aci LEARNING
AUDIT-CYBER-IT

Module 1
Operating Systems

 Updated: July 2023 CD Team

Module 1
Operating Systems

A+ 1102

Module 1 Learning Objectives

- Compare and contrast modern operating systems and their purposes.
- Compare and contrast Windows 10 editions (Home, Pro, Pro for Workstations, and Enterprise) and their features.
- Summarize general operating system installation methods.
- Identify the appropriate Windows command-line tools in a given scenario.

Module 1 Learning Objectives

- Identify and summarize the appropriate Windows System tools.
- Identify and summarize the appropriate Windows Control Panel utility.
- Configure Windows client networking.
- Summarize features and tools of macOS and Linux desktop operating systems.

Table of Contents

Topic: Common Operating Systems

In this section, we will cover:

- Windows 10
- Linux
- OS X
- Google Chrome OS
- Android
- iOS

Windows 10

Windows 10 is the most distributed desktop OS worldwide — over 75 million devices run Windows 10.

- Windows 10 is the successor to Windows 8.1.
- Several Windows 10 versions are available, including Home, Pro and Enterprise editions.

Cortana was introduced to the Windows environment.

Linux

Linux is a widely used operating system and can be used for several purposes; for example, popular social media providers use it as a web server.

Linux commands are case-sensitive.

The Linux kernel is open-source code. Enabling the creation of different versions of the operating systems, also referred to as distro’s.

OS X

macOS is based on a Unix kernel operating system and powers every Mac; it is specifically designed for the proprietary hardware it runs on.

Several different editions of the Mac OS are available. The latest version released in 2022, macOS 13 (Ventura).

All devices, one seamless experience.

Google Chrome OS

Google Chrome OS is based on the Linux OS.

The beauty is in simplicity.

Google Chrome OS was specifically designed for web browsing.

No data is stored on the actual computer; it is stored in the cloud.

Android

Android is a mobile operating system based on the Linux kernel owned by Google.

The Android operating system is open-source, making it freely accessible to anyone.

Mobile devices are primarily the systems that use them.

Android supports cloud storage and syncing of devices.

iOS

iOS is Apple’s mobile operating system used with Apple mobile devices.

The App Store, which is Apple’s application repository, provides Apple users with a central repository for Apple approved applications.

IOS supports cloud storage and syncing of devices via iCloud.

Topic:
File Systems

In this section, we will cover:

- Pre-boot Execution Environment (PXE)
- Network Boot
- File Allocation Table 16-bit (FAT16) and 32-bit (FAT32)
- Extensible File Allocation Table (exFAT)
- New Technology File System (NTFS)
- Apple File System (APFS)
- Hierarchical File System Extended (HFS+)
- Third Extended File System (ext3)
- Fourth Extended File System (ext4)
- Windows 10

Preboot Execution Environment (PXE)

The Preboot Execution Environment (PXE) allows users to install an Operating System from across the network.

The PXE Operating System is preconfigured with the necessary applications/tools.

Network Boot

Network boot must be configured on the device's BIOS/UEFI, allowing a user to boot the device from the network.

Network boot is a process that allows a user to load an OS and other programs from the network without having it stored locally on the device.

File Allocation Table 16-bit (FAT16)

File Allocation Table 16-bit (FAT16) is a 16-bit file system.

FAT16 can support a max hard drive volume size of 2GB; however, a later revision allowed up to 4GB.

FAT16 is a legacy file system from 1987.

FAT16 is versatile and compatible with Microsoft, Linux, and Mac operating systems.

File Allocation Table 32-bit (FAT32)

File Allocation Table 32-bit (FAT32) is a 32-bit file system that supports file sizes up to 4GB and a maximum volume size of up to 2 TB.

File Allocation Table 32-bit (FAT32) is used on various devices.

FAT32 is versatile and compatible with Microsoft, Linux, and Mac.

Extensible File Allocation Table (exFAT)

An Extensible File Allocation Table (exFAT) supported larger file sizes and disk partitions and was developed by Microsoft to replace FAT32.

Extensible File Allocation Table (exFAT) is optimized for flash drives and is compatible with all major operating systems.

New Technology File System (NTFS)

The New Technology File System (NTFS) was released in 1993 with Windows NT 3.1. The NTFS file system supports larger file sizes and partitions and is primarily used in Microsoft Operating Systems.

The New Technology File System (NTFS) provides security options like access control, encryption, compression, journaling, and file recovery if the system is shut down improperly.

Apple File System (APFS)

The Apple File System (APFS) is optimized for solid-state drive storage and supports encryption, snapshots, and data integrity.

The Apple File System (APFS) is 64-bit.

Hierarchical File System Extended Format (HFS+)

Hierarchical File System Extended Format (HFS+) is a journaling file system developed by Apple that allows for a larger number of files by optimizing storage capacity, allowing for smaller files and larger allocation blocks.

Linux (Read-Only)
Windows (Not Supported)

HFS+ replaced HFS and has better journaling like NTFS and ext4 so that data can save smoother to the hard drive. When power is lost to a device, it can reduce the chance of corruption in folders or files being used.

Third Extended File System (ext3)

Third Extended File System (ext3) is a journaled files system used primarily by Linux.

It was developed to replace the ext2 file system and includes logging.

Fourth Extended File System (ext4)

Fourth Extended File System (ext4) improves performance, reliability, and capacity.

Metadata and journal checksums.

Timestamping down to the nanosecond.

Backward compatibility.

An unlimited number of subdirectories.

Windows 10

Editions

Pro edition: lacks some features that are present in Enterprise and Education editions:

- AppLocker
- BranchCache
- Credential Guard

Home edition: lacks some features that are present in the Pro edition:

- Domain Join
- BitLocker
- Group Policy
- Hyper-V
- RDP (client only)

Versions and Upgrade Paths

Windows 7 SP1 to Windows 10

Windows 8 to 8.1 (only)
Windows 8.1 to 10
Windows 10 to Windows 11

You must reinstall if you are upgrading from 32-bit to 64-bit.

You must update from Windows 8 to Windows 8.1 in order to upgrade to Windows 10.

Upgrade Paths

Topic: Commands

In this section, we will cover:

- Microsoft Command-Line Tools

Help

1

With no argument:
It lists and briefly describes every system command.

with switch “/?”:
It lists the available additional commands or detailed help information on the specified command, definition, syntax and options.

2

help [<command>]

[<command>] /?

winver

Displays the version of Windows that is running and the build number.

attrib

1

Displays, sets, or removes attributes assigned to files or directories. If used without parameters, **attrib** displays attributes of all files in the current directory.

2

```
C:\Users\TroyAthmann>attrib /?
Displays or changes file attributes.

ATTRIB [+R | -R] [+A | -A] [+S | -S] [+H | -H] [+O | -O] [+I | -I] [+X | -X] [+P | -P] [+U | -U]
       [drive:][path][filename] [/S [/D]] [/L]

  +   Sets an attribute.
  -   Clears an attribute.
  R   Read-only file attribute.
  A   Archive file attribute.
  S   System file attribute.
  H   Hidden file attribute.
  O   Offline attribute.
  I   Not content indexed file attribute.
  X   No scrub file attribute.
  V   Integrity attribute.
  P   Pinned attribute.
  U   Unpinned attribute.
  B   SMR Blob attribute.
  [drive:][path][filename]
      Specifies a file or files for attrib to process.
  /S  Processes matching files in the current folder
      and all subfolders.
  /D  Processes folders as well.
  /L  Work on the attributes of the Symbolic Link versus
      the target of the Symbolic Link
```

dir

Displays a list of files and directories, their individual and cumulative size, and the free space (in bytes) remaining on the disk.

1

```
C:\Users\TroyAthmann>dir /?
Displays a list of files and subdirectories in a directory.

DIR [drive:][path][filename] [/A[[:]attributes]] [/B] [/C] [/D] [/L] [/N]
  [/O[[:]sortorder]] [/P] [/Q] [/R] [/S] [/T[[:]timefield]] [/W] [/X] [/4]

  [drive:][path][filename]
              Specifies drive, directory, and/or files to list.

  /A          Displays files with specified attributes.
  attributes   D  Directories                R  Read-only files
               H  Hidden files               A  Files ready for archiving
               S  System files               I  Not content indexed files
               L  Reparse Points             O  Offline files
               -  Prefix meaning not
  /B          Uses bare format (no heading information or summary).
  /C          Display the thousand separator in file sizes.  This is the
              default.  Use /-C to disable display of separator.
  /D          Same as wide but files are list sorted by column.
  /L          Uses lowercase.
  /N          New long list format where filenames are on the far right.
  /O          List by files in sorted order.
  sortorder    N  By name (alphabetic)       S  By size (smallest first)
               E  By extension (alphabetic)  D  By date/time (oldest first)
               G  Group directories first    -  Prefix to reverse order  /P
     Pauses after each screenful of information.
  /Q          Display the owner of the file.
  /R          Display alternate data streams of the file.
  /S          Displays files in specified directory and all subdirectories.
```

2

```
C:\>dir
 Volume in drive C is Windows
 Volume Serial Number is 8ED7-97DF

 Directory of C:\

07/15/2022  07:12 AM    <DIR>          Athmann
05/21/2022  10:50 AM    <DIR>          eclipse
07/18/2022  11:58 AM    <DIR>          HP_LaserJet_Enterprise
07/11/2022  07:45 PM    <DIR>          Program Files
07/18/2022  12:01 PM    <DIR>          Program Files (x86)
05/20/2022  04:23 PM    <DIR>          Python27
05/20/2022  01:00 PM    <DIR>          Users
07/14/2022  08:15 AM    <DIR>          Windows
               0 File(s)              0 bytes
               8 Dir(s)  847,797,600,256 bytes free
```

Wildcards

1

* - Used for any quantity of characters

*.txt	Any file with any quantity of characters with a “txt” file extension.
*1.txt	Will find any file with any quantity of characters, but it must end with “1” and have a “txt” file extension.
File.*	The filename must be exactly “File”, but any file extension.

2

? - Used for single character

file?.txt	It must start with “file” and have exactly 1 or 0 characters trailing it, and have a “txt” file extension.
?file?.txt	Must have exactly 1 or 0 characters leading **and** trailing “file” and have a “txt” file extension.
file??.txt	It must start with “file” and have 2, 1 or 0 characters trailing it and have a “txt” file extension.

cd

```
Displays the name of or changes the current directory.

CHDIR [/D] [drive:][path]
CHDIR [..]
CD [/D] [drive:][path]
CD [..]

  ..   Specifies that you want to change to the parent directory.
```

1

Used to change to a different directory. If there are spaces in a directory's name, it must be enclosed with quotes ("").

