Logs

Security logs can be a useful last defence against attacks and a tool for forensics investigations into the source of a past attack or unauthorised entry.

Customise what security logs are kept by setting [Audit Policies](#).



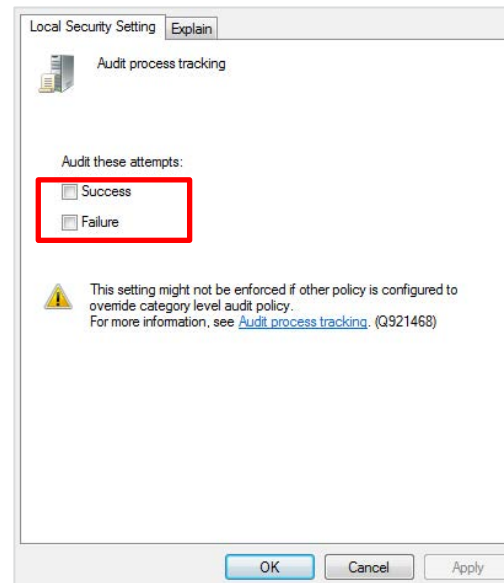
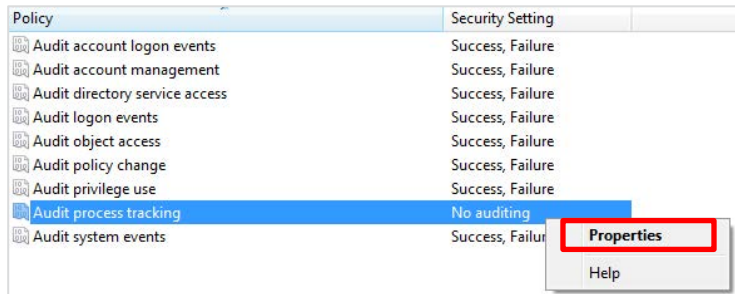
Audit Policy Settings

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

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

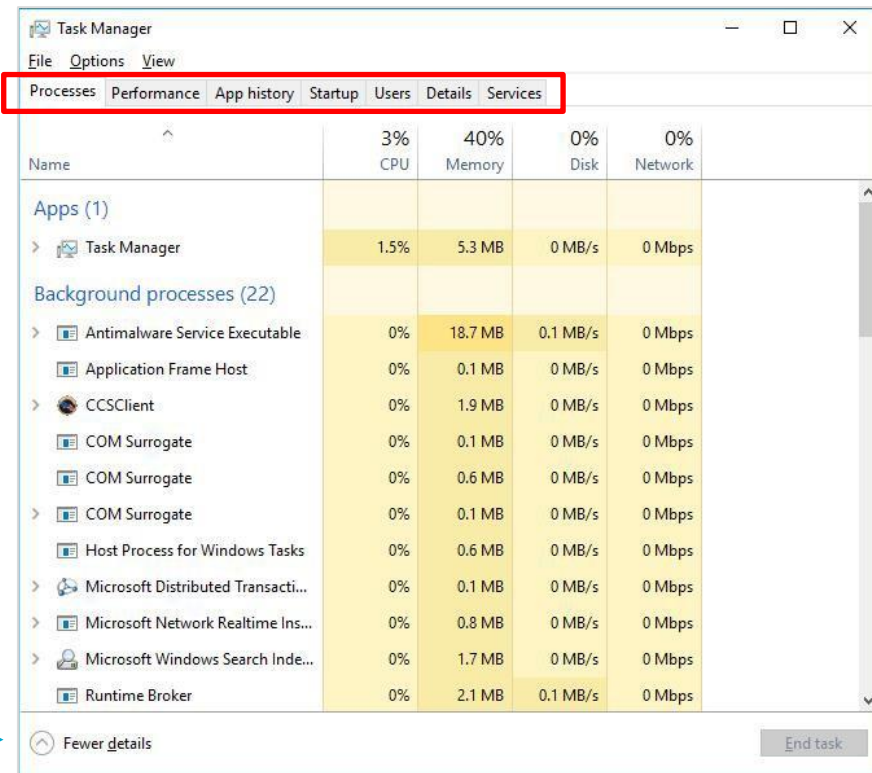
Task Manager

Shows programs, services and processes currently running.

Shows network activity and resource utilisation.

