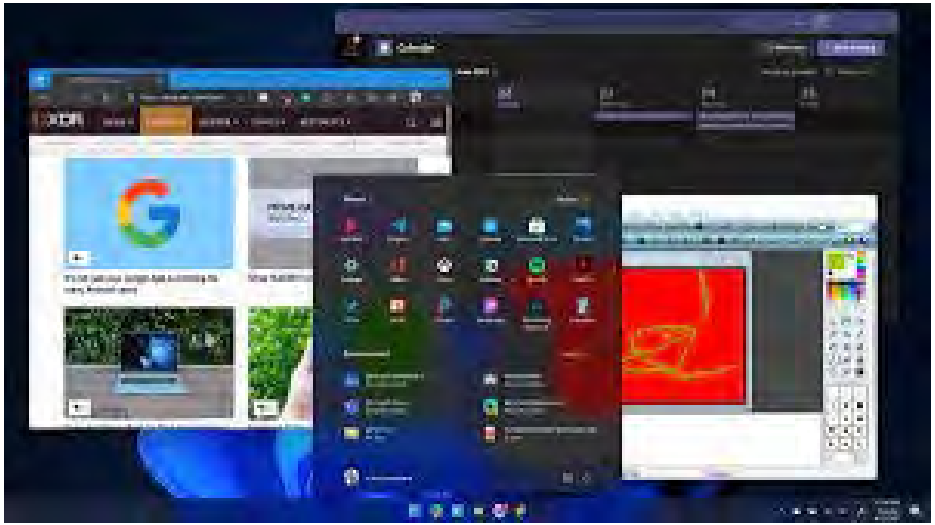
CH 3: Tools to Troubleshoot and Maintain

- Install and Manage Windows Applications
- Manage Windows Performance
- Troubleshoot Windows

Topic A: Install and Manage Windows Applications



Application Installation and Configuration

- OS requirements:
  - Software build for macOS will not run-on Windows.
  - Some applications might not be supported in newer operating systems.
- System requirements:
  - CPU & GPU speed
  - RAM & Disk space
- Installation and deployment:
  - Distribute ran from a USB drive or download from the Internet.
- Permissions and other security considerations:
  - Granted read/execute permission.
  - Ensure that software is from trusted sources.

Windows Programs and Features

- Applications install to the Program Files directory.
  - Data files install to the user home directory or All Users directory.

- 64-bit Windows and 32-bit Applications.
  - Applications are installed to the Program Files (x86) directory.
  - 64-bit shared system files are stored in %SystemRoot%\system32.
  - 32-bit shared system files are stored in %SystemRoot%\syswow64.

- Use setup app for the program to install it.
  - Exit other applications.
  - Might need to disable anti-virus software during installation.

- Use Programs and Features to repair or uninstall applications.

Dedicated graphics card or integrated

- Dedicated graphics card or integrated?
  - Dedicated is required for - graphics design, or gaming
  - Integrated in CPU or chipset for- internet browsing or movies
  - Adapter graphics cards can be integrated into a motherboard, or even a USB adapter
  - Video RAM requirements

External hardware token requirements

- External hardware token requirements
  - An app might have a requirement for using a more secure authentication method than a simple password
  - External hardware tokens are smart cards or USB device that stores some cryptographic user identification data.
  - User must present the token and supply a password, PIN, or fingerprint
  - 2FA authentication

Other Considerations

- Shadow IT and impact to business
  - Licensing/compliance
  - User training and education
  - Increased support requirements
  - IOT connecter to corporate NW (shadow IT)

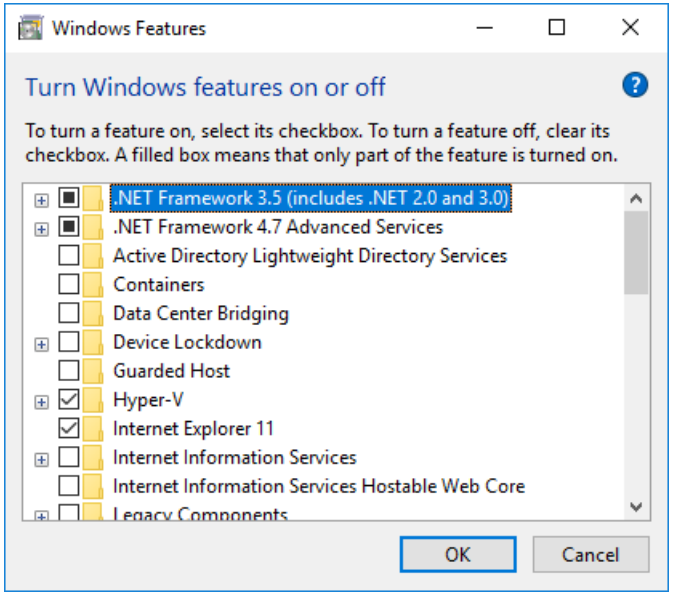
always ckeck the license before doing any installiation
trhis in a acorpreet inoviroment

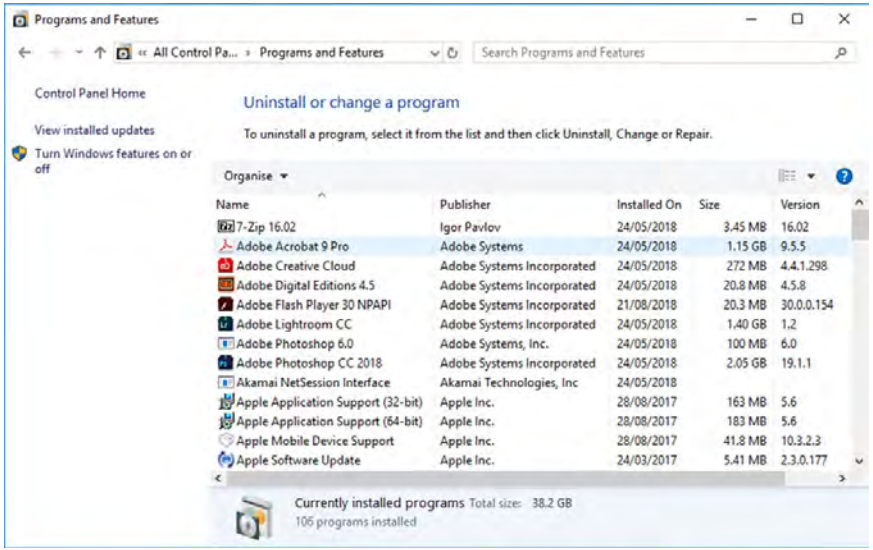
- Impact to operation
  - Deployment and support tools - GPO to deploy applications users do not have to log on to the local client with administrator privileges.
  - Easy Roll-Back’s

- Impact to device and network
  - Resource consumption/ background services
  - Risks from faulty applications – Computer virus.
  - Bandwidth usage

Windows OS Tools

- Use Programs and Features to:
  - Repair or uninstall applications.
  - Enable or disable optional Windows components.





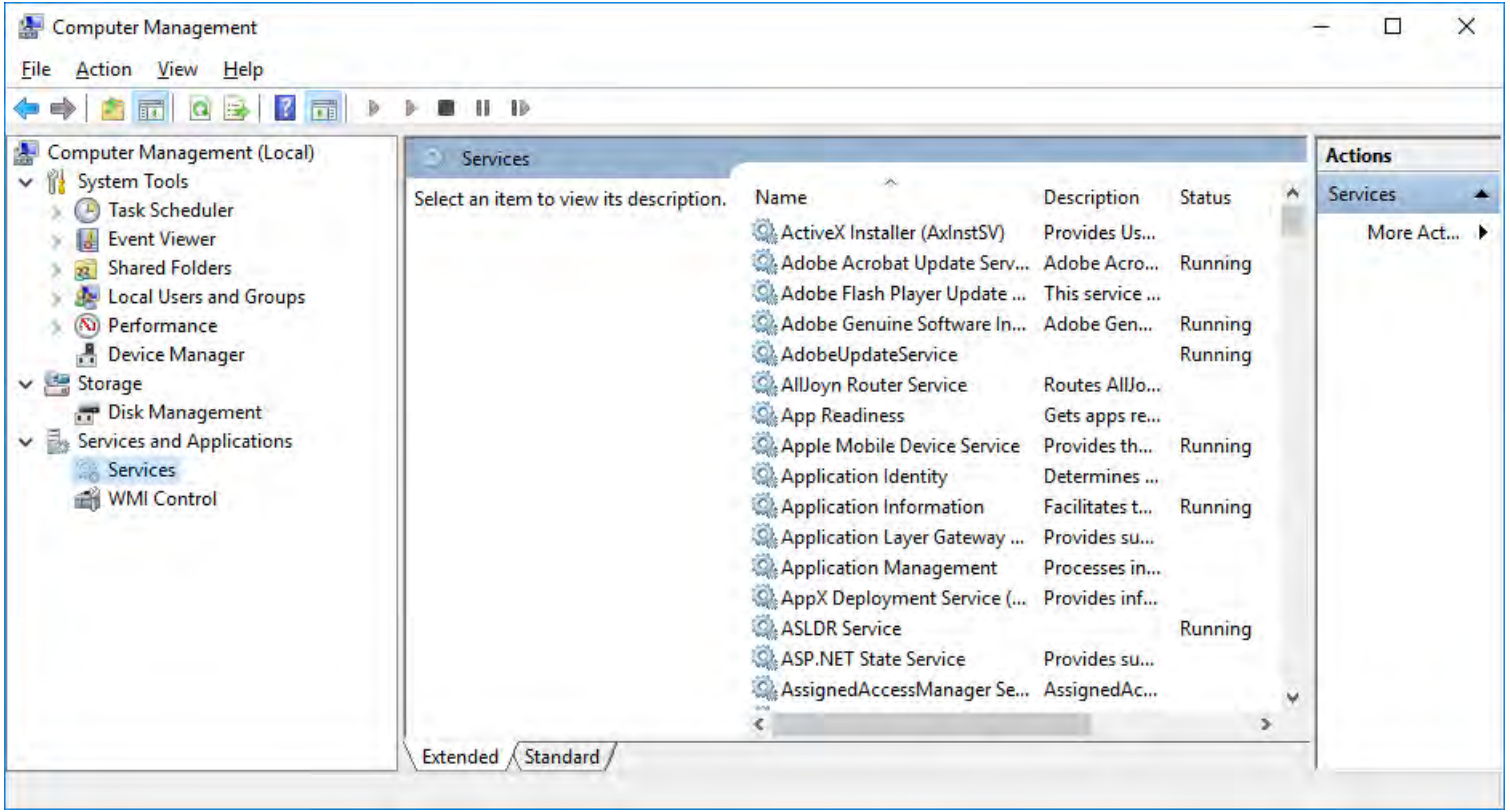
Application and Print Services

- Services provide functionality to Windows such as:
  - Logon
  - Network browsing
  - Indexing files
- Services may be installed by:
  - Windows
  - An application
    - Anti-virus
    - Database
    - Backup software

Service: Windows machines run services to provide functions.

Background: A process that runs without a window and does not require any sort of user interaction.