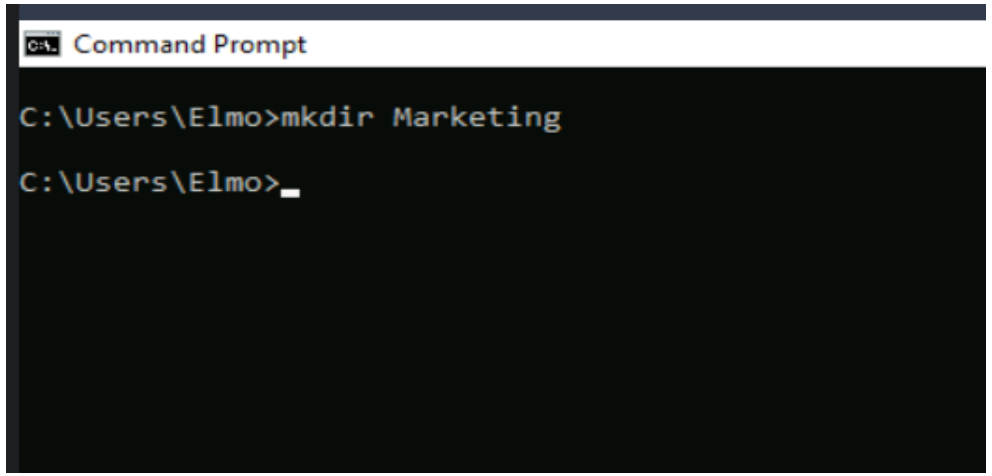
2

```
C:\Users\Public>cd Documents

C:\Users\Public\Documents>cd..

C:\Users\Public>cd Downloads

C:\Users\Public\Downloads>cd ..\Documents

C:\Users\Public\Documents>cd \

C:\>cd Windows\System

C:\Windows\System>cd %homepath%

C:\Users\TroyAthmann>_
```

mkdir/rmdir

1

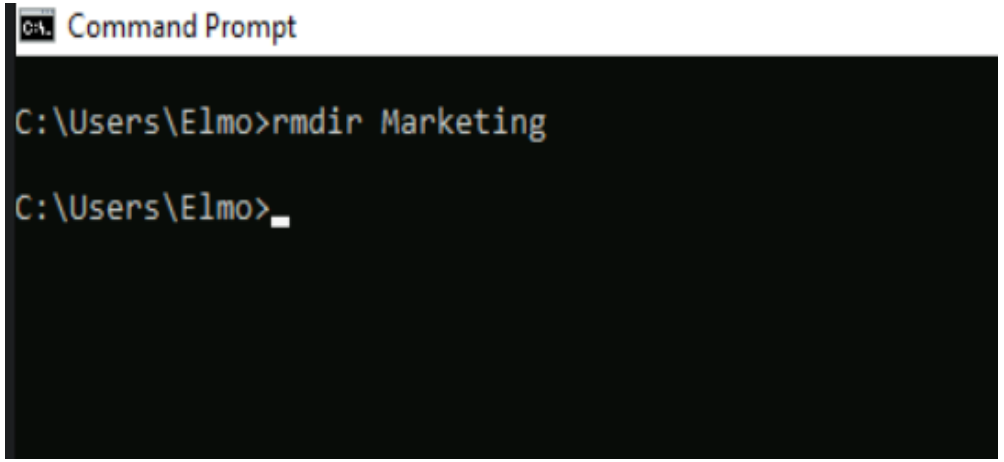
mkdir or md creates a directory.



2

rmdir – removes (deletes) a directory.

You can't delete a directory that contains files, including hidden or system files. You can not delete the current working directory.



copy

Copies one or more files from the source location to the specified destination.

Can be used in Recovery Console.

```
COPY [/D] [/V] [/N] [/Y | /-Y] [/Z] [/L] [/A | /B ] source [/A | /B]
    [+ source [/A | /B] [+ ...]] [destination [/A | /B]]

  source       Specifies the file or files to be copied.
  /A           Indicates an ASCII text file.
  /B           Indicates a binary file.
  /D           Allow the destination file to be created decrypted
  destination  Specifies the directory and/or filename for the new file(s).
  /V           Verifies that new files are written correctly.
  /N           Uses short filename, if available, when copying a file with a
               non-8dot3 name.
  /Y           Suppresses prompting to confirm you want to overwrite an
               existing destination file.
  /-Y          Causes prompting to confirm you want to overwrite an
               existing destination file.
  /Z           Copies networked files in restartable mode.
  /L           If the source is a symbolic link, copy the link to the target
               instead of the actual file the source link points to.
```

xcopy

1

Copies files and directories, including subdirectories.

More functionality than copy; its default behavior is only to copy files and not subdirectories inside of a folder unless you use the /s switch in the command.

robocopy

2

Copies file data from one location to another. More robust then **xcopy**

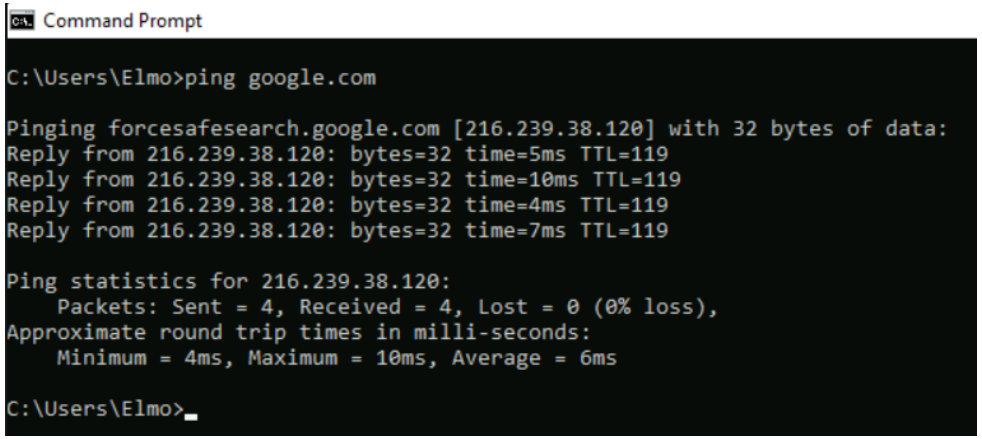
robocopy, unlike **xcopy**, can be used to mirror — or synchronize — directories.

ping

1

A powerful tool used to test device network connectivity

Can use FQDN or IP address



2

The ping switch -n will set the quantity of pings, or -t, for continuous ping attempts.

Commands are as follows:

ping -n 2 8.8.8.8 will ping the target twice

ping -t 8.8.8.8 will continuously perform pings until it is manually stopped

ping -n 2 acilearning.com will ping target x4 (bonus: it also displays the resolved IP address)

tracert

1

Displays the number of hops through Routers between two devices with a three-ping set being sent with a TTL=1 and incrementing by 1 to TTL=30 or upon reaching the destination.

Can use FQDN or IP address

A useful tool for troubleshooting connection paths,

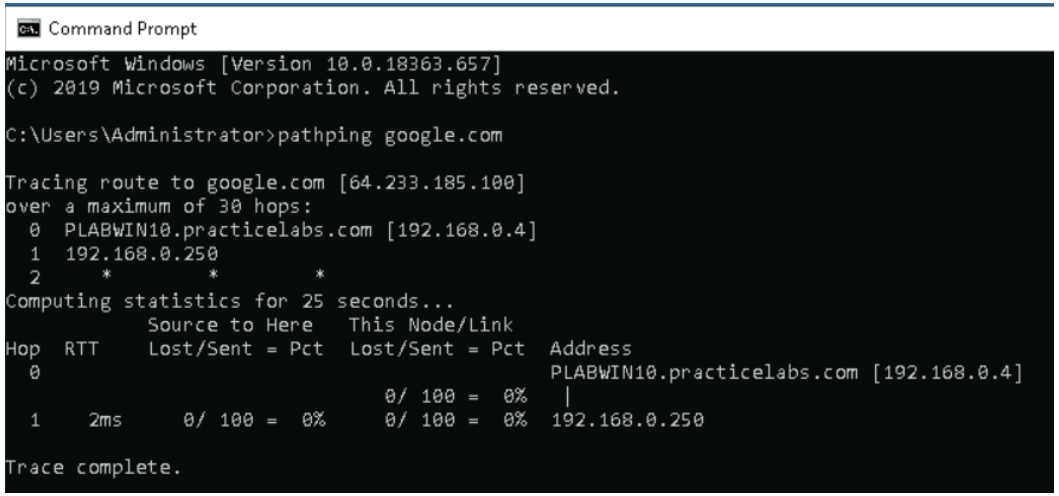
2

```
C:\Windows\system32>tracert acilearning.com

Tracing route to acilearning.com [143.204.29.64]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  ZenWiFi_ET8-B360 [192.168.50.1]
  2     1 ms    <1 ms    <1 ms  modem.Home [192.168.61.1]
  3    23 ms    27 ms    22 ms  hlrn-dsl-gw01.hlrn.qwest.net [207.225.112.1]
  4    23 ms    27 ms    22 ms  63-225-124-1.hlrn.qwest.net [63.225.124.1]
  5    23 ms    23 ms    23 ms  99.82.182.192
  6     *        *        *     Request timed out.
  7    24 ms    24 ms    24 ms  52.93.74.225
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11     *        *        *     Request timed out.
 12     *        *        *     Request timed out.
 13    23 ms    22 ms    22 ms  server-143-204-29-64.den50.r.cloudfront.net [143.204.29.64]

Trace complete.

C:\Windows\system32>
```

pathping

1

Provides information about network latency and network loss at intermediate hops between a source and destination. Works like **tracert** but with a little more info.



2

This command sends multiple echo Request messages to each router between a source and destination over a period and then computes results based on the packets returned from each router.

Because this command displays the degree of packet loss at any router or link, so you can determine which routers or subnets might be experiencing network problems.

pathping

1

The first step (top) is to determine the path like tracert.

2

The second step (below the orange line) is to collect and report the statistics of 100 pings to each router in the path.

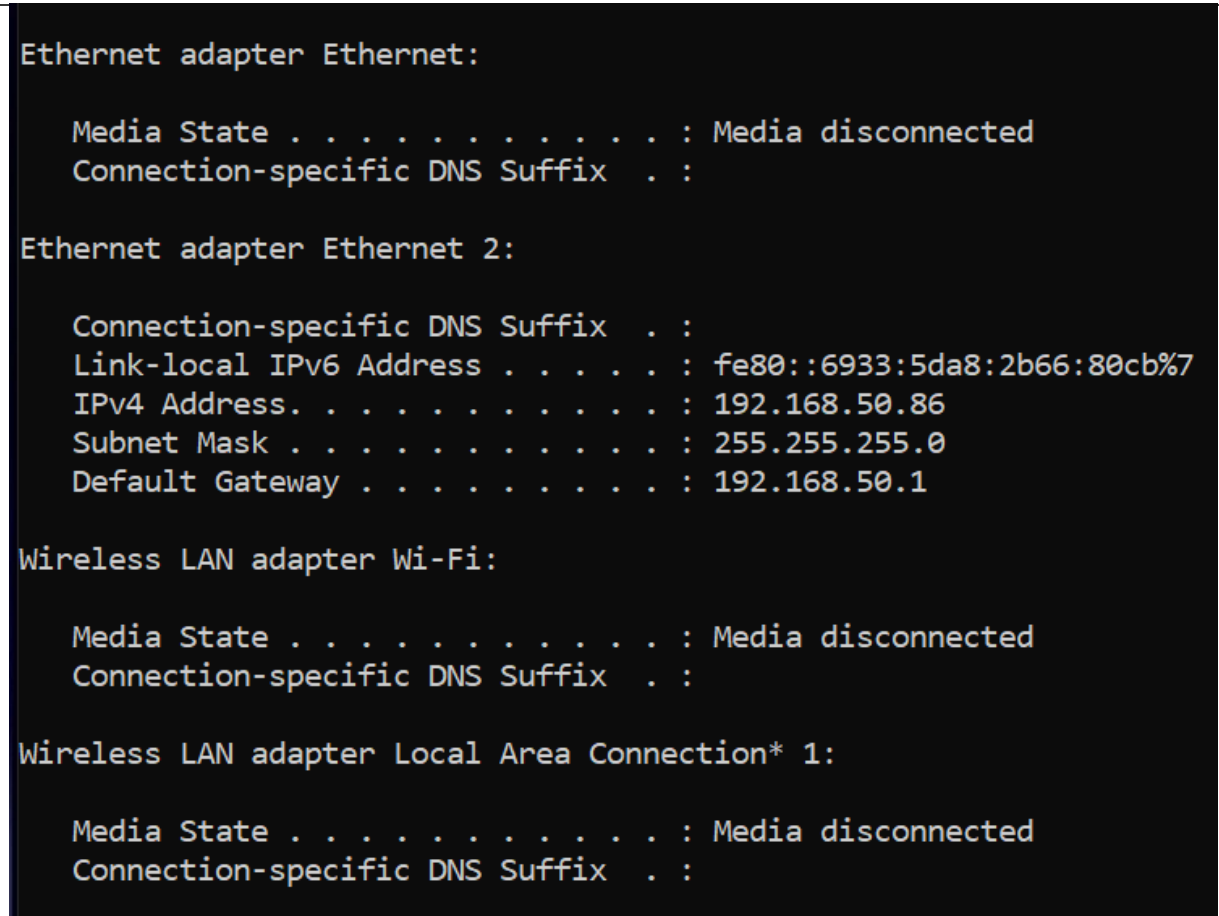
```
C:\Users\TroyAthmann>pathping athmann.org

Tracing route to athmann.org [74.208.236.155]
over a maximum of 30 hops:
  0  TATHMANN-22 [192.168.50.86]
  1  ZenWiFi_ET8-B360 [192.168.50.1]
  2  modem.Home [192.168.61.1]
  3  hlrn-dsl-gw01.hlrn.qwest.net [207.225.112.1]
  4  63-225-124-1.hlrn.qwest.net [63.225.124.1]
  5     *        *        *
Computing statistics for 100 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                           TATHMANN-22 [192.168.50.86]
                                 0/ 100 =  0%   |
  1    0ms     0/ 100 =  0%     0/ 100 =  0%  ZenWiFi_ET8-B360 [192.168.50.1]
                                 0/ 100 =  0%   |
  2    0ms     0/ 100 =  0%     0/ 100 =  0%  modem.Home [192.168.61.1]
                                 0/ 100 =  0%   |
  3   23ms     0/ 100 =  0%     0/ 100 =  0%  hlrn-dsl-gw01.hlrn.qwest.net [207.225.112.1]
                                 0/ 100 =  0%   |
  4   24ms     0/ 100 =  0%     0/ 100 =  0%  63-225-124-1.hlrn.qwest.net [63.225.124.1]

Trace complete.
```