[Search](#) → Task Manager

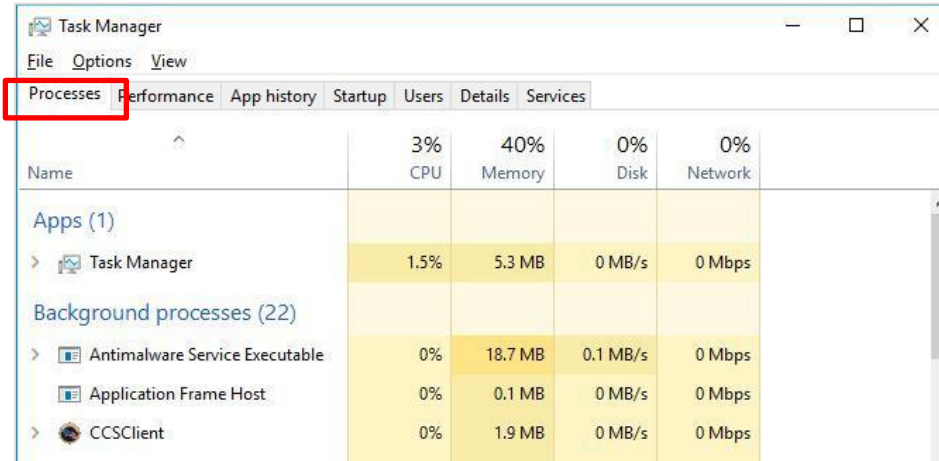
Note: If the Task Manager is showing few details, then click 'More details' here.



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.

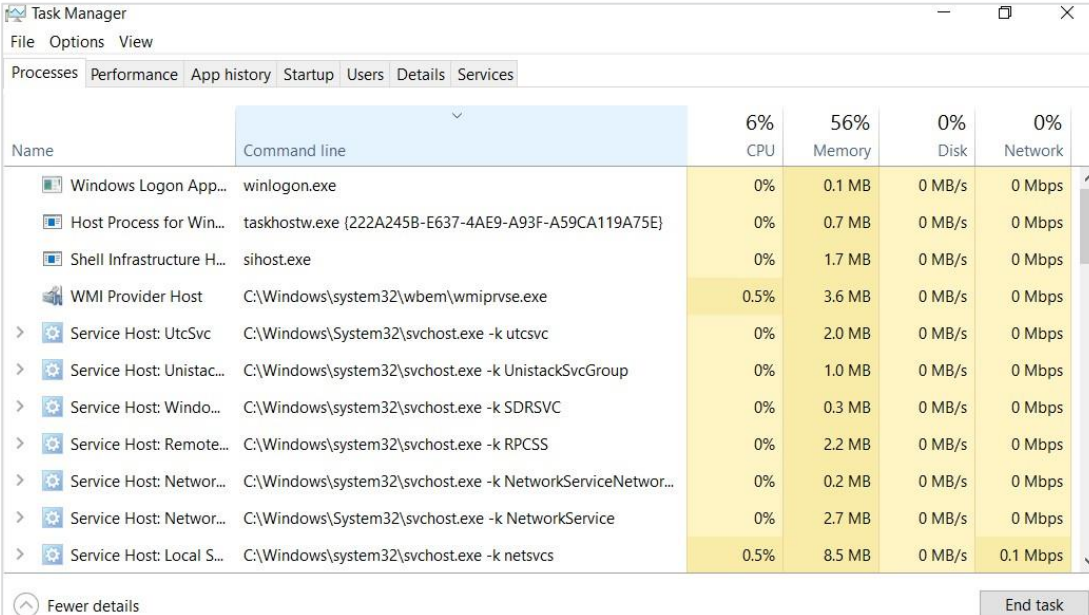


Task Manager				
File Options View				
Processes Performance App history Startup Users Details Services				
Name	3% CPU	40% Memory	0% Disk	0% Network
Apps (1)				
> Task Manager	1.5%	5.3 MB	0 MB/s	0 Mbps
Background processes (22)				
> Antimalware Service Executable	0%	18.7 MB	0.1 MB/s	0 Mbps
Application Frame Host	0%	0.1 MB	0 MB/s	0 Mbps
> CCSCClient	0%	1.9 MB	0 MB/s	0 Mbps

Task Manager: Processes

Some processes essential for Windows.

Some malware can only be ended here.