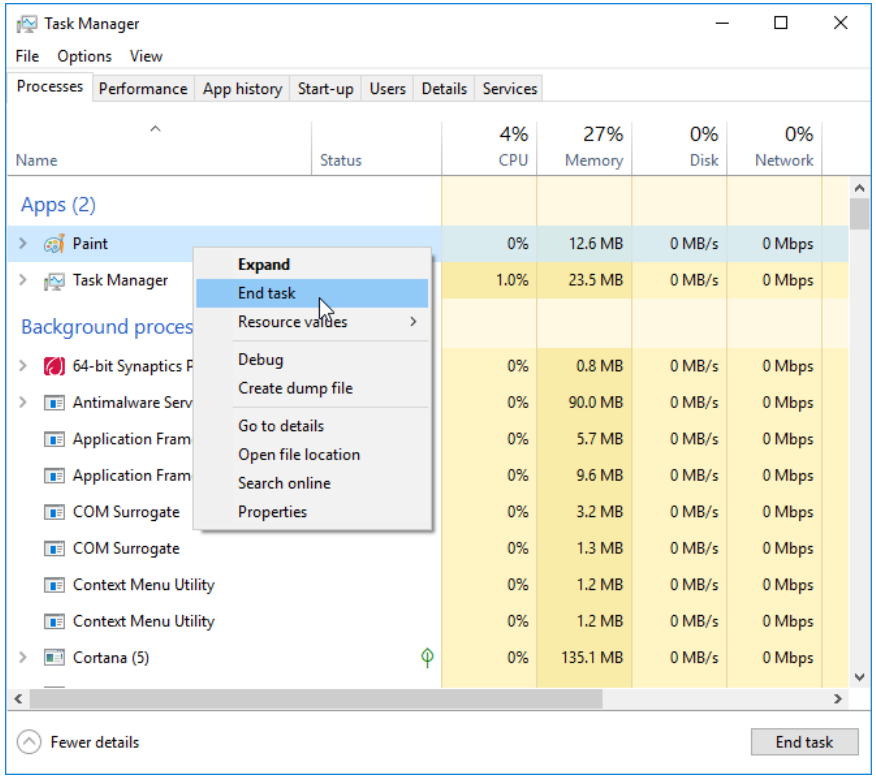
Application and Print Services

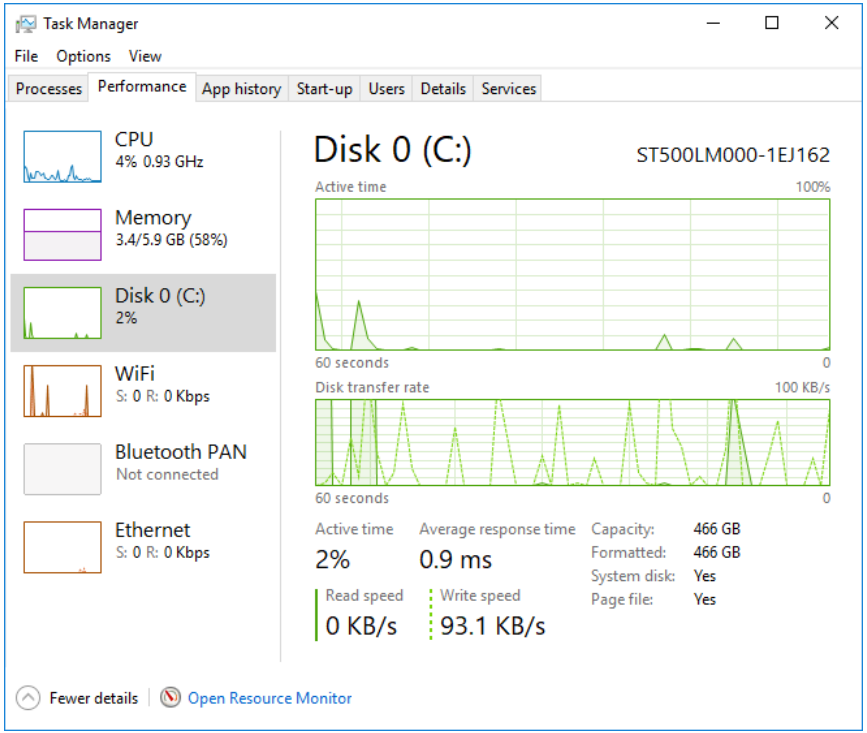


Task Manager

- Can end unresponsive application.
  - User can end items they started.
  - Administrative user must end items not started by the user.
- Can monitor system key resources.
- Open using:
  - **Ctrl+Shift+Esc**.
  - **Ctrl+Alt+Delete**, then select **Task Manager**.
  - Right-click the taskbar and select **Task Manager**.
- Significant differences between Windows 7 and Windows 8.1/10.

Task Manager



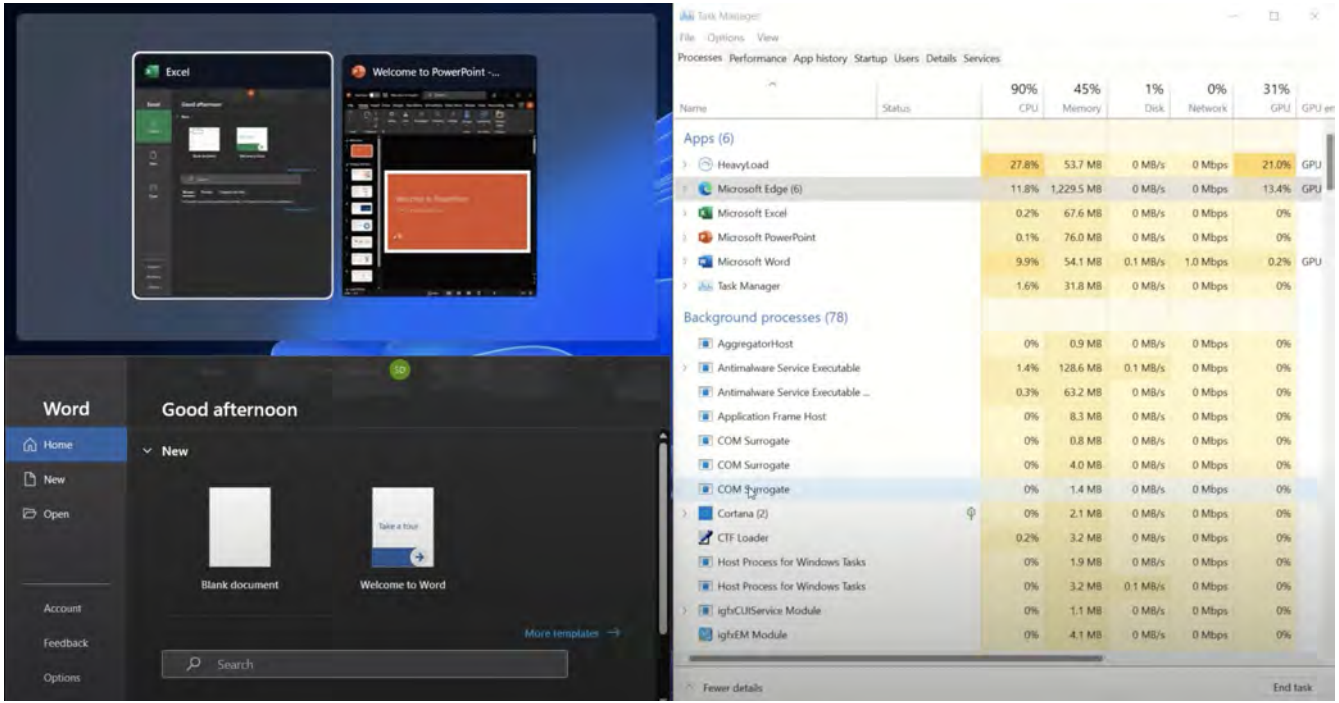


Task Manager

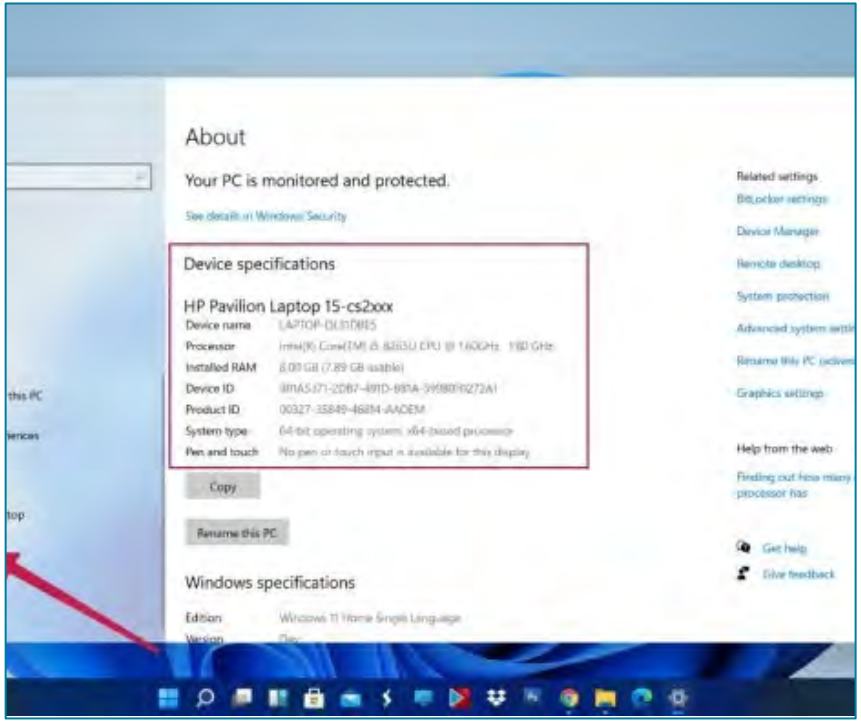
- tasklist
  - tasklist /sv
    - Shows list of services within each process

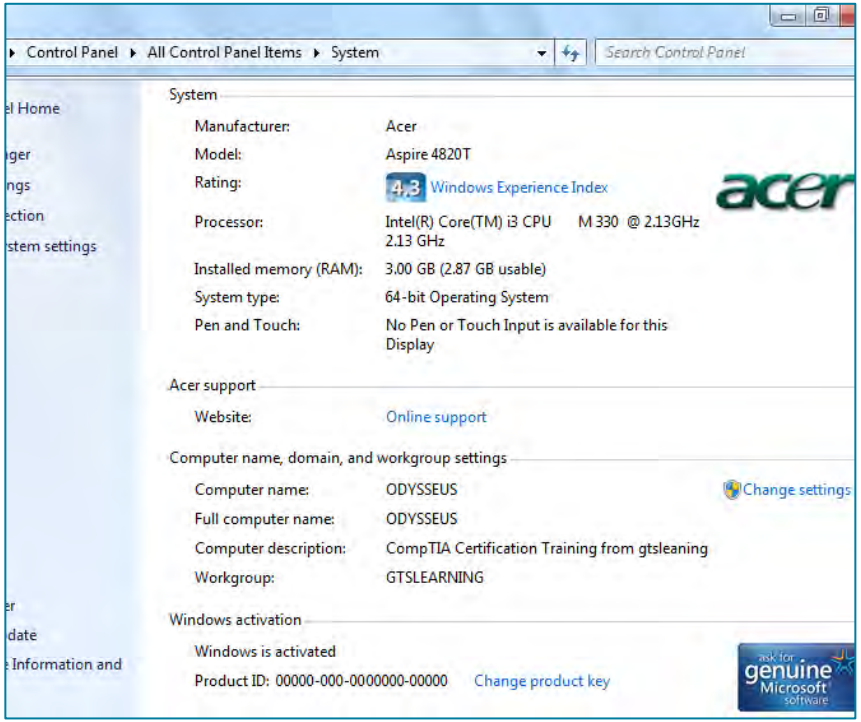
- taskkill
  - taskkill /pid *process_id*
  - taskkill /im *image_name*
  - Use /t option to halt all child processes
  - Use /f option to terminate without user notification
  - Open an administrative level command prompt to terminate Explorer

Topic B: Manage Windows Performance



System Properties



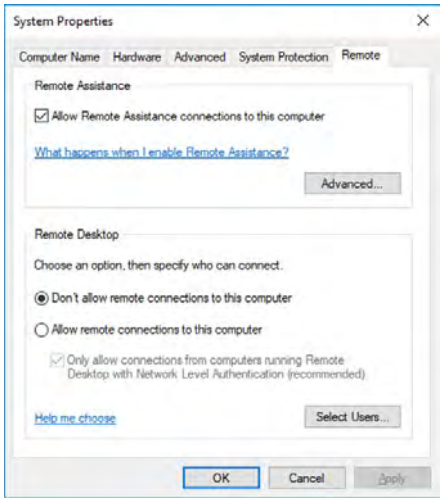


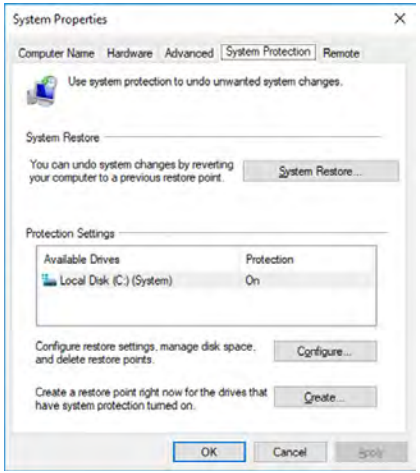
Advanced System Properties

Remote Assistance: A Windows remote support feature allowing a user to invite a technical support professional to help them over a network using chat.