ipconfig

1

Displays Windows Network Configuration of the device

The default output is Link-local IPv6; IPv4 addresses, MAC addresses, IP addresses, Subnet Mask and Gateway.



Ipconfig /all

The /all parameter is more verbose with MAC address, DHCP info, Gateway, DNS Servers, etc.

/release and /renew parameters manage the DHCP IP address lease

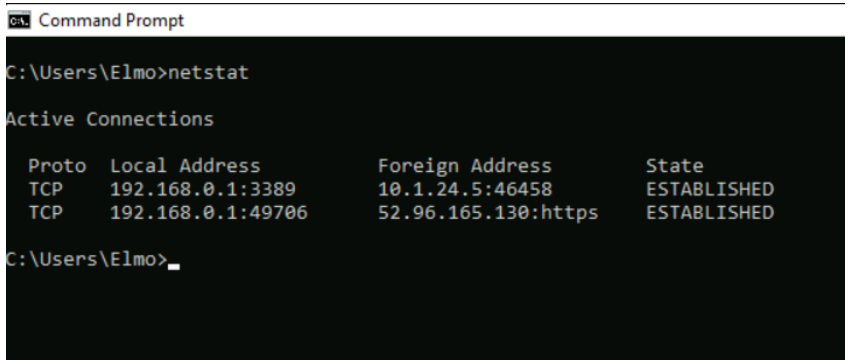
/displaydns, /flushdns, and registerdns parameters are used to display, flush or register DNS, respectively.

```
C:\Users\TroyAthmann>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : TATHMANN-22
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek USB GbE Family Controller
   Physical Address. . . . . . . . . : 00-E0-4C-B5-CD-46
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : ASIX AX88179 USB 3.0 to Gigabit Ethernet Adap
   Physical Address. . . . . . . . . : 00-05-1B-C3-64-0C
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::6933:5da8:2b66:80cb%7(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.50.86(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Friday, July 29, 2022 2:45:07 PM
   Lease Expires . . . . . . . . . . : Saturday, July 30, 2022 2:45:06 PM
   Default Gateway . . . . . . . . . : 192.168.50.1
   DHCP Server . . . . . . . . . . . : 192.168.50.1
   DHCPv6 IAID . . . . . . . . . . . : 637535515
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2A-17-BE-C1-8C-B8-7E-6E-40-24
   DNS Servers . . . . . . . . . . . : 192.168.50.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

netstat

1

Displays active TCP & UDP Statistics for the ports on the local system. The default shows only active ports and the following columns of information: protocol, local address, foreign address, state of the connection.



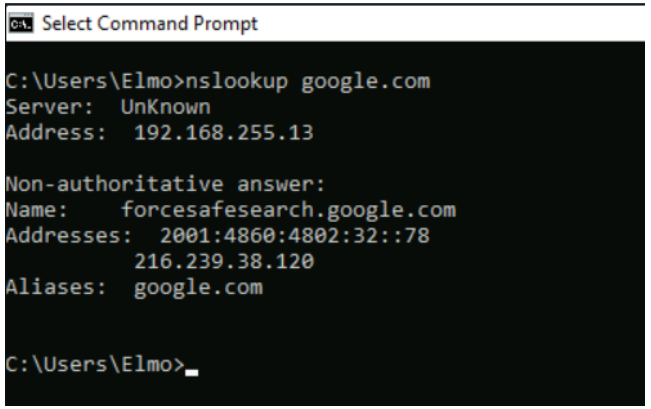
2

It is useful for troubleshooting network connectivity problems and a security overview of all the network activities and port availability.

nslookup

1