Name	Command line	6% CPU	56% Memory	0% Disk	0% 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

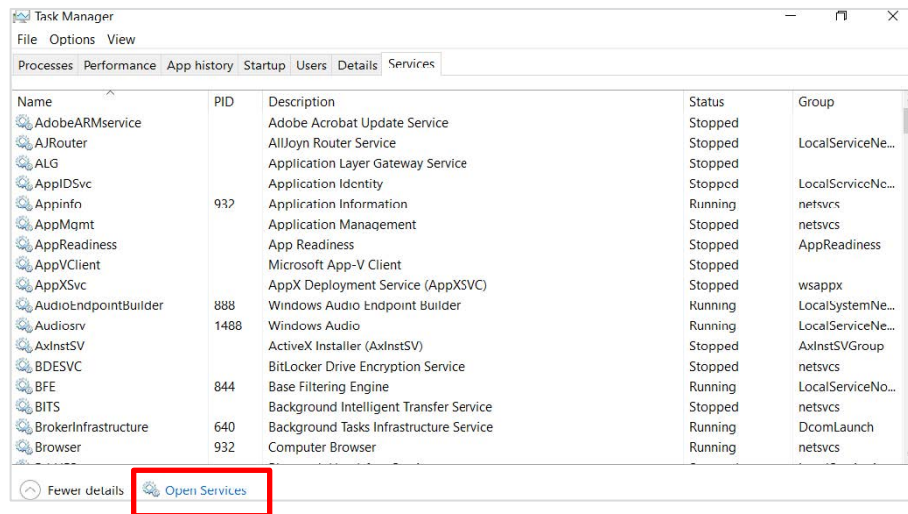
Task Manager: Services

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

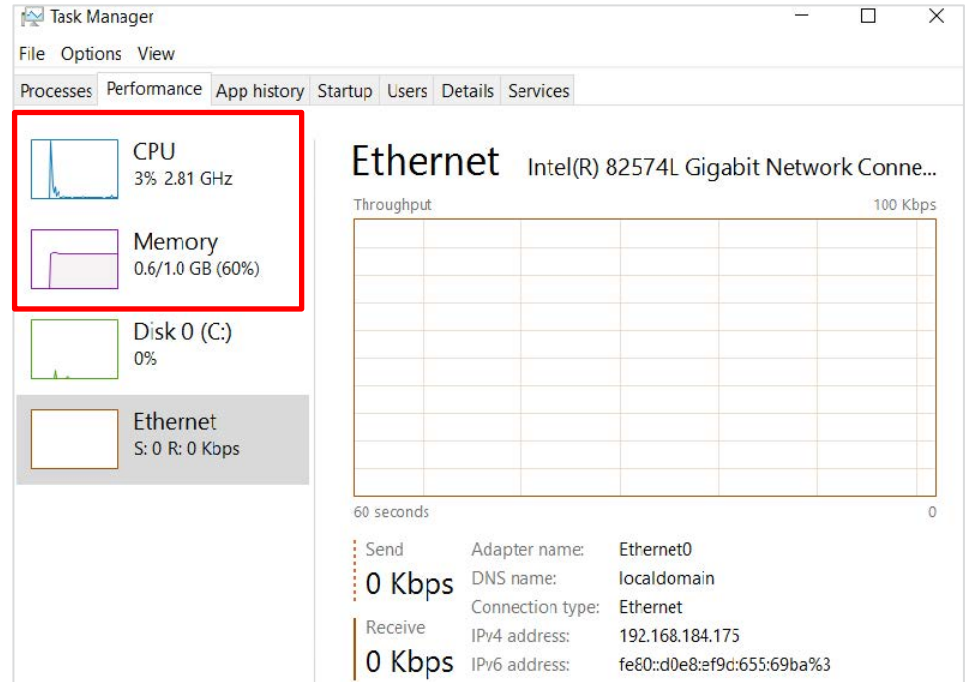


Task Manager: Performance

CPU: Monitors current and past resource use.