Remote Desktop: A Windows feature that allows a remote user to initiate a connection at any time.

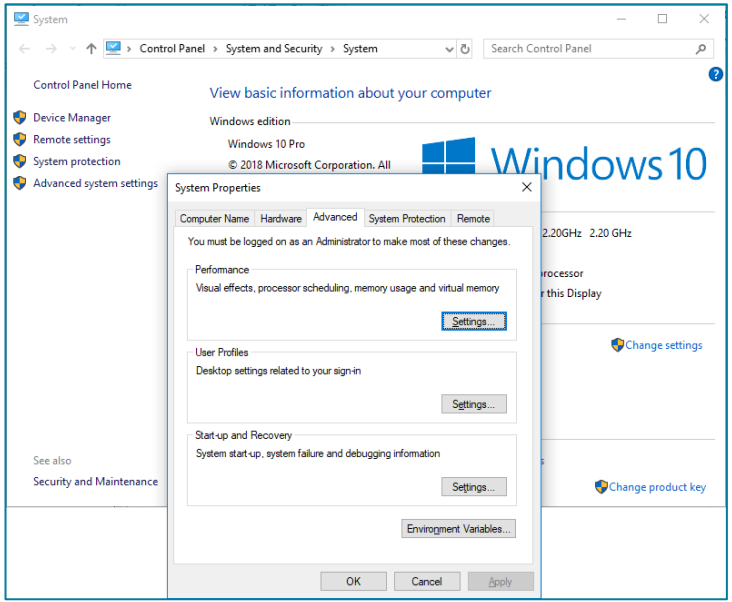
- Remote settings
- System protection
- Advanced settings





Advanced System Properties

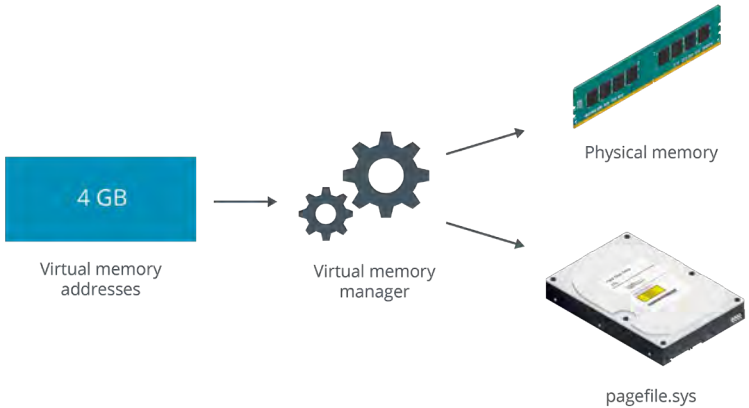
- Performance options:
  - Configure desktop visual effects
  - Virtual Memory
  - Foreground/Background processing priority
- Startup and recovery options
- Environment variables
- User Profiles



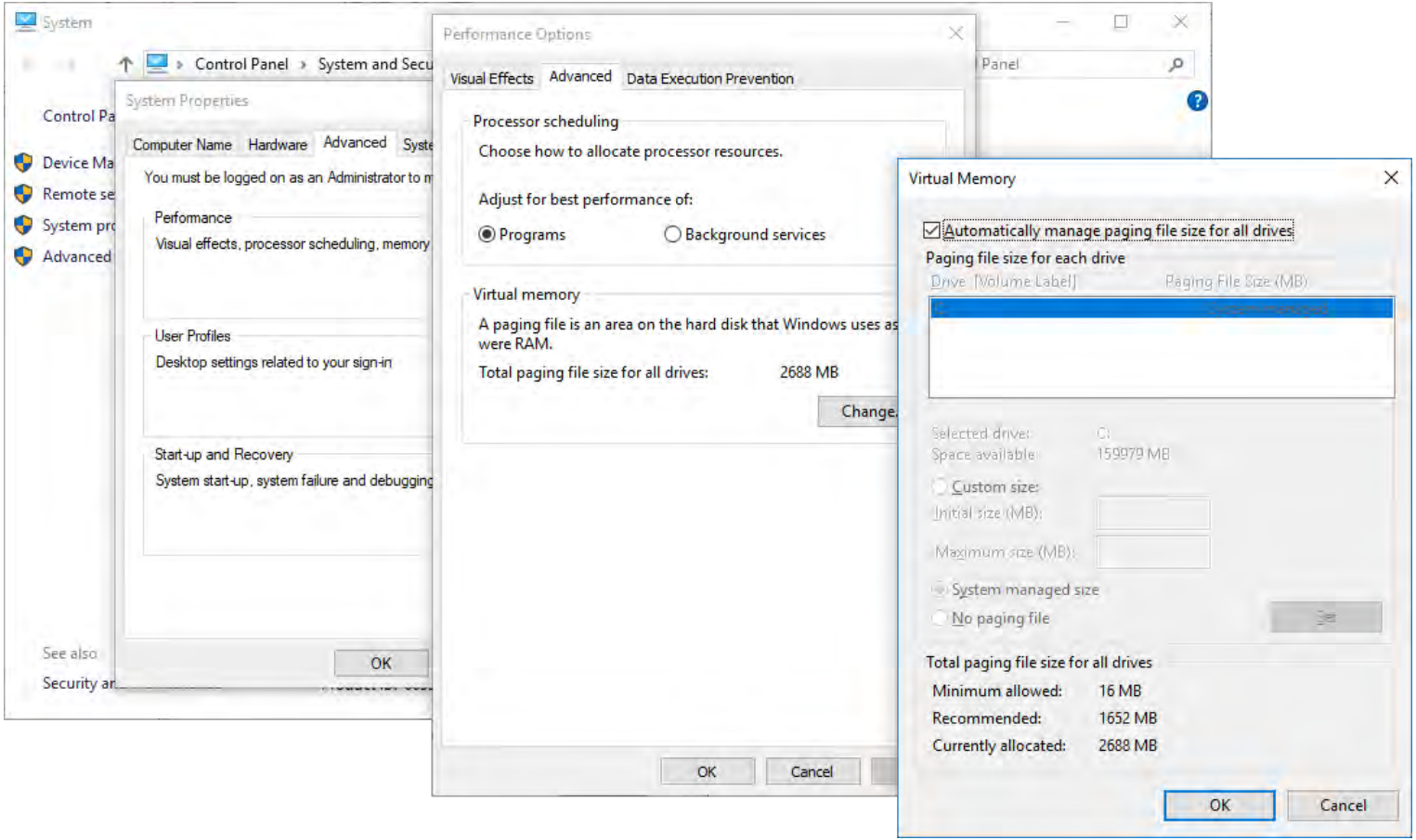
Virtual Memory

Virtual memory or **Pagefile:** An area on the hard disk allocated to contain pages of memory that is used when there is not sufficient physical RAM available.

- Windows sets appropriate level for pagefile.
- Each physical disk has a pagefile.
- Pagefile doesn't have to use contiguous disk space.
- Virtual memory is not as fast as physical memory.



Virtual Memory

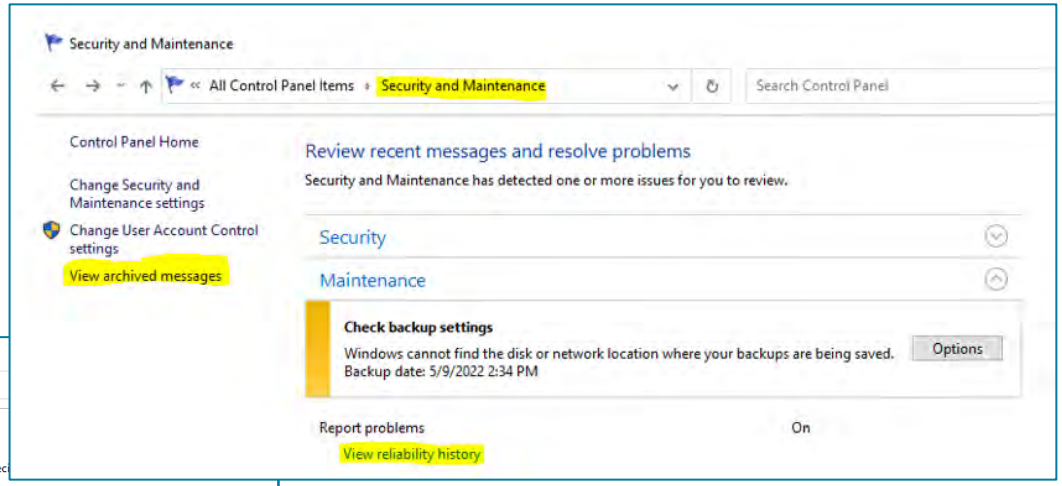


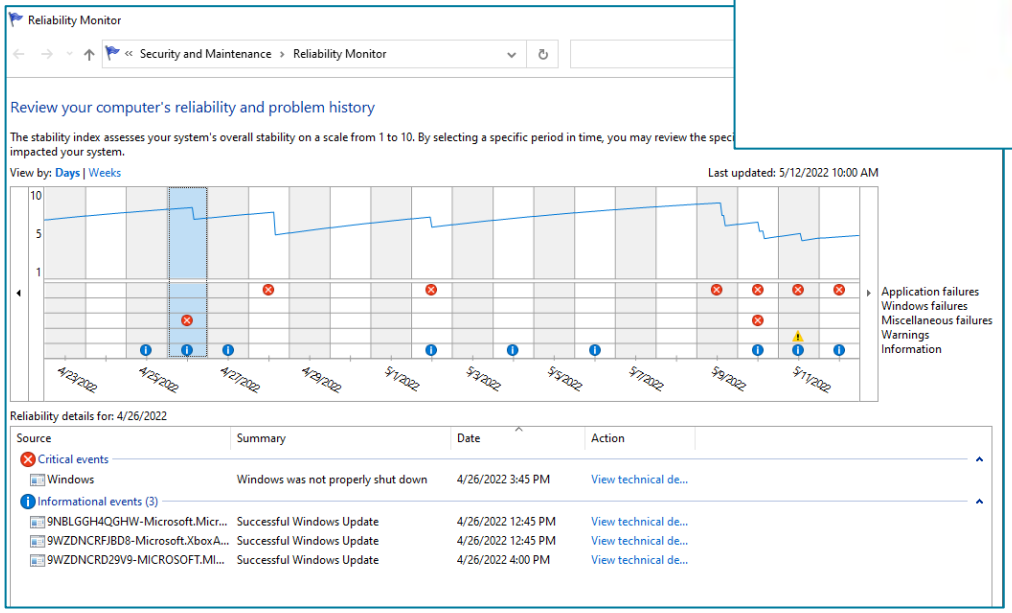
Windows Performance Management Tools

- **Task Manager**—as you have seen, you can use the **Performance** tab in **Task Manager** to monitor utilization statistics in real time.
- **Resource Monitor**—shows an enhanced version of the sort of snapshot monitoring provided by **Task Manager**.
- **Reliability Monitor**—displays a log of "system stability" events, so you can see at a glance whether a particular application has stopped responding frequently
- **Performance Monitor**—configure detailed reports on different system statistics and log performance over time.