Displays information that you can be used to verify Domain Name System records and diagnose infrastructure problems.
The command resolves Domain names to IP Addresses.



2

https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/nslookup

chkdsk

1

Checks the file system and file system metadata of a volume for logical and physical errors.

If a bad sector is detected, **chkdsk** will inform the OS of the bad sector and tag it as such so that the OS will not write to that area again.

2

If used without parameters, chkdsk displays only the status of the volume and does not fix any errors. If used with the /f, /r, /x, or /b parameters, it fixes errors, accordingly, on the volume.

sfc

1

System File Check (sfc) scans and verifies the integrity of all protected system files and replaces incorrect versions with correct versions.

You must be logged on as a member of the Administrators group to run this command.

2

If this command discovers that a protected file has been compromised, it retrieves the correct version of the file from the systemroot\system32\dllcache folder and then replaces the incorrect file.

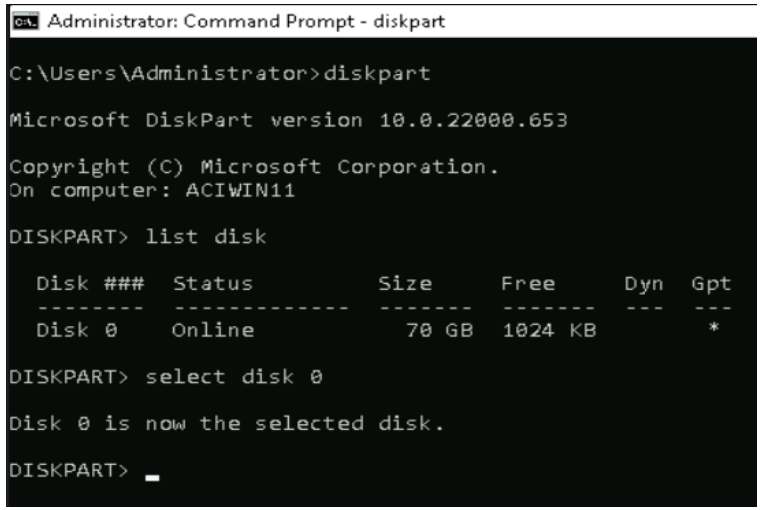
https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/sfc

diskpart

1

Helps manage your computer's drives (disks, partitions, volumes, or virtual hard disks).

https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/diskpart -



2

You must first list, and then select an object to modify. After an object has been selected, any **diskpart** commands that you type will act on the selected object.

an asterisk (*) appears next to the object that has been selected.

diskpart <parameter>

format

1

The Format command is used to remove all data from the disk. You must be a member of the Administrators group to format a hard drive.

Creates a new root directory and file system. It can also check for bad sectors on the disk. To be able to use a new disk, you must first use this command to format the disk.

2