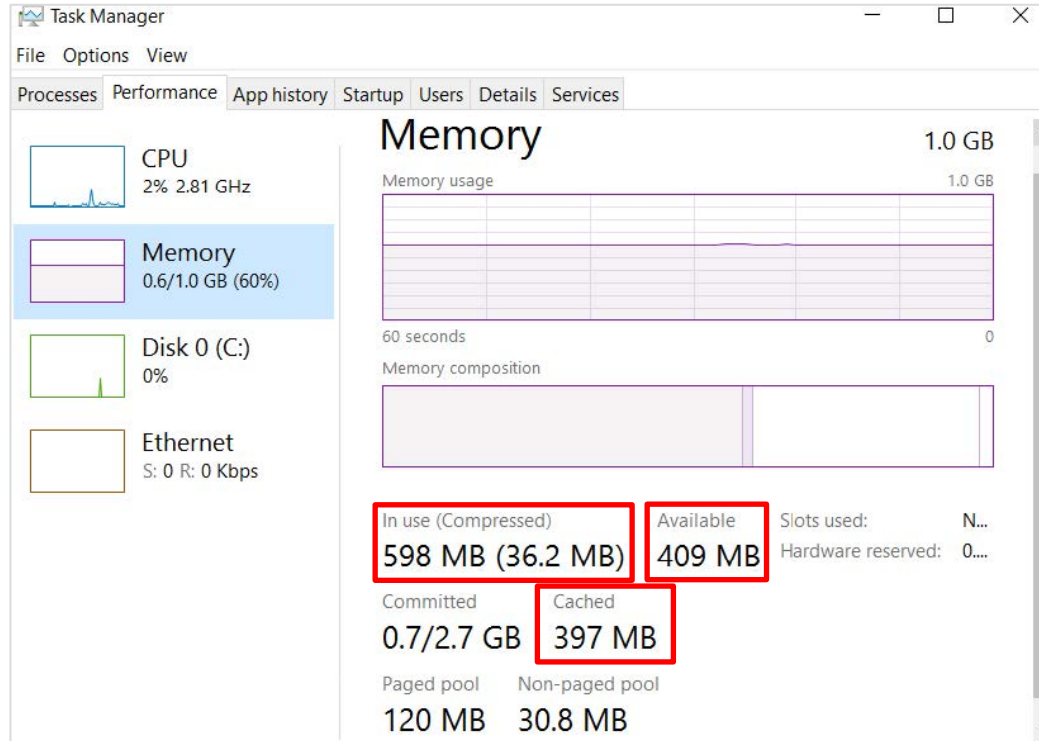
CPU usage by core.

Multi-core Processors.



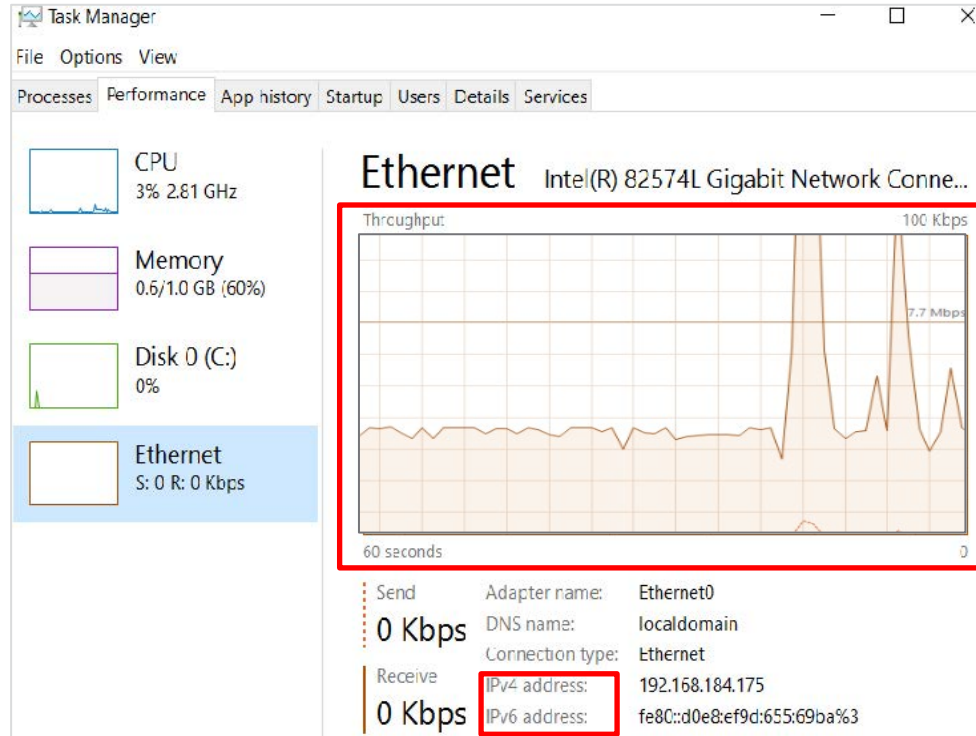
Task Manager: Performance

Memory usage:



Task Manager: Ethernet

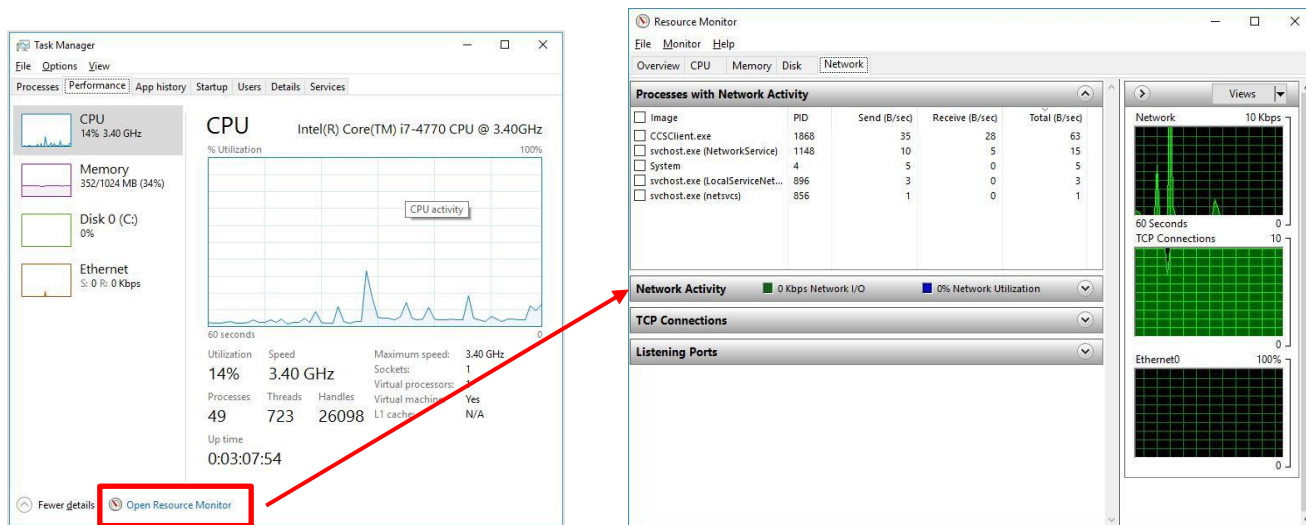
Ethernet usage:



Task Manager: Performance tab

Performance problems can arise from a broken router, switch, or cable, or from the computer itself.

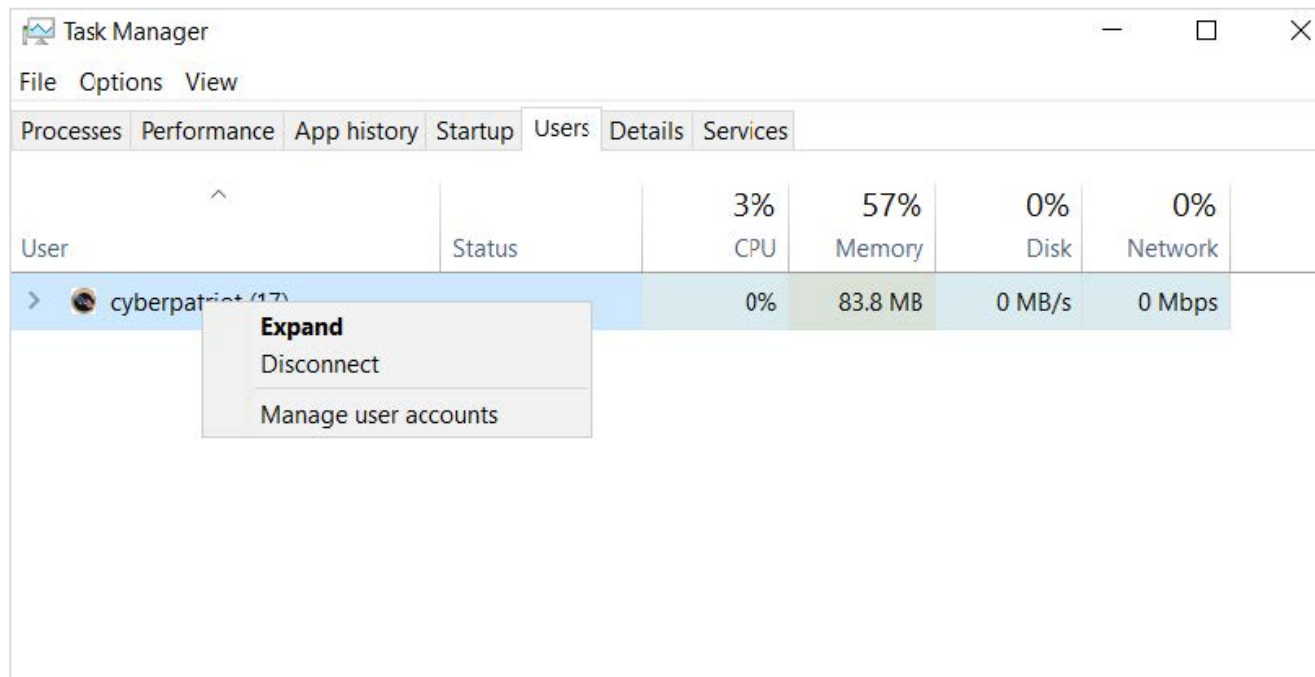
To see resource utilisation details: [Click Open Resource Monitor](#)