Reliability Monitor

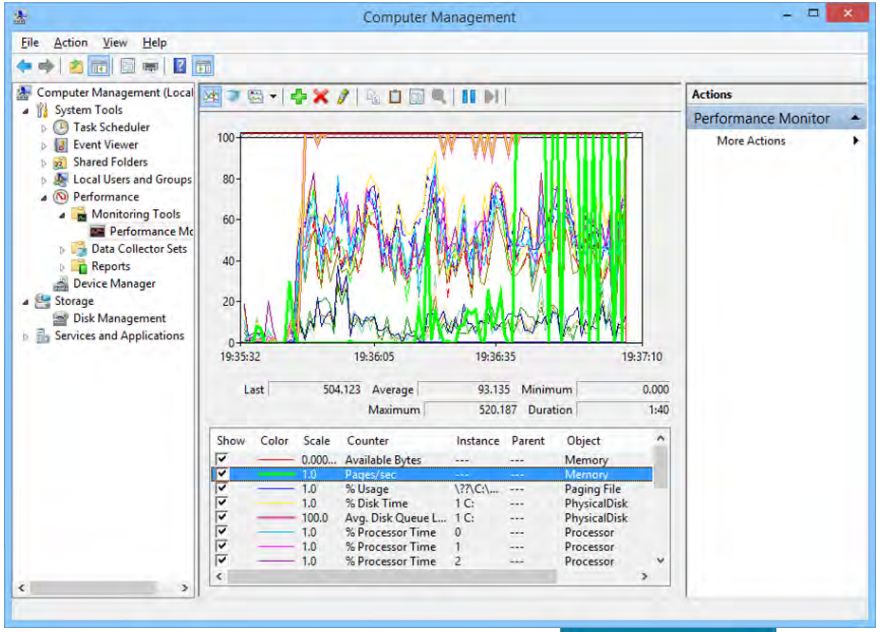




Windows Performance Management Tools

Objects: A data structure in Windows that represents system resources.

- Objects:
  - Processor
  - Physical Disk
  - Memory
  - Paging File
- Counters for each object
- Instances for multiple objects



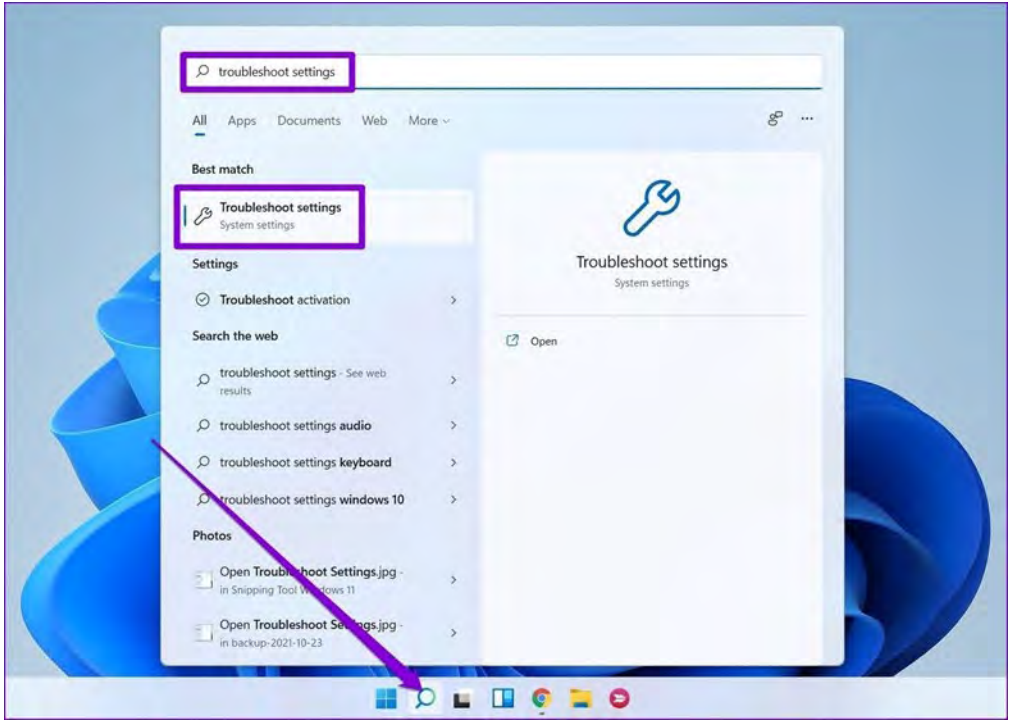
Windows Performance Management Tools

Data Collector Sets: Windows log files that record information for viewing in real time or later. (Can Create a Baseline)

Counter logs: Windows log files that allow you to collect statistics about resources and can be used to determine system health and performance.

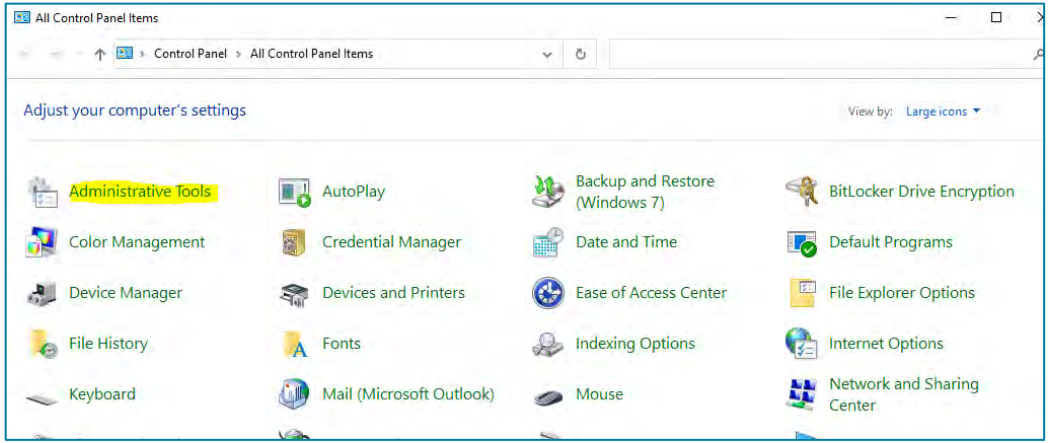
Trace logs: Windows log files that allow you to collect statistics about services, including extensions to Event Viewer to log data that would otherwise be inaccessible.

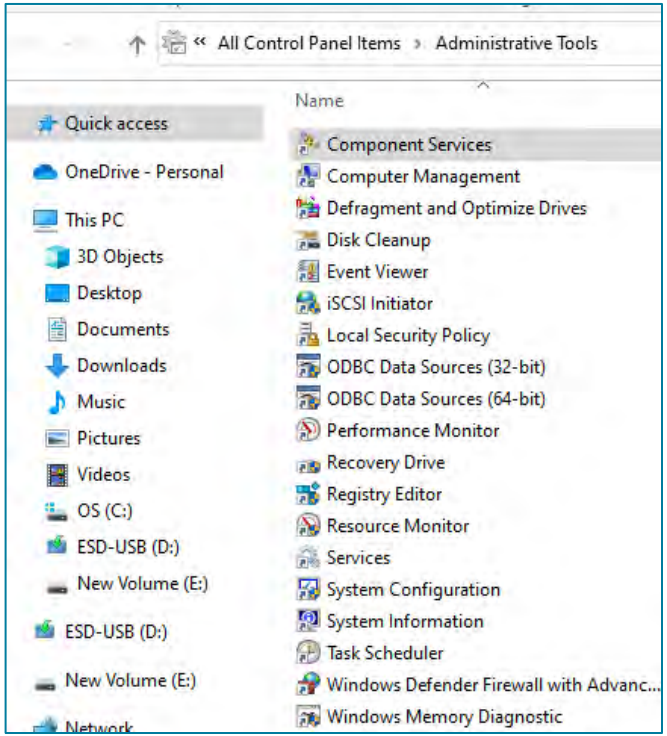
Topic C: Troubleshoot Windows



Administrative Tools

Control Panel / Administrative Tools





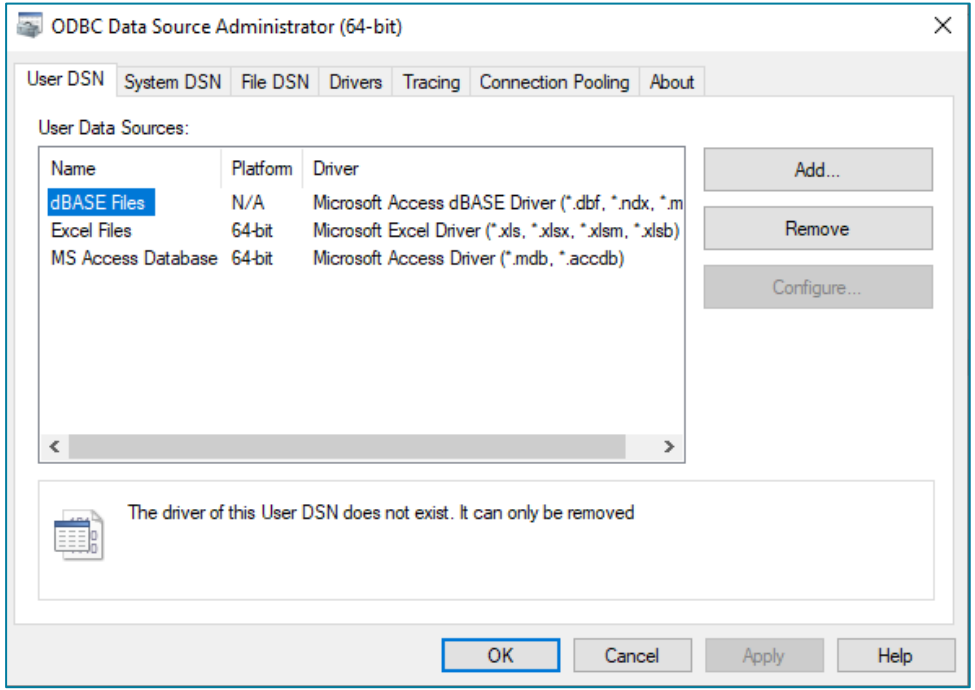
ODBC Open Database Connectivity

Control Panel / Administrative Tools

ODBC

(Open Database Connectivity)

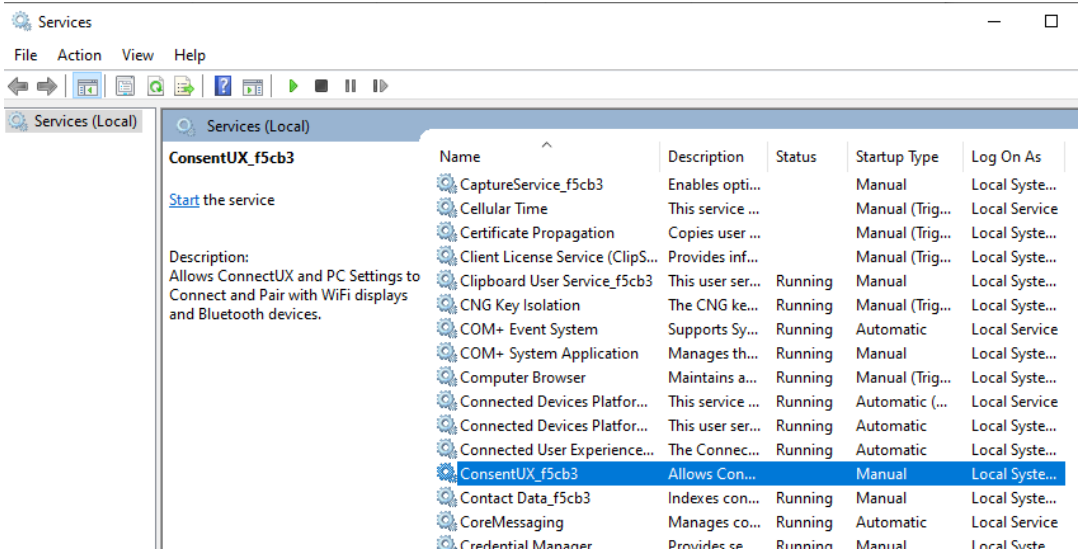
- **Application independence**
- **Database and OS doesn't matter**
- **Users probably won't need this**