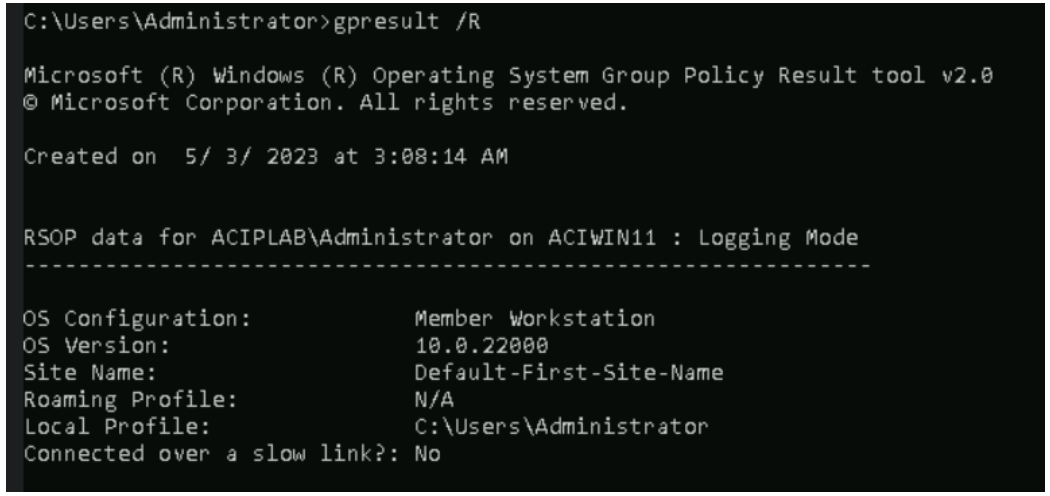
Can be used from the recovery console

https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/format -

gpresult

1

Displays the applied Group Policies for a local or domain-joined user and computer.
Executing the command will display the Resultant set of Policies (RSOP) report.



2

Group Policy is the primary administrative tool for defining and controlling how programs, network resources, and the operating system operate for users and computers in an organization. In an Active Directory environment, Group Policies are applied to users or computers based on their membership in sites, domains, or organizational units.

gupdate

1

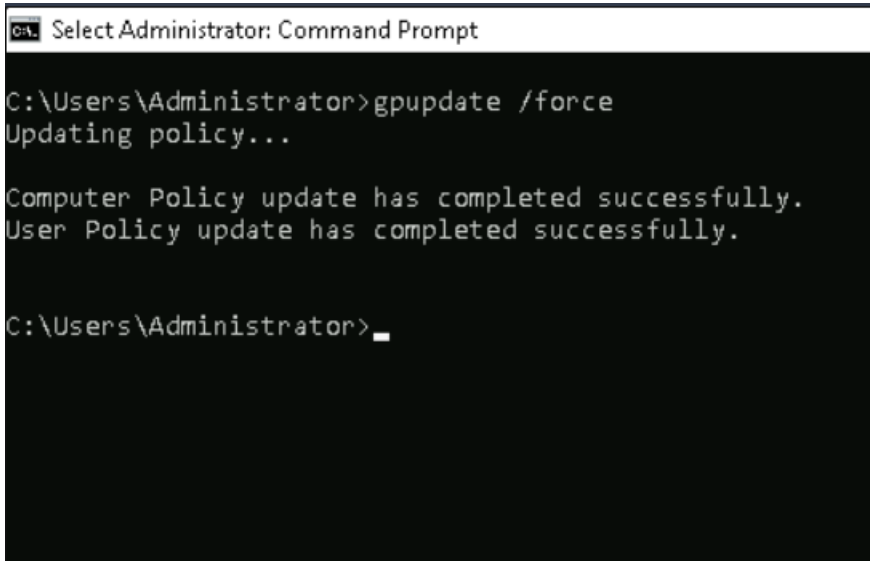
Updates Group Policy Settings for Users and Computers.

https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/gpupdate -

2

To force an update of all Group Policy settings, execute the following in the Command Prompt window:

gpupdate /force

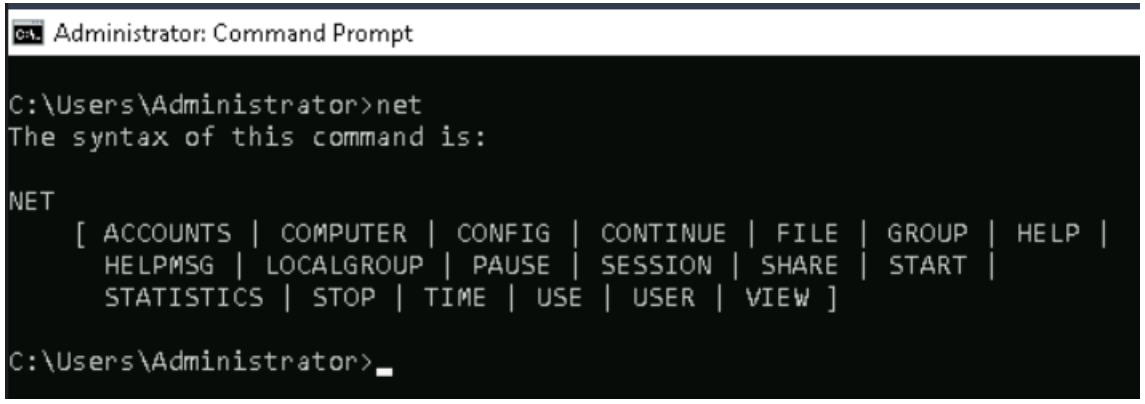


net

1

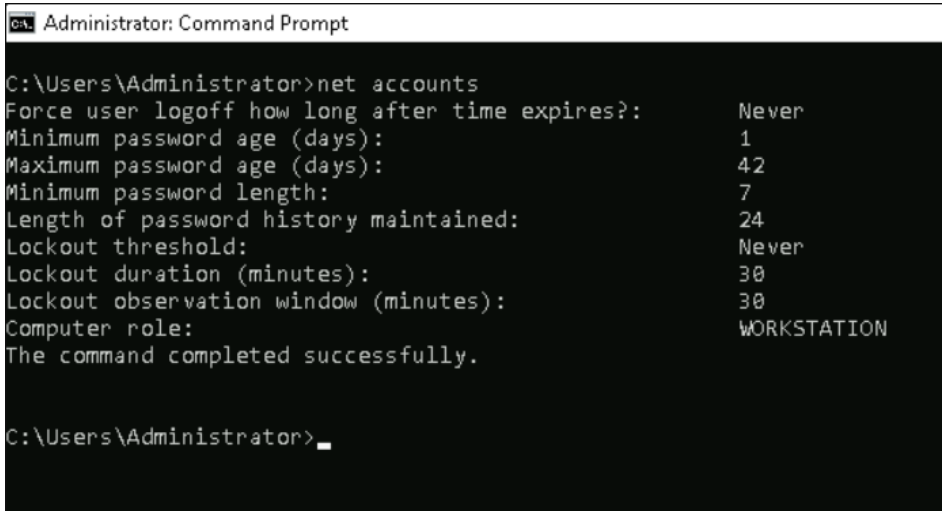
Manages almost any aspect of a network and its settings, including network shares, network print jobs, and network users. It can even manage some local system settings, for example, starting and stopping a service.

https://docs.microsoft.com/en-us/troubleshoot/windows-server/networking/net-commands-on-operating-systems -



2

Often used for troubleshooting and Administration of a Windows device.
Execute net Accounts in the Command Prompt window; the default settings of the Account Lockout policy and Password Policy in the local computer will be displayed.



Topic: Features and Tools of Windows 10

In this section, we will cover:

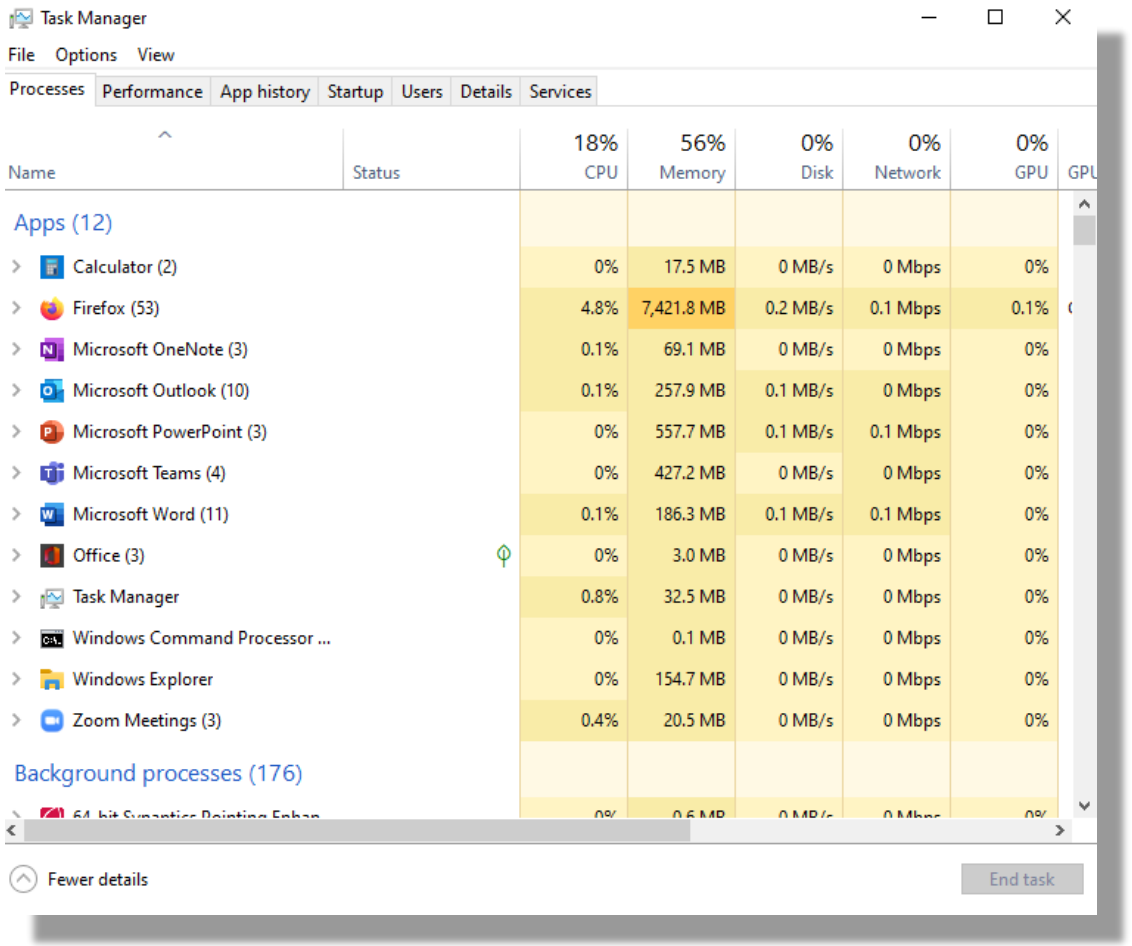
- Task Manager
- MS Management Console (MMC)
  - Event Viewer
  - Disk Management
  - Services
    - Device Manager
  - perfmon
  - Performance Monitor
  - Task Scheduler
  - compmgmt
  - Computer Management
  - msinfo32