Task Manager: Users

List of logged-in users

- Disconnect
- Logoff



Services (Not In Task Manager)

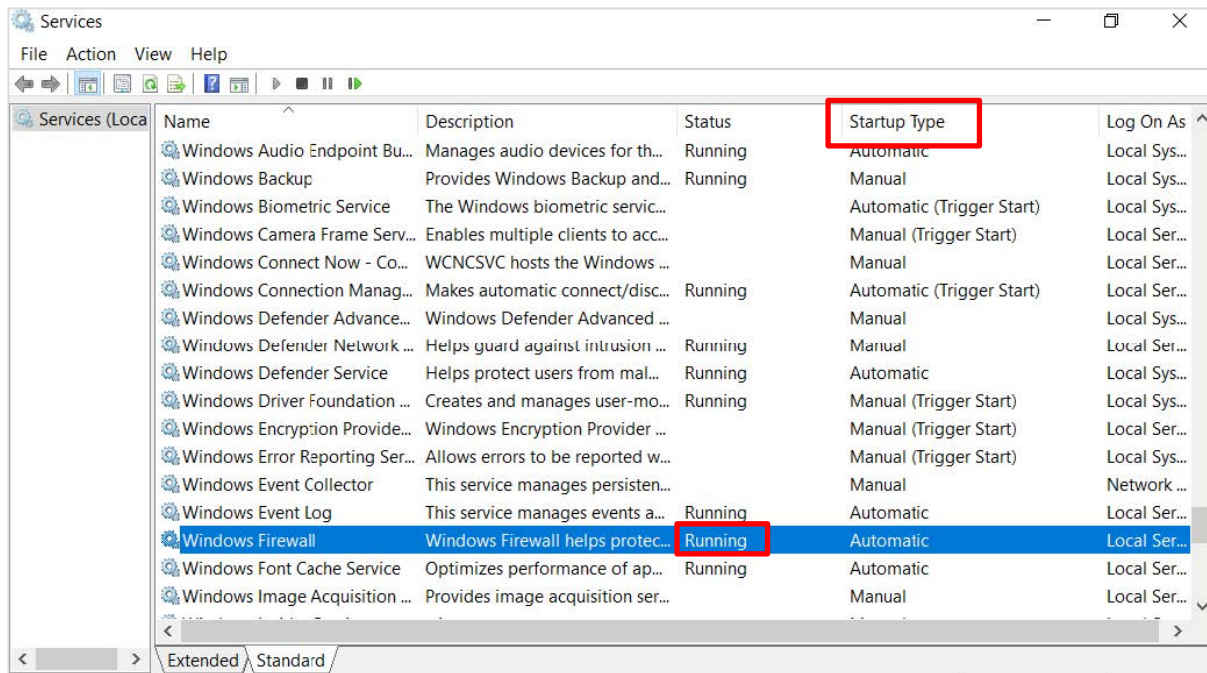
Search → [Services.msc](#)

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 organisation
- Insecure

The most insecure services are those that allow remote connections.

Example: Remote Desktop Protocol

Search → [Services.msc](#)