Services

Control Panel / Administrative Tools

Type: services.msc



Background process

- No user interaction
- Useful when troubleshooting the startup process
- Many services startup automatically
- Command-line control

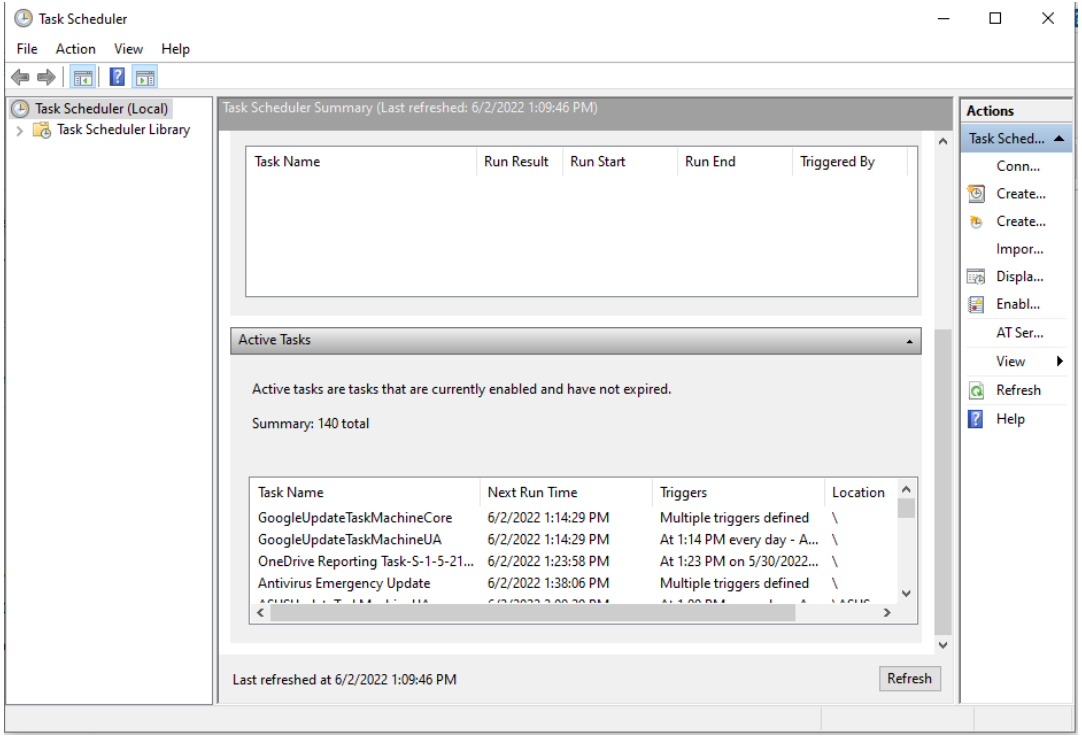
net start, net stop

Task Scheduler

Control Panel / Administrative Tools

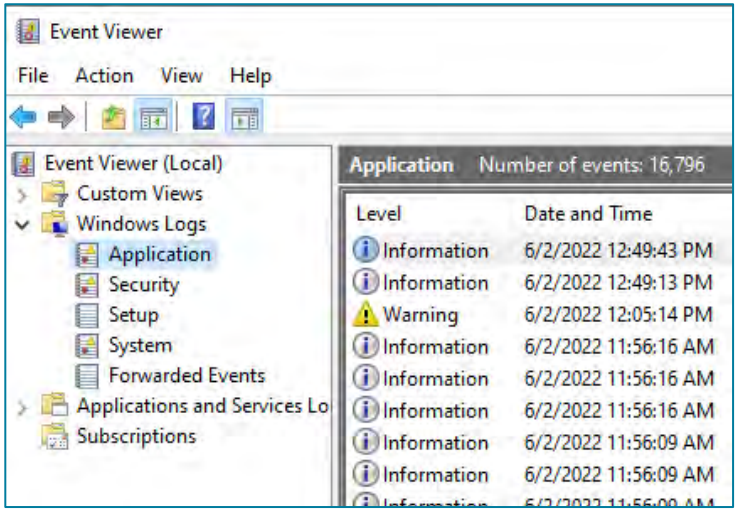
Schedule an application or batch file to RUN

- **Plan your future**
- **Includes predefined schedules**



Event Viewer

Type: eventvwr.msc

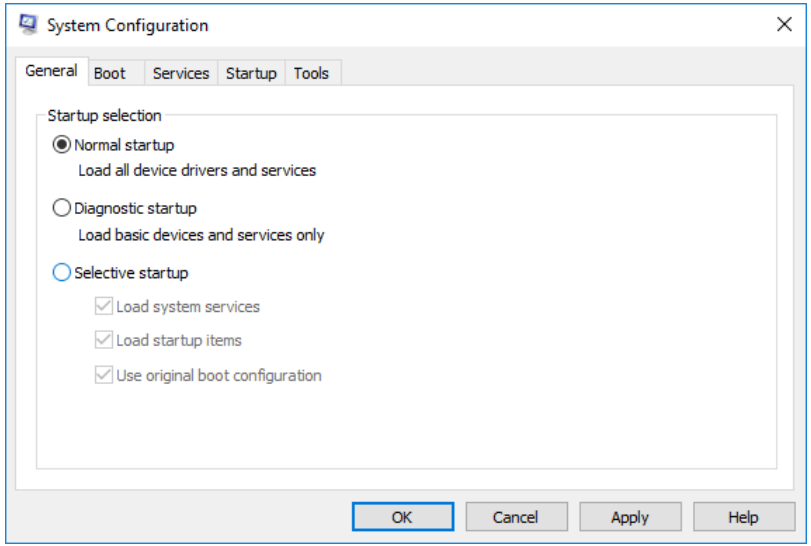


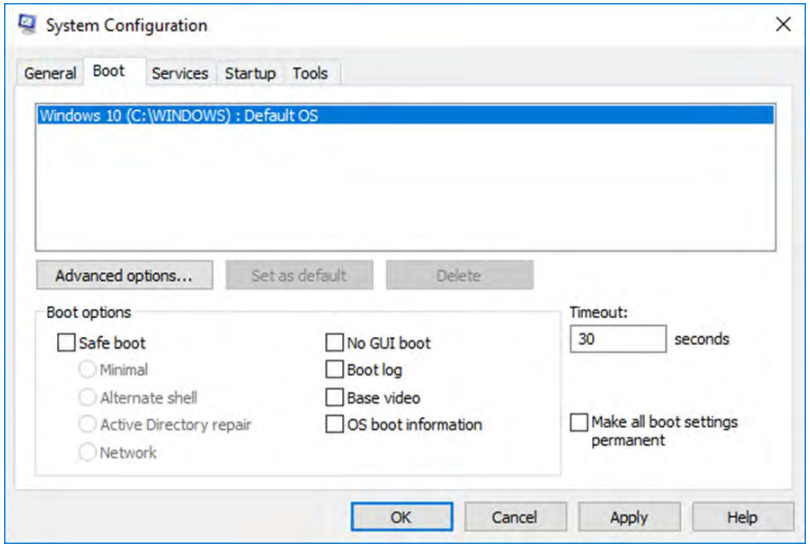
Log File	Description
System Log	Contains information about service load failures, hardware conflicts, driver load failures, and so on.
Security Log	This log holds the audit data for the system.
Application Log	Contains information regarding application errors.
Setup	Records events generated during installation.

Event	Description
Information	Significant events that describe successful operations, such as a driver or service starting or a document printing.
Warning	Events that may indicate future problems, such as when the system runs low on disk space.
Error	Significant problems, such as service failures and device conflicts.
Critical	An unrecoverable error that made the application or Windows close unexpectedly.

The System Configuration Utility

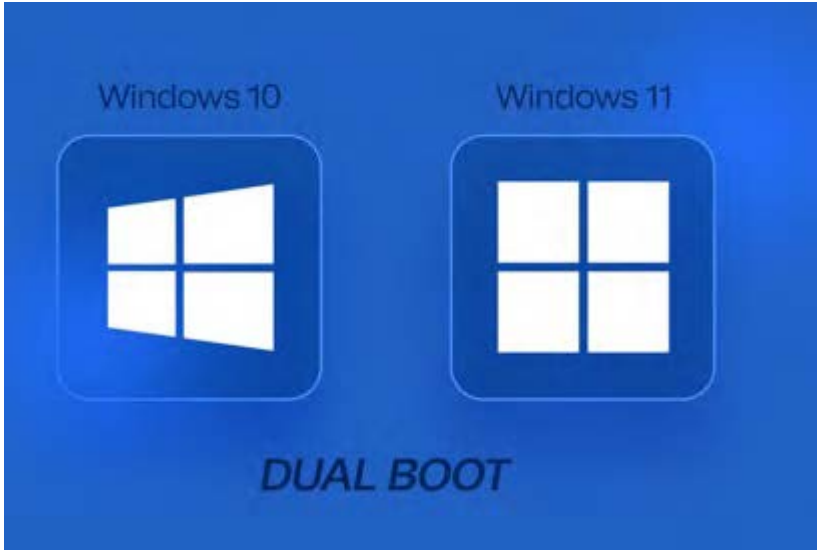
The System Configuration Utility (msconfig) is used to modify various an affect the way the computer boots and loads Windows.



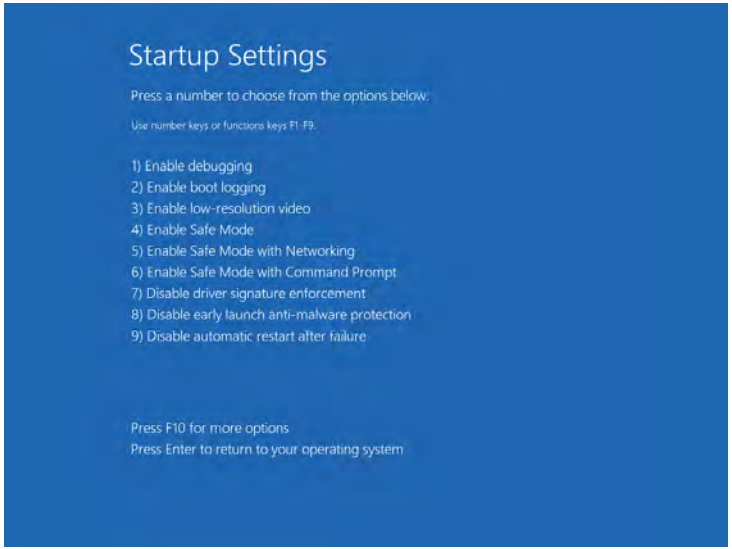


Troubleshooting Tips Boot Process

- Firmware-controlled
  - Power on self test (POST
  - Boot device priority
- Boot manager
  - Boot Configuration Database (BCD)
  - Legacy BIOS/MBR versus EFI/GPT
- Windows load
  - Kernel and drivers
  - Services and winlogon



Troubleshooting Tips Boot Process



- Advanced boot options
  - F8 from BIOS boot
  - SHIFT-click Restart from power icon with UEFI boot
- Safe Mode

Troubleshoot Application and Service Fault Issues

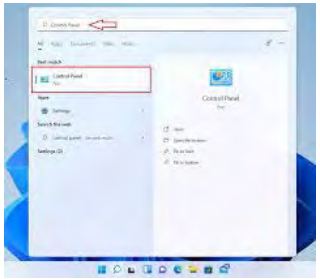
- Time drift
  - Failure of authentication, backup, and other date/time sensitive services
  - Synchronize to Servers must be consistent
  - real time clock (RTC) chip

  - Relying on the internal time can lead to servers and clients drifting out of sync, especially if some of the clients' remote clients

  - Ideally, time should be configured in a domain and use either GPS synchronized time sources or a pool of Internet time sources.