- System Information
- Resource Monitor
- Local Security Policy
- System Configuration
- System Restore
- Disk Defragmenter
- Defragment and Optimize Drives
- Mobility Center
- Certificate Manager
- Local Users and Groups
- Disk Cleanup
- Windows Defender Firewall

Task Manager

There are several tabs for quick system assessment and a good starting point for troubleshooting the system. The tabs are:

- Processes
- Performance
- App History
- Startup
- Users
- Details
- Services

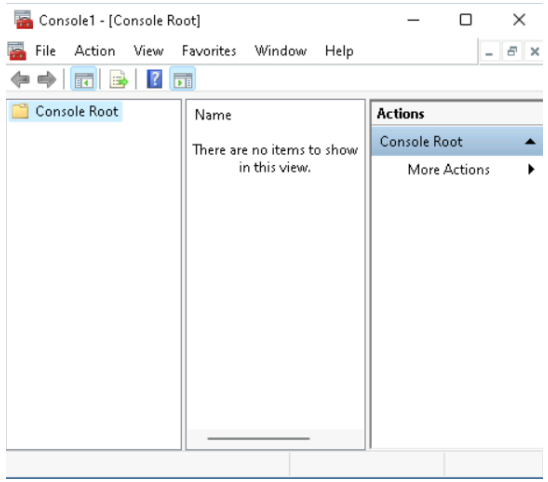
Task Manager is a Microsoft Windows tool for displaying several key resource consumption indicators.



mmc.exe

1

Microsoft Management Console is an Administrator program within Windows that allows access to advanced tools for managing desktops and servers.



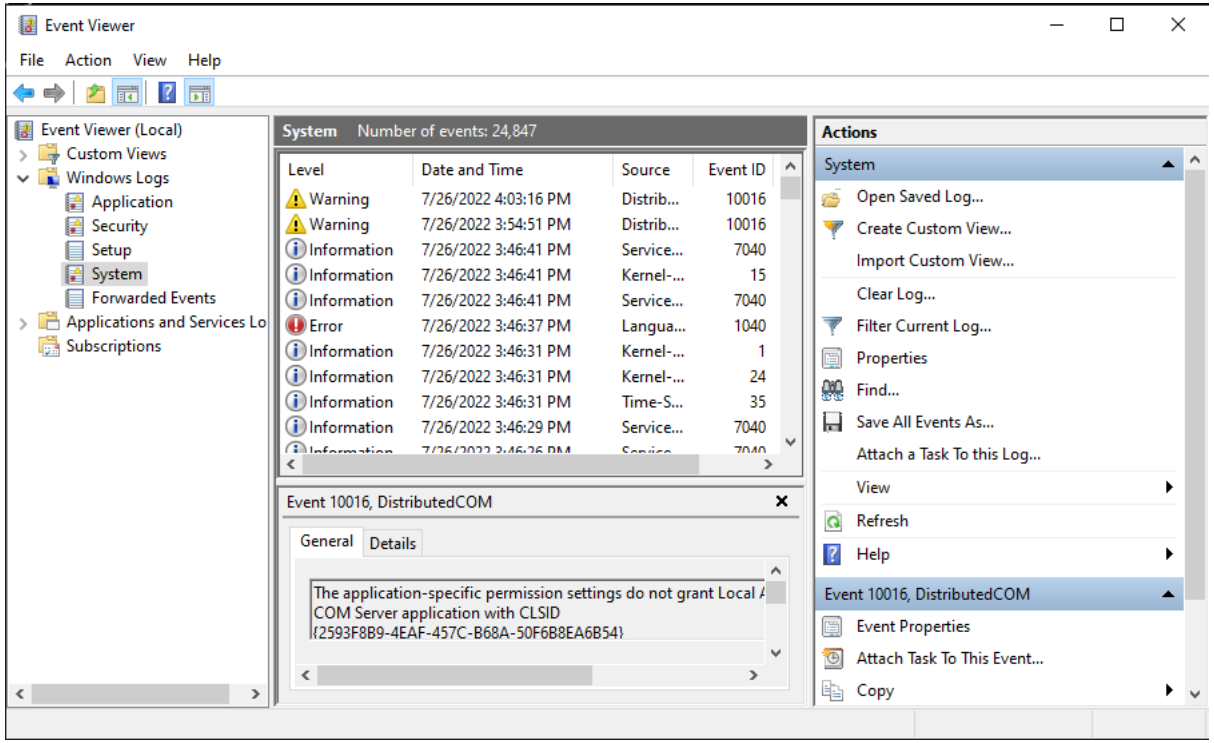
2

Framework for building custom Management Consoles using built-in snap-ins that offer various features for tasks and system management.

Event Viewer

Event Viewer is a log event console. The folder **Windows Logs** contains categories of frequently referenced events captured by Windows for troubleshooting.

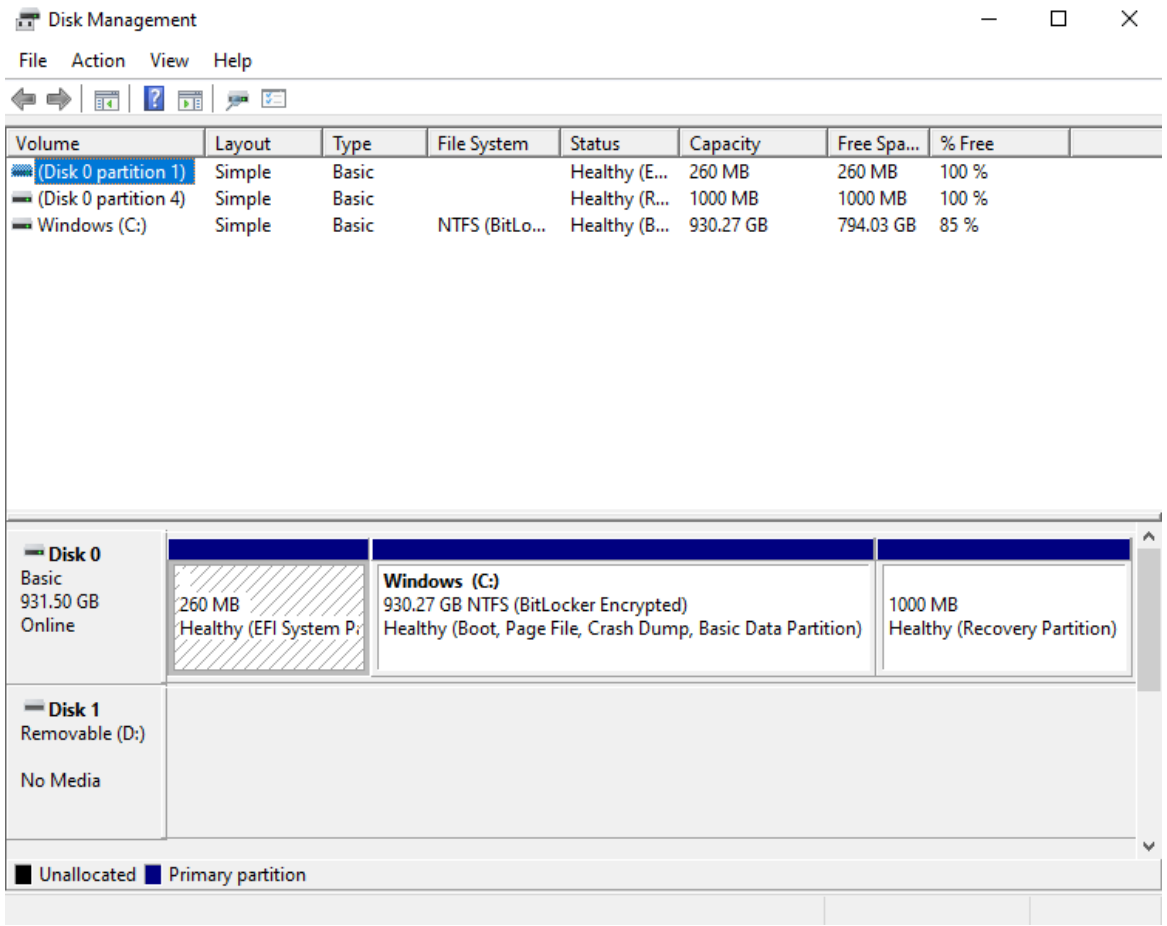
Setup is for capturing events related to software installations.
Application and **System** contain logs of installed software or system processes, respectively.
Security captures successful and failed login attempts for user accounts.



Disk Management

Disk Management is a tool used for monitoring and managing the attached hard drives.

This application is used for creating partitions, formatting drives, changing drive letters, and shrinking and extending volumes.



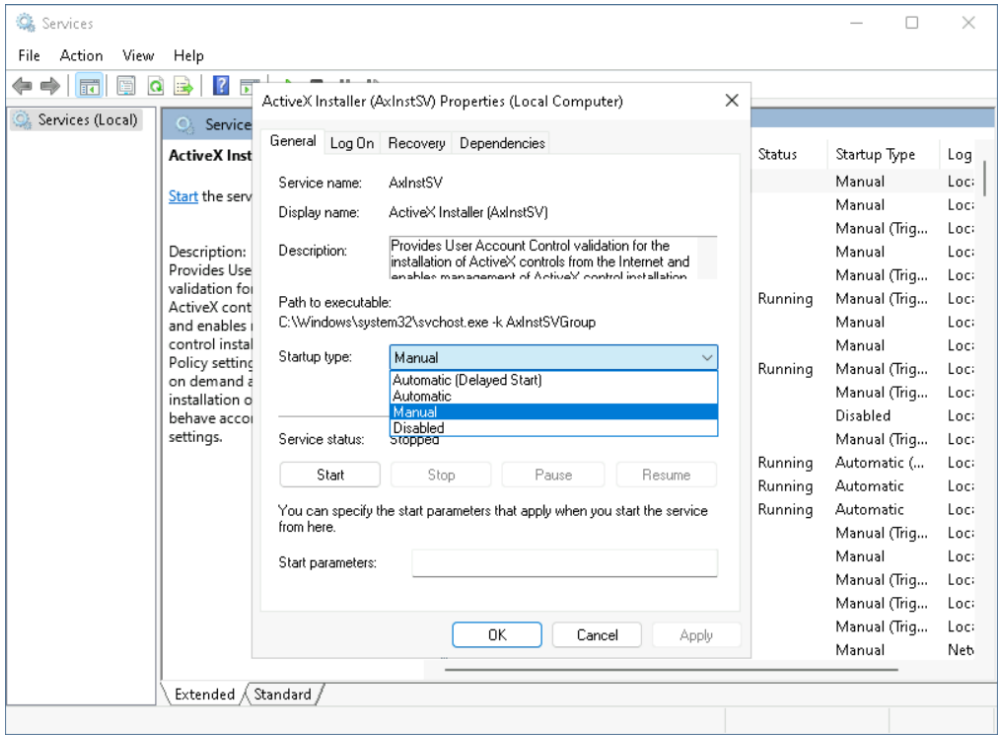
services.msc

1

The services.msc console provides a list of all services available on the device.
Type services.msc in the Windows run search box to open the Services console.

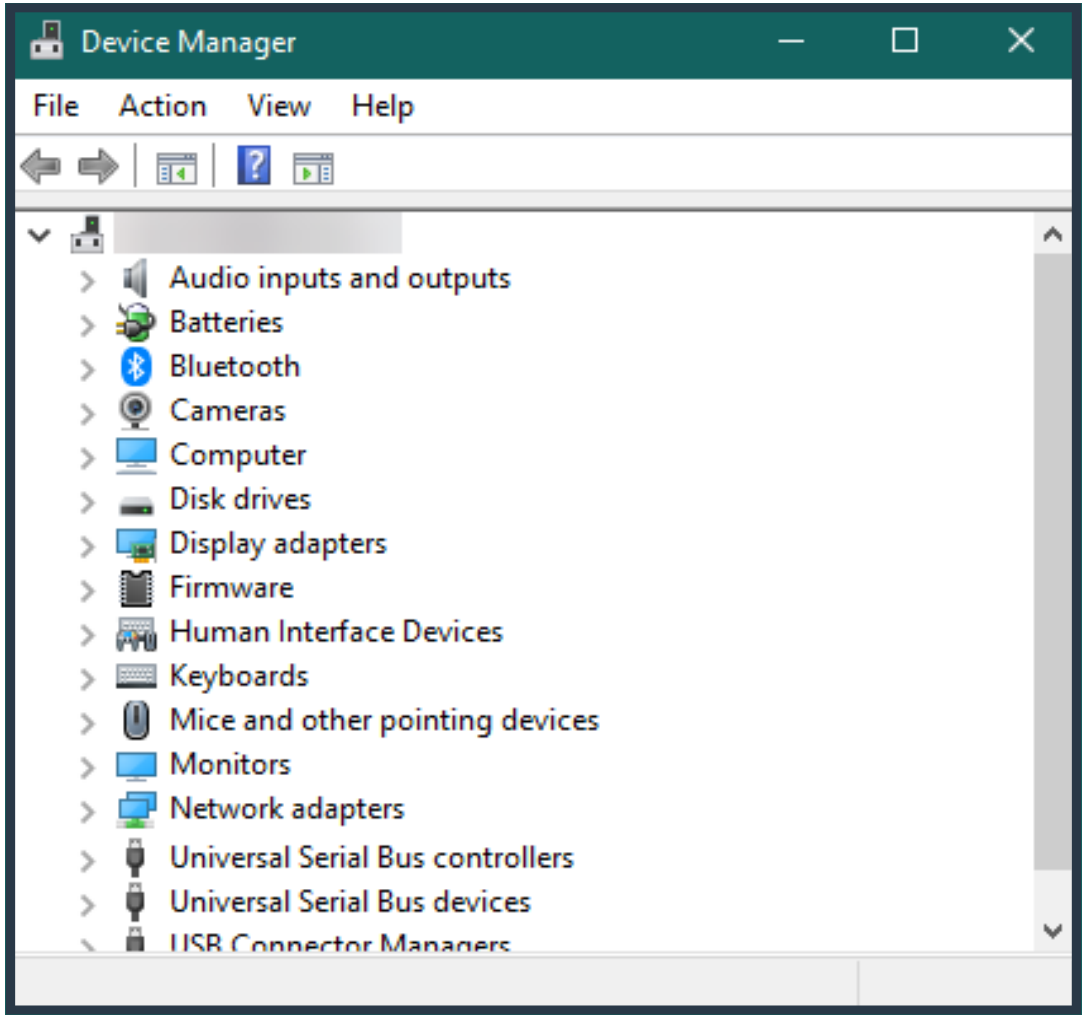
Its function is to manage how a service start when the device is powered on by selecting any of the following:
Automatic, delayed
automatic, manual, and disabled.

2



Device Manager

Device Manager is used to view the physical devices connected to the computer's motherboard, for example, USB thumb drives, network adapter cards, keyboards, etc.
Device drivers are specific software used to facilitate communication between the motherboard and the physical devices.

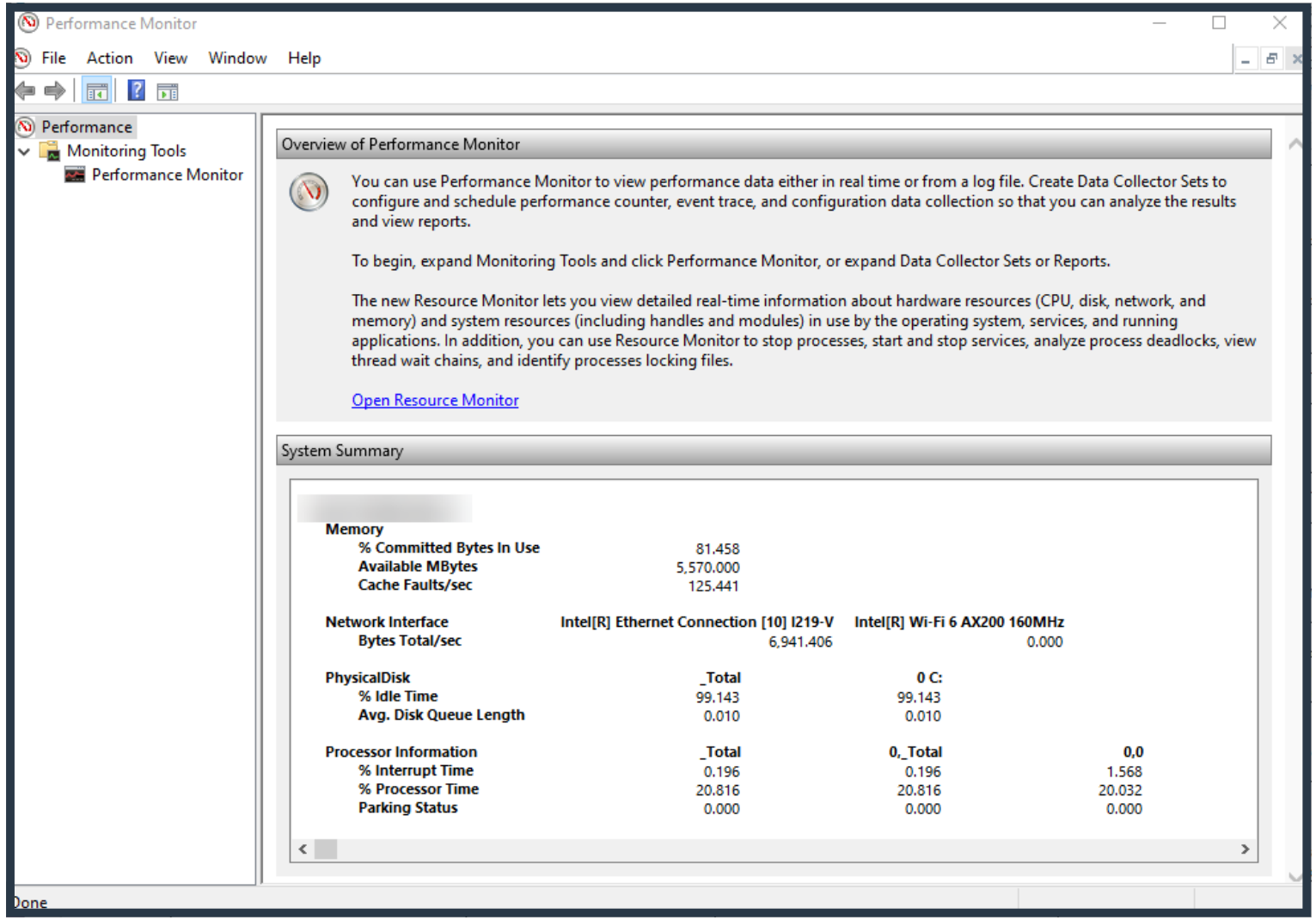


Performance Monitor

Performance Monitor monitors system resource usage — for example, the CPU, RAM, and network resource utilization.

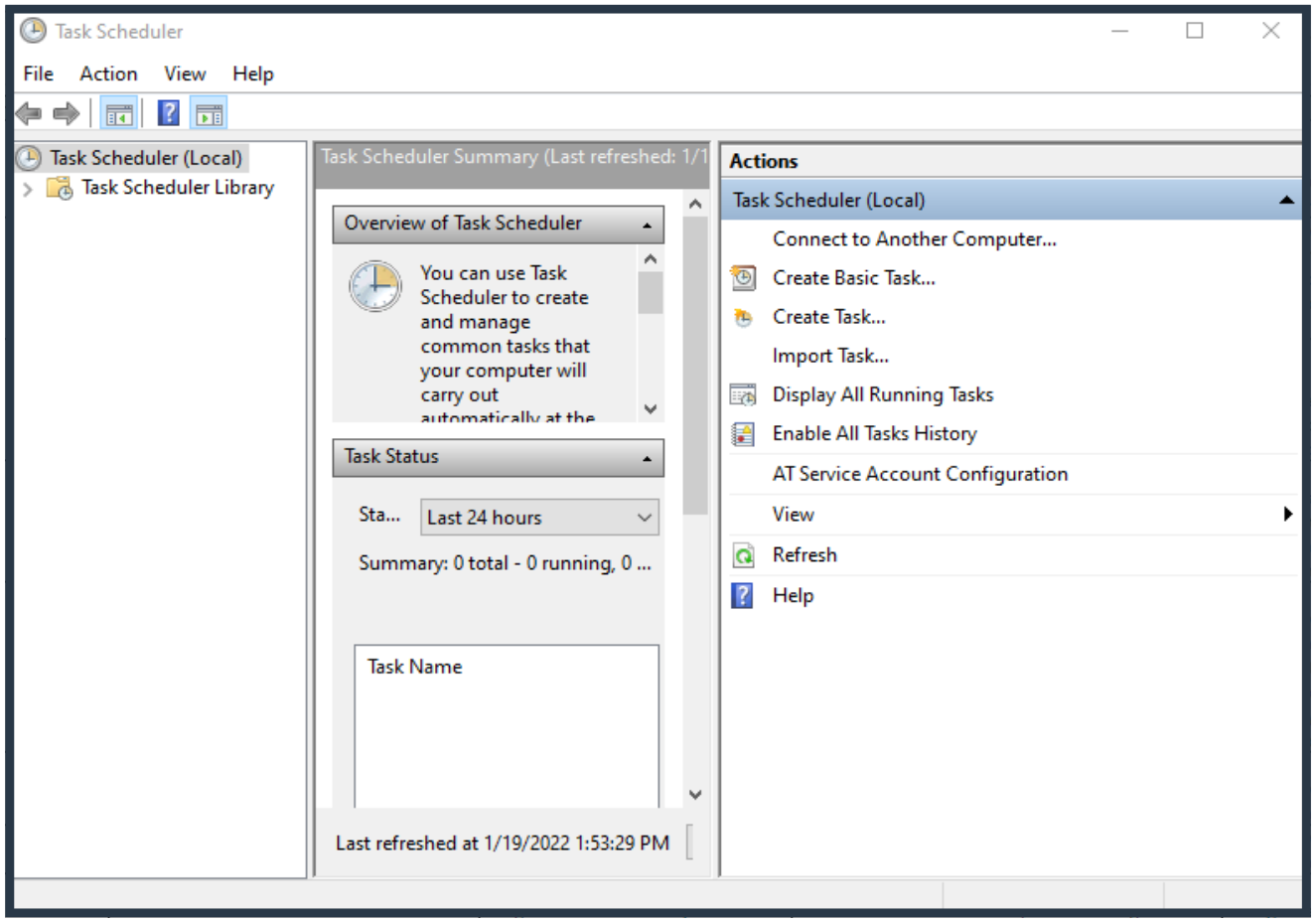
Type "perfmon.exe" in the Windows run search box.

Performance Monitor gives users the ability to log what users want to monitor and create baselines when the PC is running optimally for comparison later.



Task Scheduler

The Task Scheduler application can be used to schedule repetitive tasks on a Windows device, for example, running an anti-virus scan on a weekly basis.

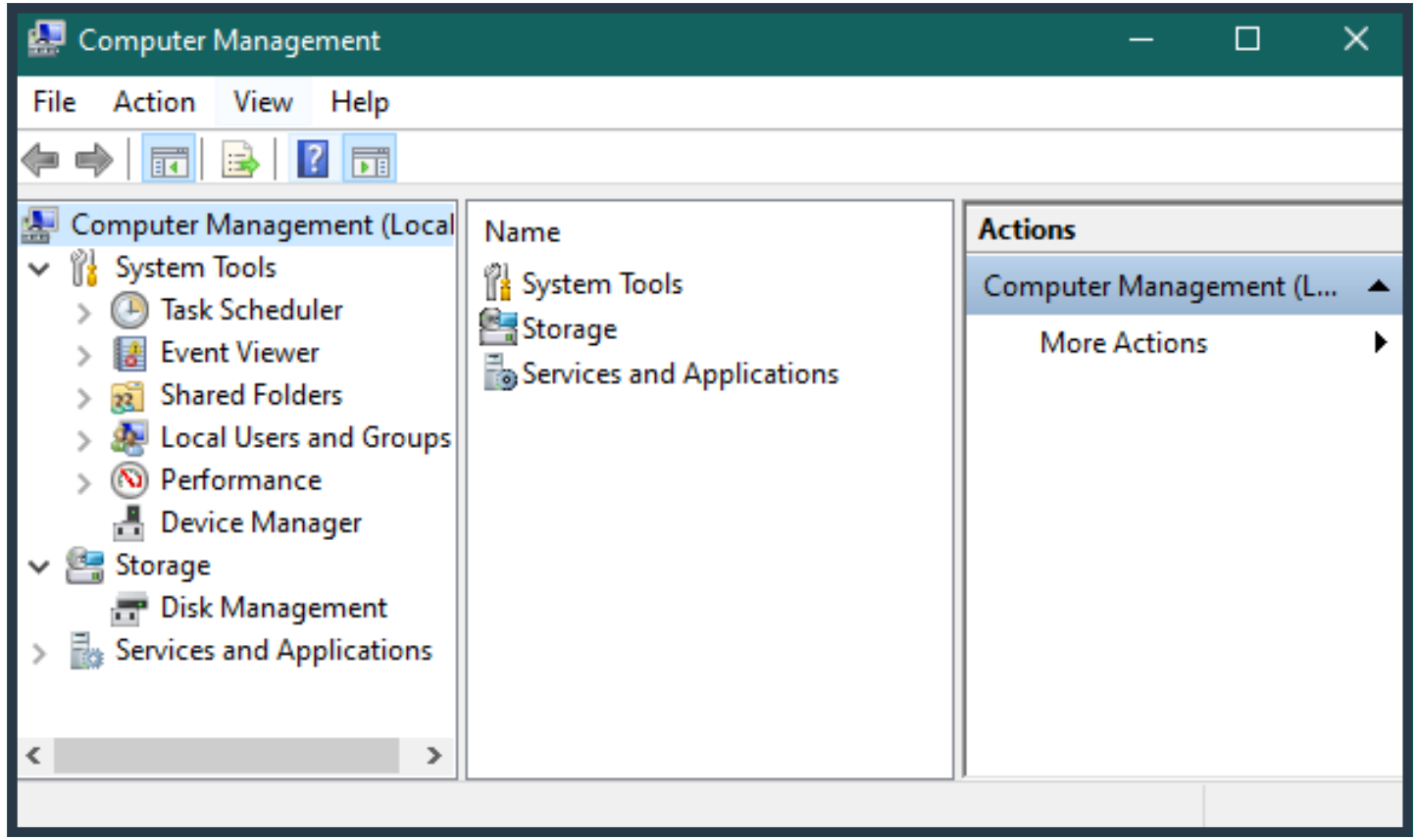


Computer Management

Computer Management is a system property application that allows users to view and manage system components.

Computer Management can be opened by right clicking Start and selecting Computer Management.

The Computer Management application is a central repository for Windows Device Management Tools.



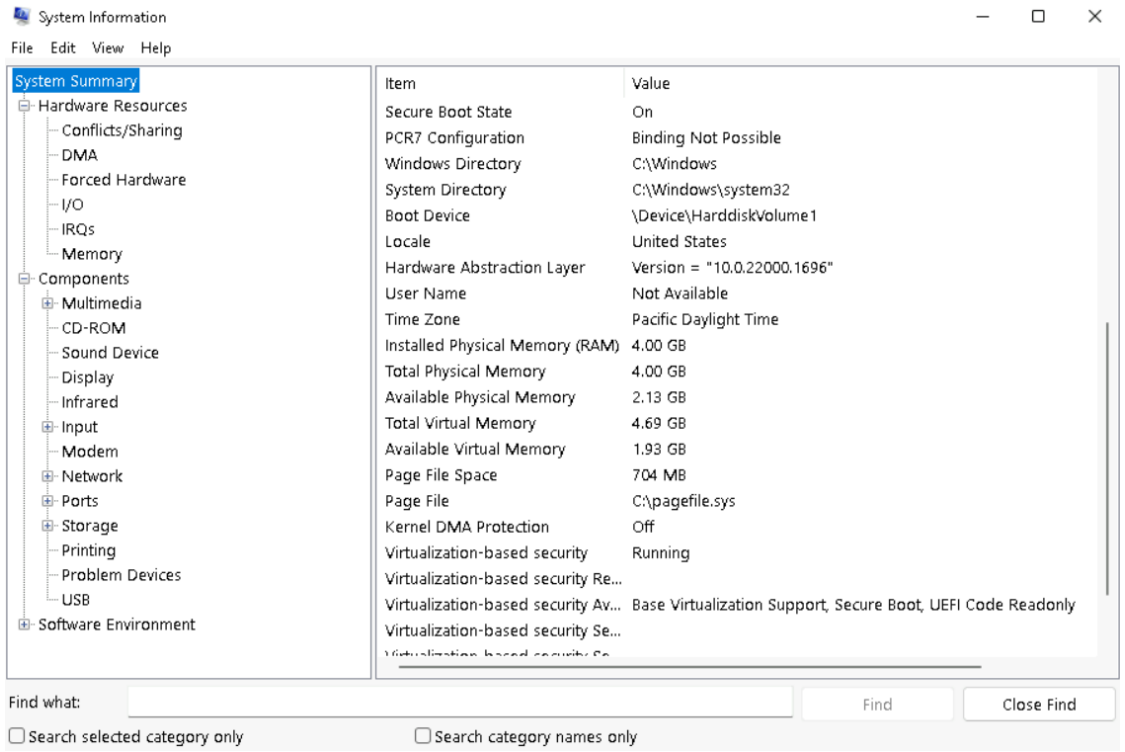
System Information (msinfo32.exe)

1

msinfo32.exe command is used to open the System Information window on Windows devices.

The System Information tool is used to display information about the device.
It displays information about the CPU, the amount of RAM installed, hard drive size and several other Hardware and Software components.

2

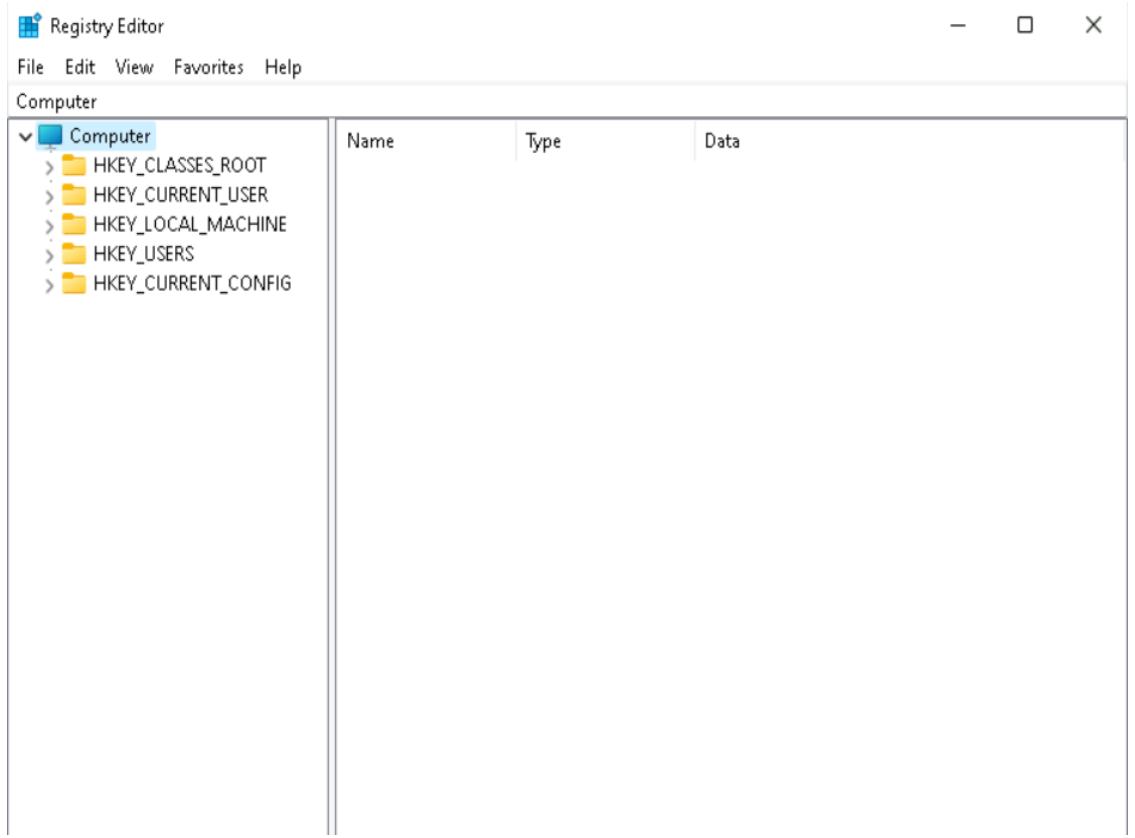


regedit.exe

1

The regedit.exe command is used to open the Registry Editor on a Windows device.
The application is a database of all the application and service configuration settings for the device.