Troubleshooting Tips Boot Process

- Fast start
  - Step 1: Open the Control Panel from the Start menu. ...
  - Step 2: Click the “System and Security” button. ...
  - Step 3: Click the “Power Options” button. ...
  - Step 4: Click the “Choose what the power buttons do” option from the left sidebar.



Troubleshooting Tips for Windows System Issues

- For slow performance check:
  - Wait for these processes to complete.
  - If the process or system continues to be unresponsive, you can either restart the service or kill the task process.
  - If killing the process doesn't restore system performance, try restarting the computer.
  - If the service or process becomes unresponsive again after restarting, disable it and check with the software vendor for any known problems.

Troubleshooting Tips for Windows System Issues

- Consider these troubleshooting techniques and solutions:
  1. Apply updates.
  2. Defragment the hard drive.
  3. Examine power management issues.
  4. Check for underpowered components.
  5. Disable application startup.
  6. Disable Windows services and/or applications.
  7. Perform a security scan.
  8. Check the configuration of anti-virus software.

Troubleshooting Tips for Windows System Issues

- If a service fails to start:
  1. Try to start the service manually.
  2. Verify the service has sufficient privileges.
  3. Verify any dependent services are started.
  4. Check system files and scan for malware.
  5. Try reinstalling affected application.
  6. Re-register software component using regsvr32.
  7. Check whether the service is supposed to run.

Troubleshooting Tips for Application Issues

- If an application crashes:
  1. Try to preserve any data being processed.
  2. Give the process time to become responsive again.
  3. If necessary, kill the process.
  4. Try to recover data from temporary files or folders if necessary.
  5. Attempt to identify whether the cause is in the data file.
  6. If you can't determine the cause, try to uninstall then reinstall the application.
  7. If available, in Programs and Features, use the Repair option.

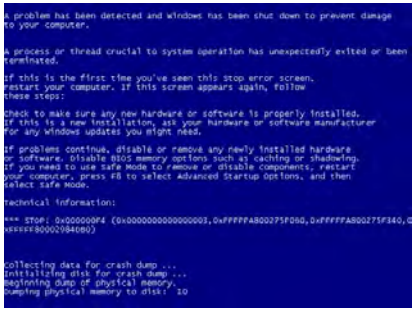
Troubleshooting Tips for Application Issues

- If you are having printing issues:
  1. Use the printer's property dialog to try printing a test page.
  2. Open the print queue and check for stalled print jobs.
  3. Restart the print spooler service.
  4. Check for any driver updates or known issues.
  5. Check permissions configured on the printer.
  6. Check for disk problems on the partition hosting the spool folder.

Blue Screens and Spontaneous Shutdowns

BSoD: This indicates an error from which the system cannot recover.

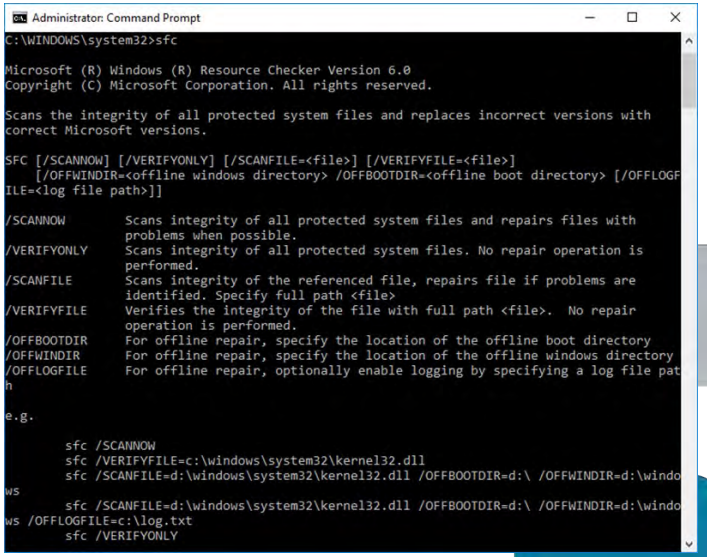
1. Use System Restore, or (if you can boot to Safe Mode), Rollback Driver to restore the system to a working state.
2. Remove new hardware or program
3. Check seating of hardware and cables
4. Run diagnostics, chkdsk, scan for malware
5. Record stop error code and search Microsoft Knowledge Base for known fixes and troubleshooting tips



Troubleshooting Tips for File and Memory Corruption

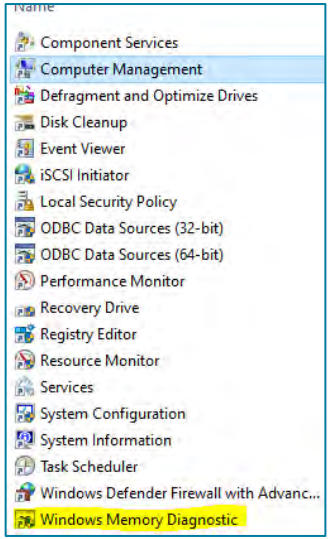
Windows Resource Protection: A Windows feature that prevents essential system files, folders, and registry keys from being replaced to help prevent application and OS failure.

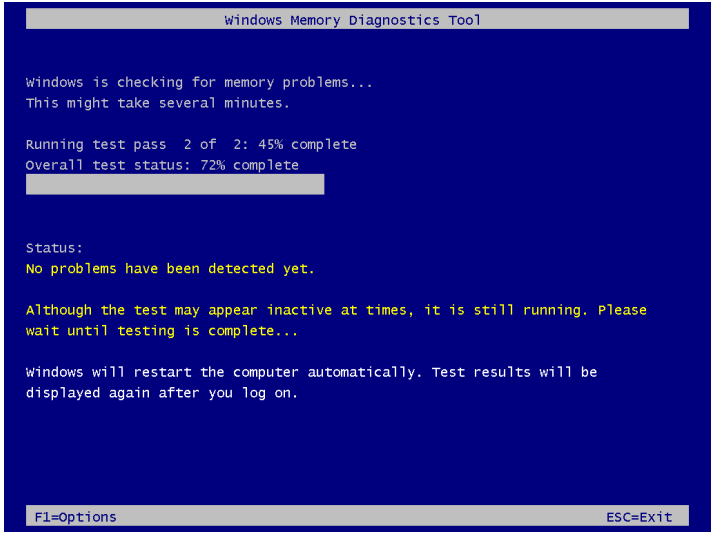
- System File Checker
  - sfc /scannow
  - sfc /scanonce
  - sfc /scanboot



Troubleshooting Tips for File and Memory Corruption

Windows includes a **Windows Memory Diagnostics tool** to test memory chips for errors.





Troubleshooting Tips for Boot Problems

POST: A hardware checking routine built into the PC firmware.

MBR: Sector on a hard disk storing information about partitions configured on the disk.

Boot sector or **Volume Boot Record (VBR):** Loads the boot manager, which for Windows is bootmgr.exe.

BCD: Windows stores information about operating systems installed on the computer in a boot configuration data store.

Troubleshooting Tips for Boot Problems

- Boot process
  - Verify the boot process is functioning normally the boot manager loads the
  - Windows boot loader winload.exe in the system root folder

- Failure to boot/Invalid boot disk

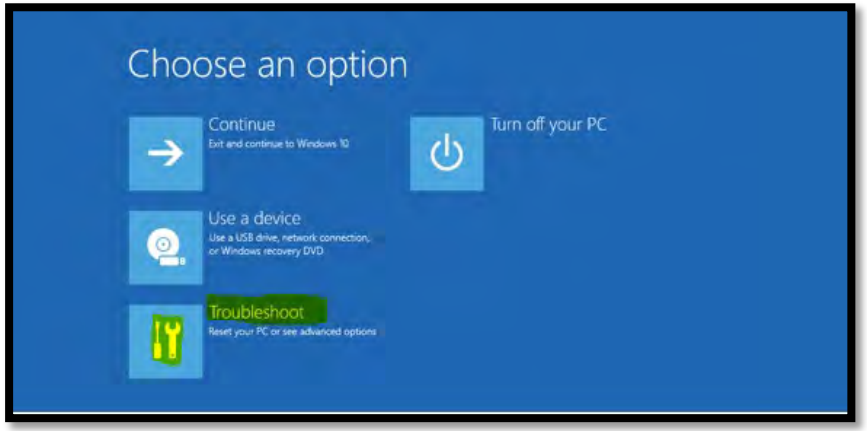
- No OS Found
  - bootrec /fixmbt
  - bootrec / fixboot (Good for GPT)
  - bootrec / rebuildbcd

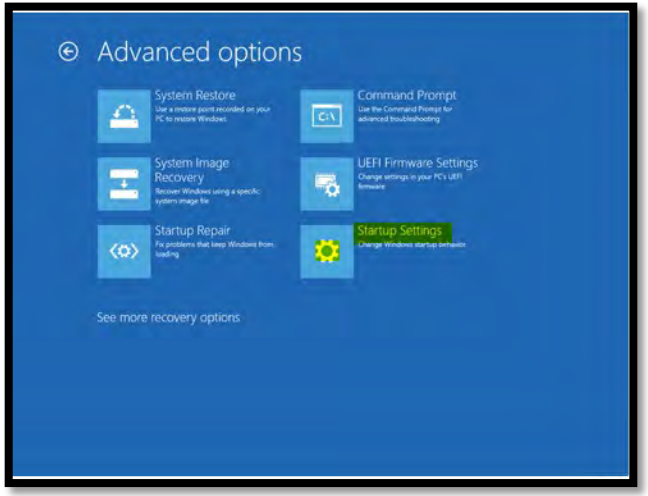
- Graphical interface fails to load/Black screen
  - Try pressing Windows+Ctrl+Shift+B to test whether the system is responsive

Safe Boot

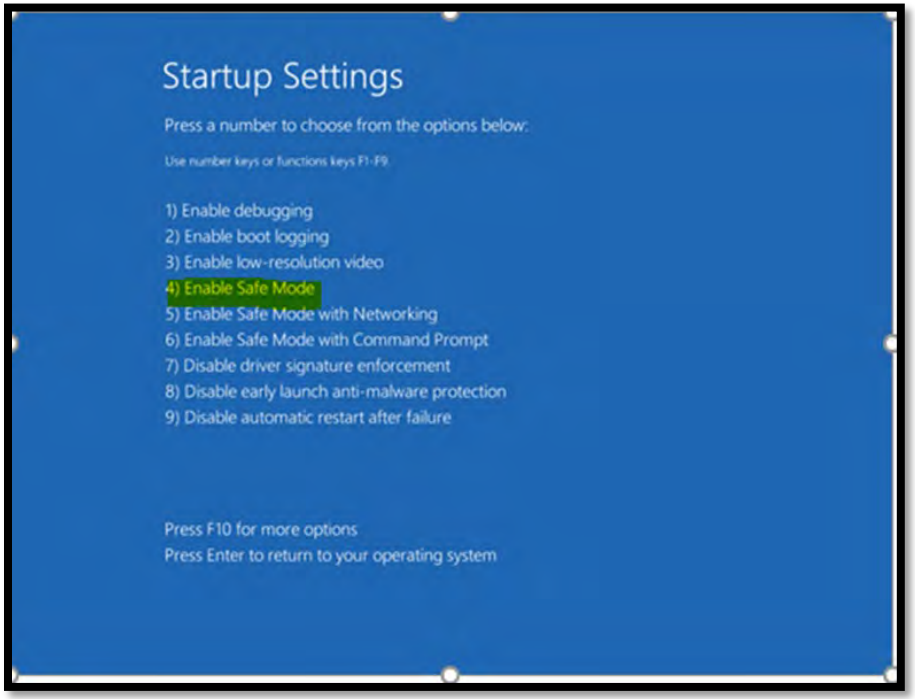
- Safe Mode loads only basic drivers and services needed to start the system.
- You can add in drivers and app services one by one to see where a problem occurs.
- It's also helpful when you are running analysis and recovery tools.
- Default display resolution for Safe Mode is SVGA (800x600).
- Different ways to access Safe Mode:
  - **System Configuration** utility if you can sign on to Windows.
  - **Advanced Boot Options** menu in Windows 7.
  - **Power→Shift** + **Restart** in Windows 8 and 10.

Safe Boot





From the first **Choose an option** screen, select **Troubleshoot**. From the next screen, select **Advanced options**. Select **Startup Settings**, then on the next screen, select **Restart**.



Safe Boot

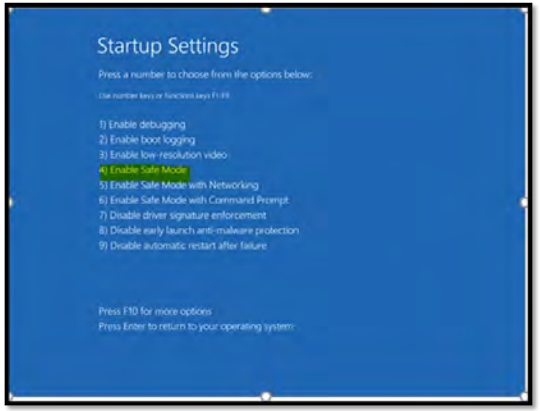
- The Startup Settings option on the Advanced options screen is available only when Windows RE is launched from the hard drive
  - Rather than another media

- What these tools can do:
  - Press 1 or F1: Enable Debugging
    - Moves system boot logs from the failing computer to another computer for evaluation

  - Press 2 or F2: Enable Boot Logging
    - Windows loads normally
    - All files used during load process are recorded
      - C:\Windows\Ntbtlog.txt
    - See what did and did not load during the boot

Safe Boot

- What these tools can do (continued):
  - Press 3 or F3: Enable Low-Resolution Video
    - Used when the video setting does not allow screen to display well enough to fix a bad setting
    - Can also use this option for problems with video drivers
  - Press 4 or F4: Enable Safe Mode
    - Launch antivirus software
    - Open Event Viewer
    - Run the System File Checker command
    - Use Device Manager to roll back a driver
    - Use Memory Diagnostics to verify memory
    - Use the chkdsk /r command to check for file system errors
    - Configure Windows for a clean boot on next restart
    - Perform other troubleshooting tasks



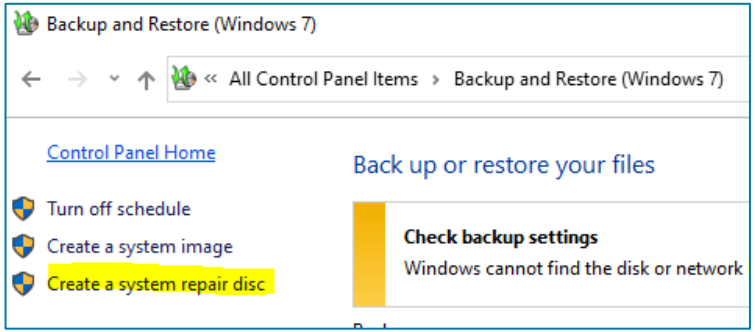
Safe Boot

- What these tools can do (continued):
  - Press 5 or F5: Enable Safe Mode with Networking
    - Use when solving a problem with booting and network access is needed
    - Also use when the Windows installation files are available on the network
  - Press 6 or F6: Enable Safe Mode with Command Prompt
    - Use the **sfc /scannow** command to verify system files
    - If problem not solved, launch System Restore
      - C:\Windows\system32\rstrui.exe

Safe Boot

- What these tools can do (continued):
  - Press 7 or F7: Disable Driver Signature Enforcement
    - All 64-bit editions of Windows require that kernel-mode drivers be digitally signed
    - Disabling this option is used by developers who are testing kernel-mode device drivers
  - Press 8 or F8: Disable Early Launch Anti-Malware Driver
    - Windows 10/8 allow antivirus software to launch a driver before any third-party drivers are launch so it can scan drivers for malware
  - Press 9 or F9: Disable Automatic Restart on System
    - Stop rebooting upon encountering a system failure
  - Press F10: Return to the Startup Settings Screen
    - Return to Windows Startup Menu screen

System Repair Disc

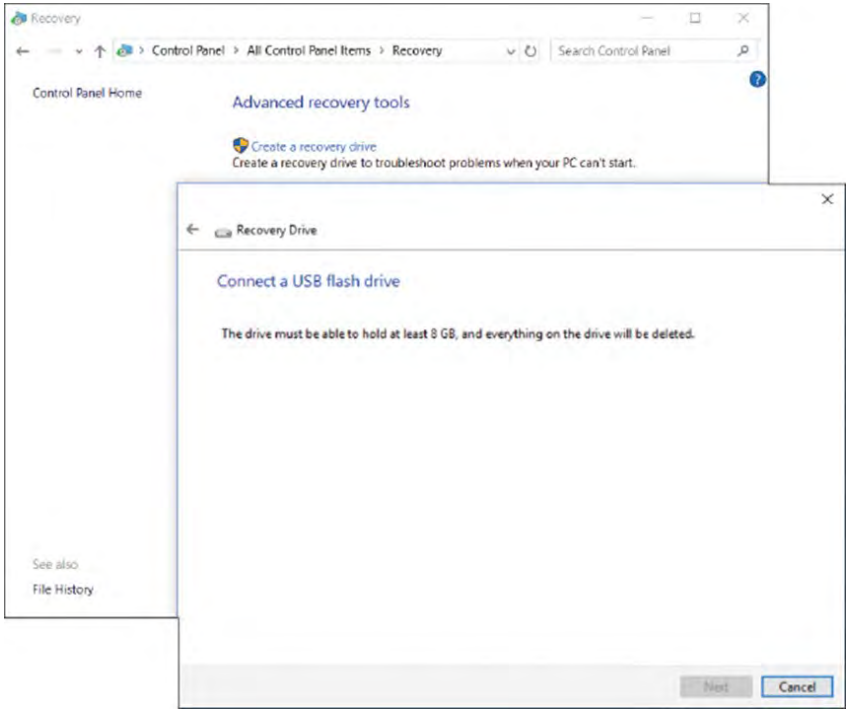


- Create a system repair disc
  - You can use it to launch Windows RE
- To create:
  - Click **Create a system repair disc** in the Backup and Restore (Windows 7) window
  - A 32-bit installation will create a 32-bit version of the repair disc and a 64-bit Windows installation will create a 64-bit version of the repair disc

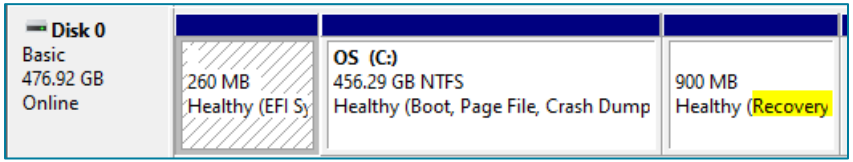
System Recovery Drive

- Most computers include an OEM recovery partition on the hard drive that contains the drivers specific for the computer
- Before a problem occurs, back up this OEM partition to a Windows recovery drive
  - A bootable USB flash drive that can access Windows 10/8 repair tools
- To create a recovery drive:
  - Open Control Panel and click **Recovery**, click **Create a recovery drive** and respond to the UAC dialog box
  - Choose whether to include system files, click **Next**
  - Windows reports the size of the USB flash drive needed, insert drive
  - Windows inspects the size of the drive
    - If large enough, you see it listed among available devices, click **Next**, click **Create** to begin the process

System Recovery Drive



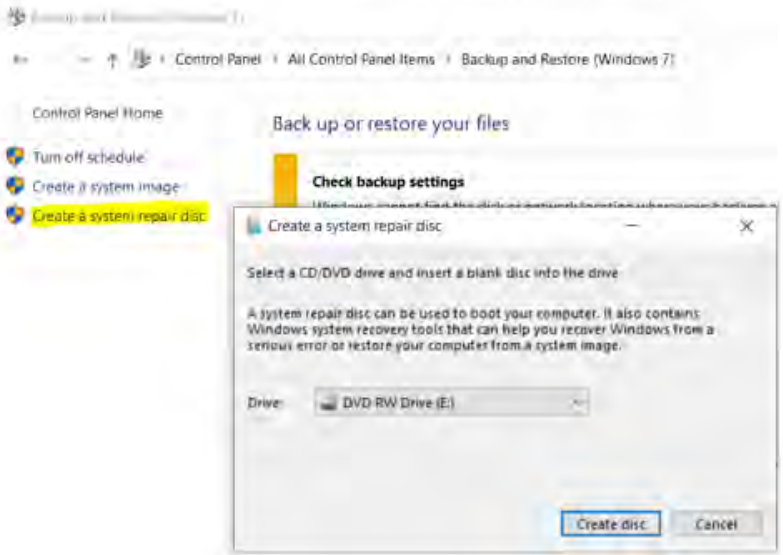
Recovery Drive is a copy (to a bootable USB flash drive) of the "recovery partition"



System Repair vs Recovery Drive

What is the difference between **'System repair disc'** and **'Recovery drive'** in Windows 10? The **recovery drive** brings your system back to factory defaults; the system repair disc will bring your computer back to the same condition it was in when you created the system repair disc.

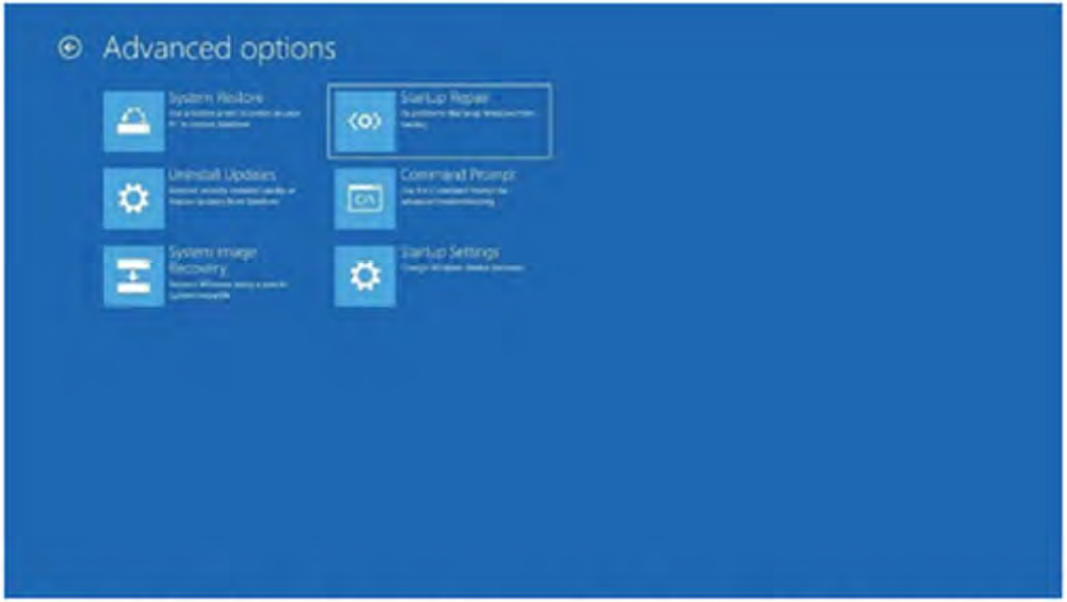
A **System Repair disc** can be created on computers and devices with Windows 7, Windows 8 and Windows 10, as long as they have a disc burning drive like a **DVD writer**. You need to boot from the System Repair disc and start the tool that interests you



Startup Repair

- **Startup repair** is a built-in diagnostic and repair tool
  - Can fix Windows system files without changing Windows settings, user data, or applications
- To run startup repair in Windows RE:
  - Drill down to the Advanced options screen and click **Startup Repair**
- Windows RE examines the system, fixes problems, reports what it did, and might offer suggestions for further fixes
- A log file of the process can be found at:
  - C:\Windows\System32\LogFiles\SRT\SRTTrail.txt

Startup Repair

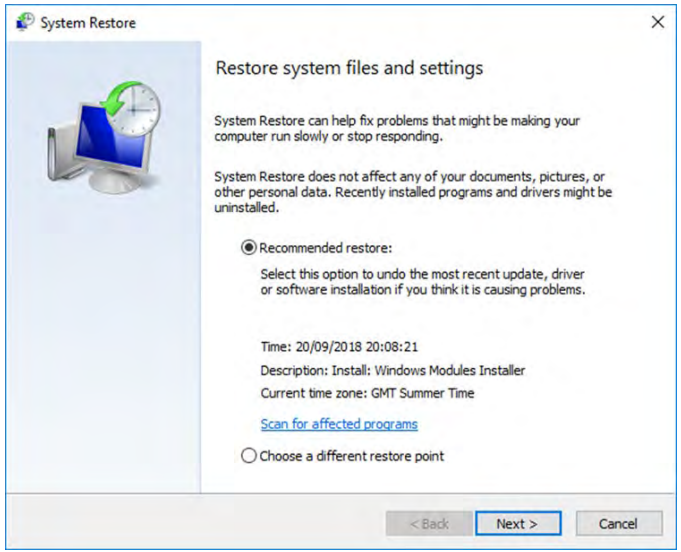


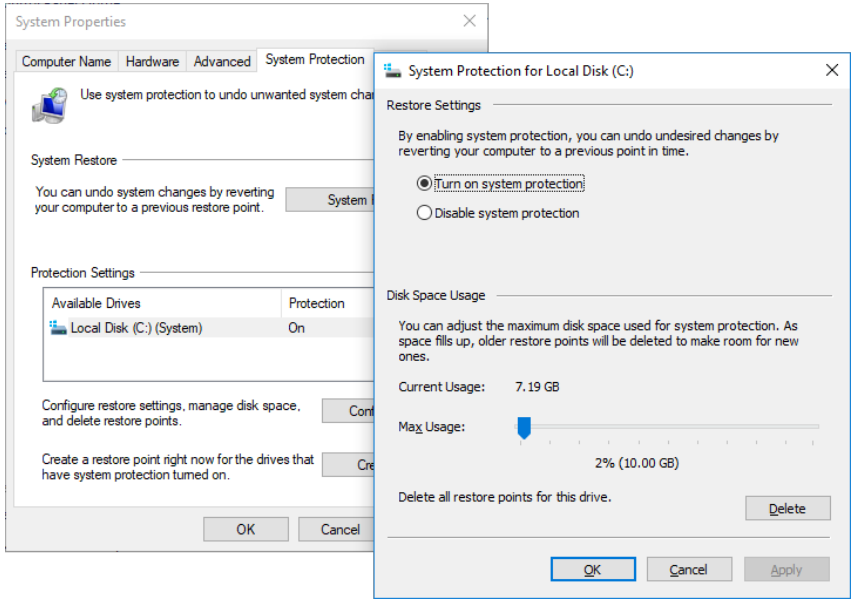
Startup repair: Instead of spending time trying to find out the problem, Windows 10 includes the Startup Repair feature designed to quickly fix most common issues that may be preventing your computer from loading correctly.

System Restore

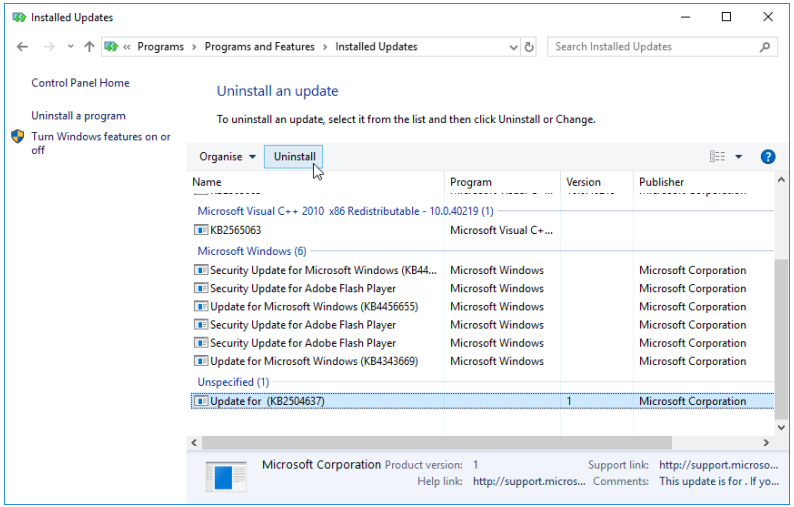
System Restore allows you to roll back from system configuration changes.

System Restore allows for multiple restore points to be maintained (some are created **automatically**) and to roll back from changes to the whole registry and reverse program installations and updates.

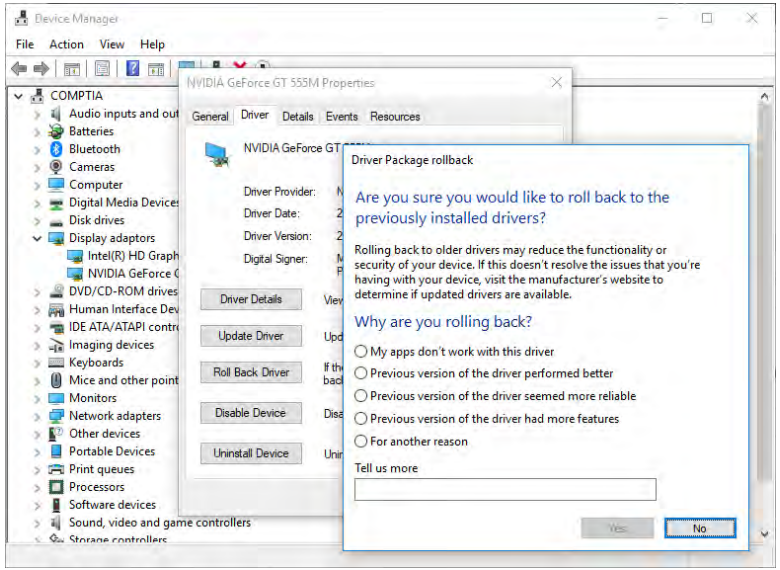




System Restore



Reverse program installations and driver updates

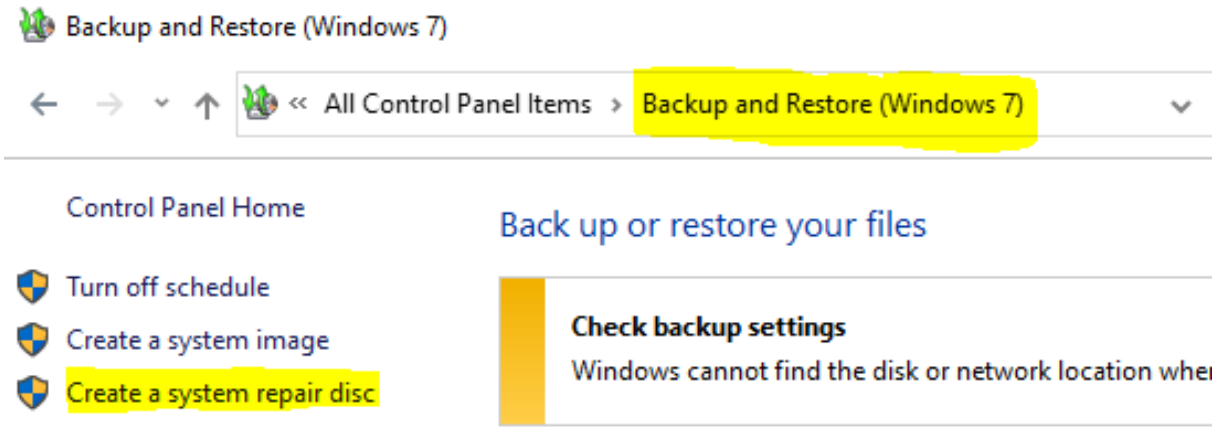


System Image

Image: A duplicate of an operating system installation (including installed software, settings, and user data).

- You can make a complete backup of the system configuration and data files. This is called an image.
- This method is simple, but you do need a backup device with large capacity.
- You create a system image using the Backup and Restore applet in Control Panel.
- Click the Create a system image link in the tasks pane.
- Select a backup device and give the image a suitable name.

System Repair and Reinstall



This creates a .WIM file

Guidelines for Troubleshooting Windows Issues

1. Examine log files and Event Viewer to get information about what has happened on the system.
2. Use the System Configuration Utility to modify system settings and files that affect the way the computer boots and loads Windows.
3. Use Task Manager to attempt to locate a reason for slow system performance.
4. Use Event Viewer to attempt to determine why a service fails to start.

Guidelines for Troubleshooting Windows Issues

- If an application crashes:
  1. Try to preserve any data that was being processed.
  2. See if the process will become responsive again or if you need to kill the process.
  3. Attempt to recover data from temporary files or folders if the process was killed.
  4. Examine Event Viewer logs.
  5. If the application repeatedly crashes, uninstall then reinstall the application or if available, use the Repair option in Programs and Features.

Guidelines for Troubleshooting Windows Issues

- If there are printing issues not related to printer hardware or network connectivity, examine Windows settings and check the following:
  1. Use the printer's property dialog box to try printing a test page. If this is successful, there must be an application or file-specific problem.
  2. Open the print queue and check for stalled print jobs.
  3. Restart the print spooler service.
  4. Check for any driver updates or known issues.
  5. Check permissions configured on the printer.

Guidelines for Troubleshooting Windows Issues

- If the user experiences frequent BSoDs:
  1. Use System Restore or, (if you can boot to Safe Mode), Rollback Driver.
  2. Remove a recently added hardware device or uninstall a recently installed program.
  3. Check seating of hardware components and cables.
  4. Run hardware diagnostics, chkdsk, and scan for malware.
  5. Make a note of the stop error code and search the Microsoft Knowledge Base for known fixes and troubleshooting tips.

Guidelines for Troubleshooting Windows Issues

If the user experiences file or memory corruption:

1. Use sfc to verify system files and restore them from cache if corrupt or damaged.
2. Use the Windows Memory Diagnostics tool to test memory chips for errors.
3. If the user is experiencing boot problems, determine the failure point.
4. Try booting into Safe Mode to troubleshoot by loading only minimal required components.
5. Try booting from the product media, a repair disc, or a recovery partition.
6. Use System Restore to rollback system configuration changes.

Guidelines for Troubleshooting Windows Issues

- Rollback updates that are causing issues by uninstalling them.
  - Open Programs and Features.
  - Select View installed updates.
  - Select the update that is causing the problem, then select the Uninstall button.

- Rollback troublesome device drivers.
  - Open Device Manager.
  - Right-click the device having the problem and select Properties.
  - Select the Driver tab.
  - Select the Roll Back Driver button.

- If all else fails, determine whether you need to perform a system restore or reinstall Windows.

Discussing Storage Device Troubleshooting

- **A user complains that a "Buffer underrun" error keeps occurring when they try to write to recordable DVDs. What would you suggest?**

- **ANSWER:**
  - Do not use other applications at the same time as DVD writing, make sure that the source files are on the local hard disk (not a removable or network drive), or try using a slower write speed.

Discussing Storage Device Troubleshooting

- **You are trying to install Windows from the setup disc, but the computer will not boot from the CD. What should you do?**

- **ANSWER:**
  - Check the boot order in system setup is set correctly; check that the disc is not dirty or scratched.

Discussing Storage Device Troubleshooting

- **If you experience an error such as “BCD missing" when booting the computer, what action could you take?**

- **ANSWER:**
  - Use the Startup Repair tool or run `bootrec /rebuildbcd`.

Discussing Storage Device Troubleshooting

- **A user reports hearing noises from the hard disk—does this indicate it is failing and should be replaced?**

- **ANSWER:**
  - Not necessarily—hard disks do make noises, but they are not all indicators of a problem. Question the user to find out what sort of noises are occurring or inspect the system yourself.