Extreme care needs to be taken when making edits using the Registry Editor Application.

2

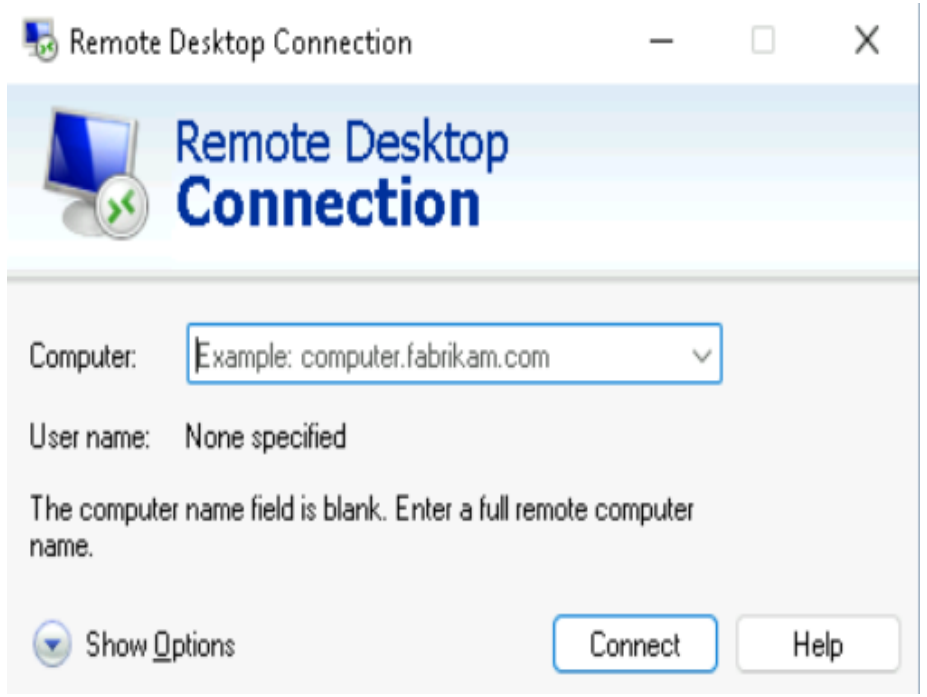


mstsc.exe

1

"mstsc.exe" stands for "Microsoft Terminal Services Client“. The application is used to connect o devices remotely on the network. When executing the command, the Remote Desktop Connection application opens.

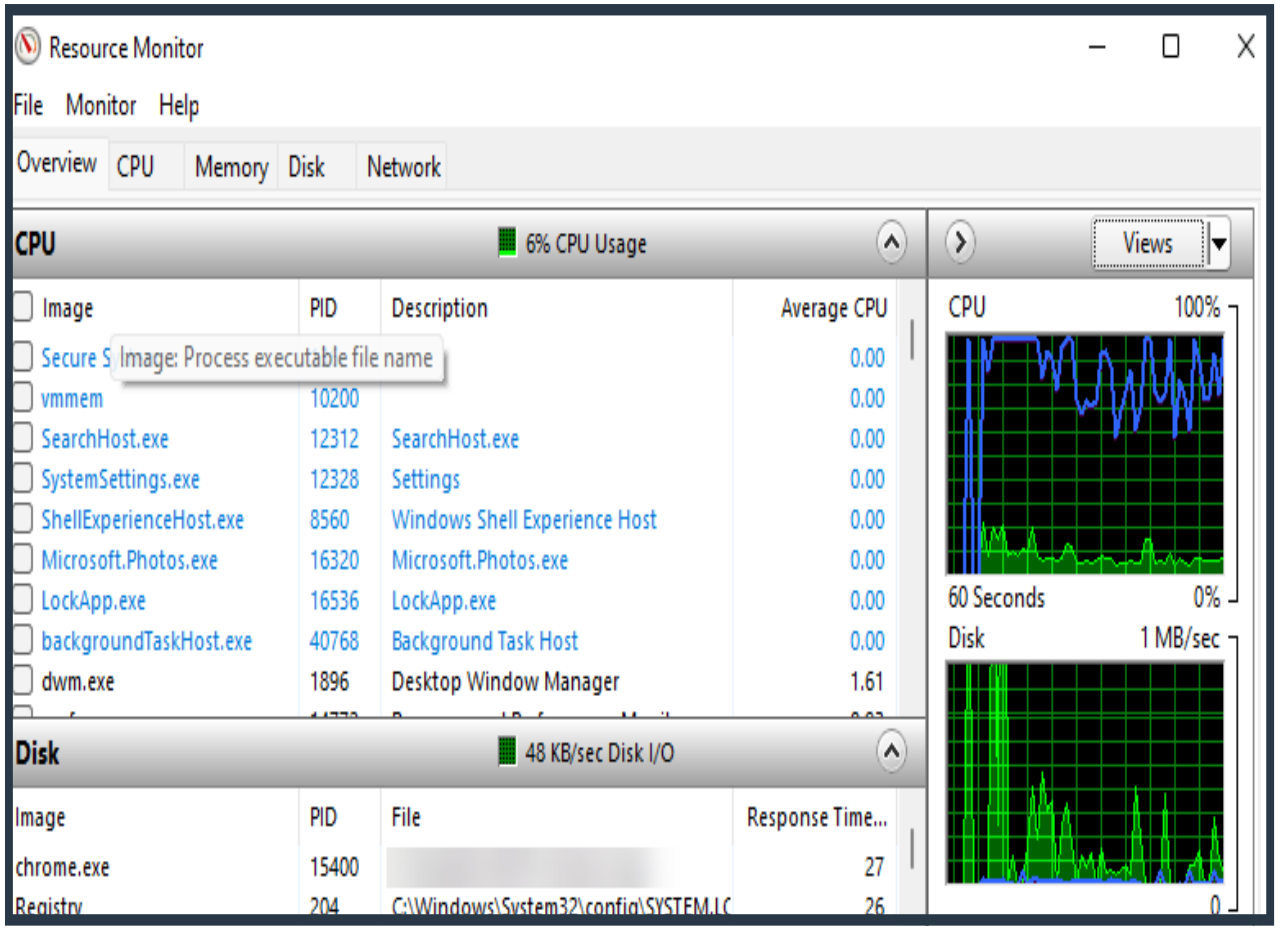
2



Resource Monitor

Resource Monitor application displays counters used to monitor system resource utilization of the device, for example, CPU, RAM and Network usage.

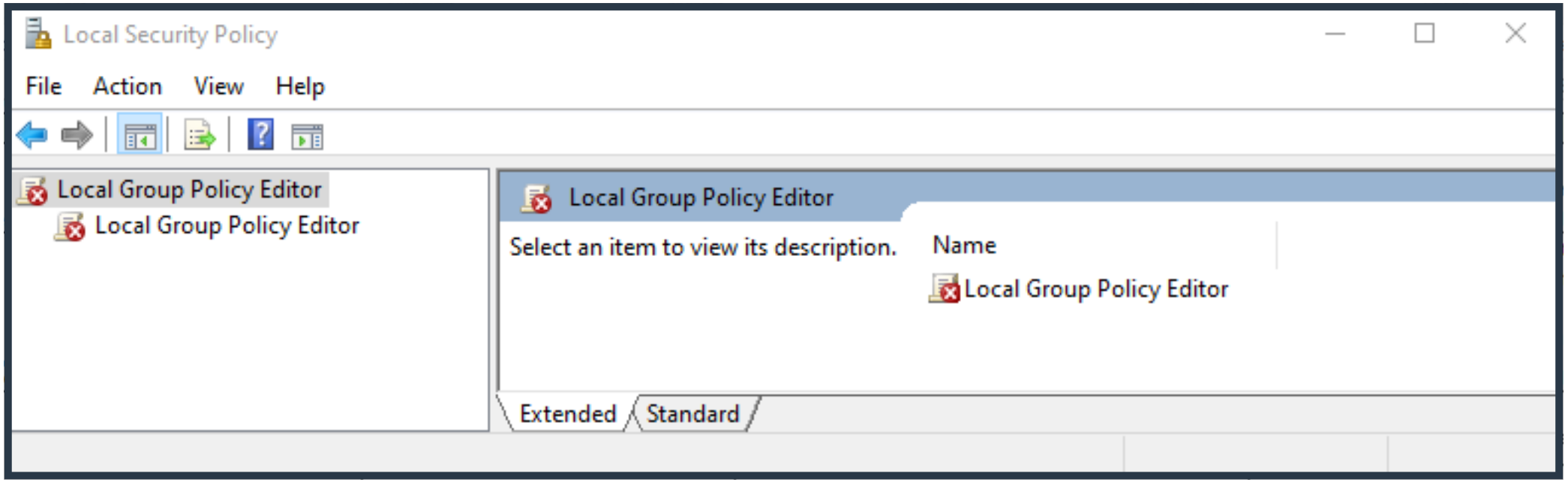
The Resource Monitor application can be opened by typing resmon.exe in the Windows Search bar.



Local Security Policy

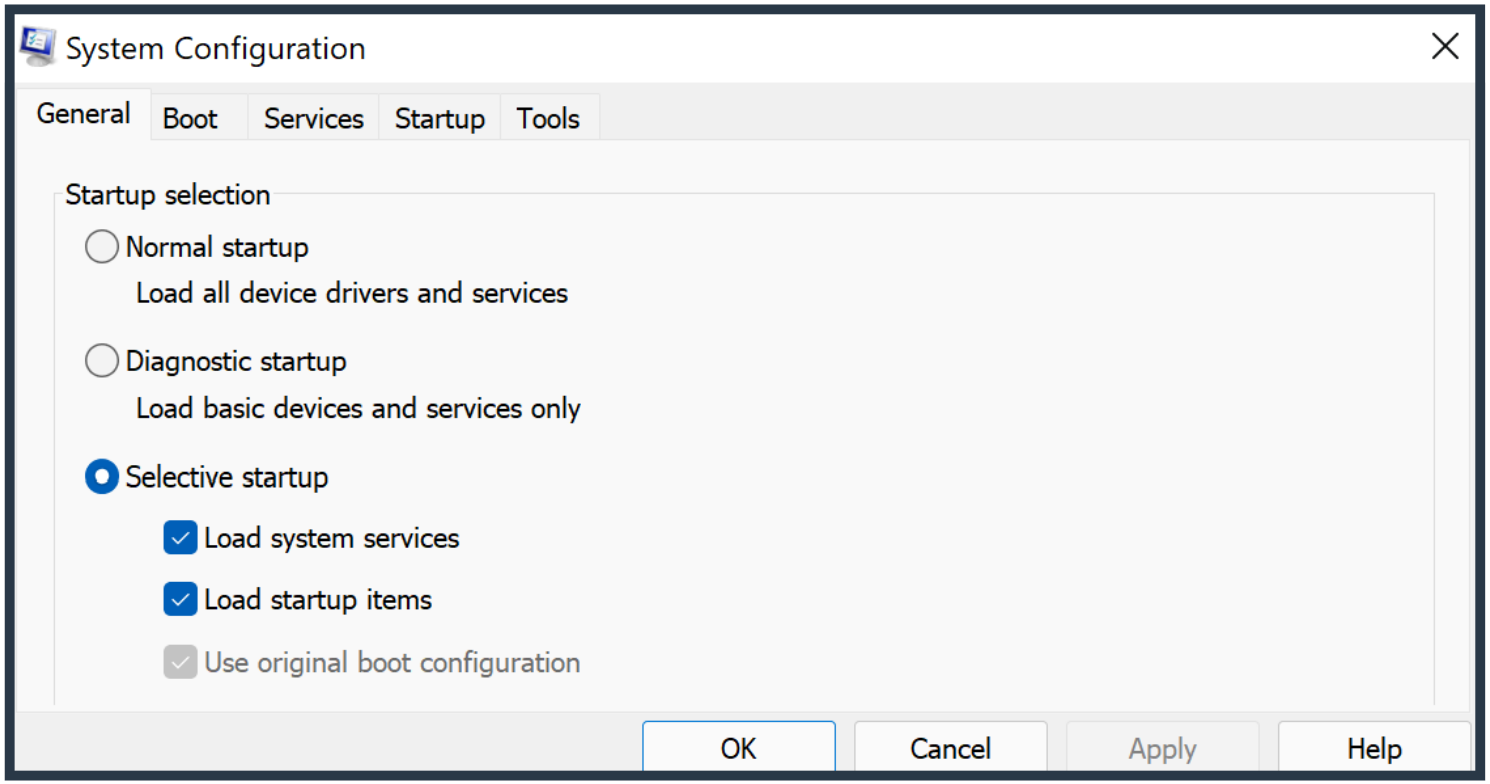
Local Security Policy is used to control the password policies of the local machine, which can be things like how long a password must be, how often to change a password, how many attempts a user can make with a password before their account is locked out, etc.

Type "SecPol" in the search bar or go to Control Panel > Administrative Tools > Local Security Policy.



System Configuration

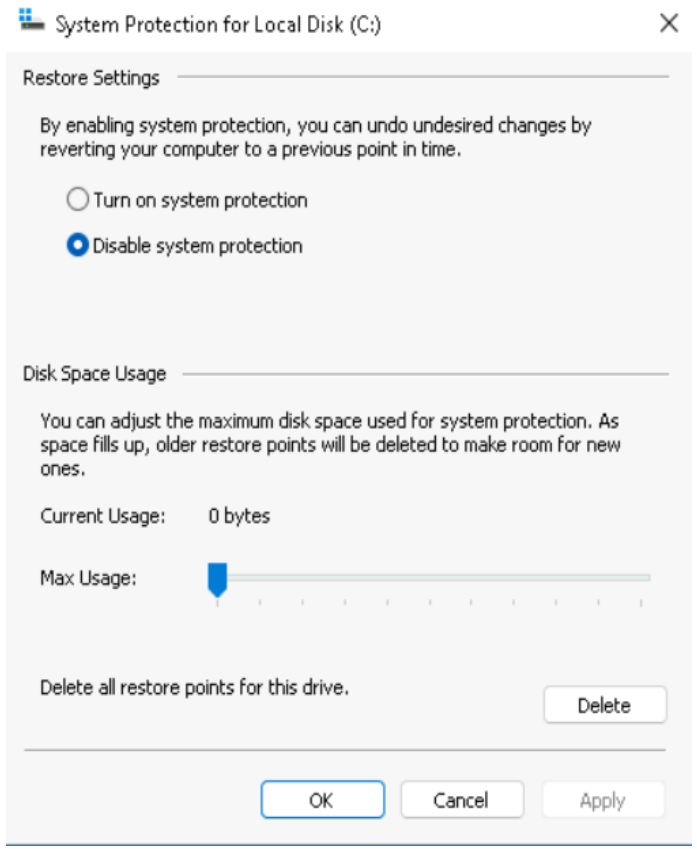
"msconfig.exe" is the executable file for System Configuration, which is a system properties window that allows a user to configure multiple settings like boot options, control on boot startup of applications, and see a list of troubleshooting tools with the startup commands for them.



System Protection

System Protection creates a snapshot of the computer's current configuration; it can be manually triggered as needed, or it will automatically create a restore point prior to system changes, like new software installs.

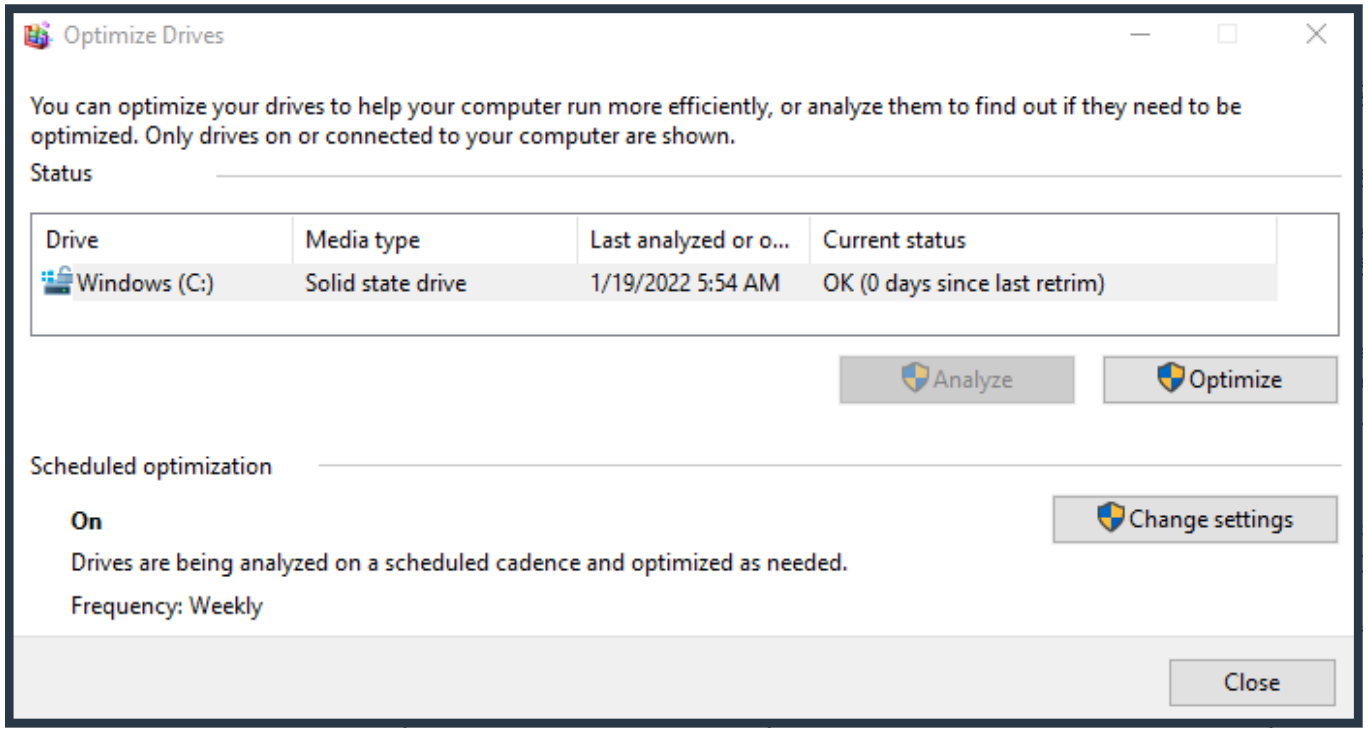
Type “Restore” in the Control Panel search box. Select “Create a restore point” > Opens System Properties > System Protection. System Protection settings can be enabled.



Disk Defragmenter

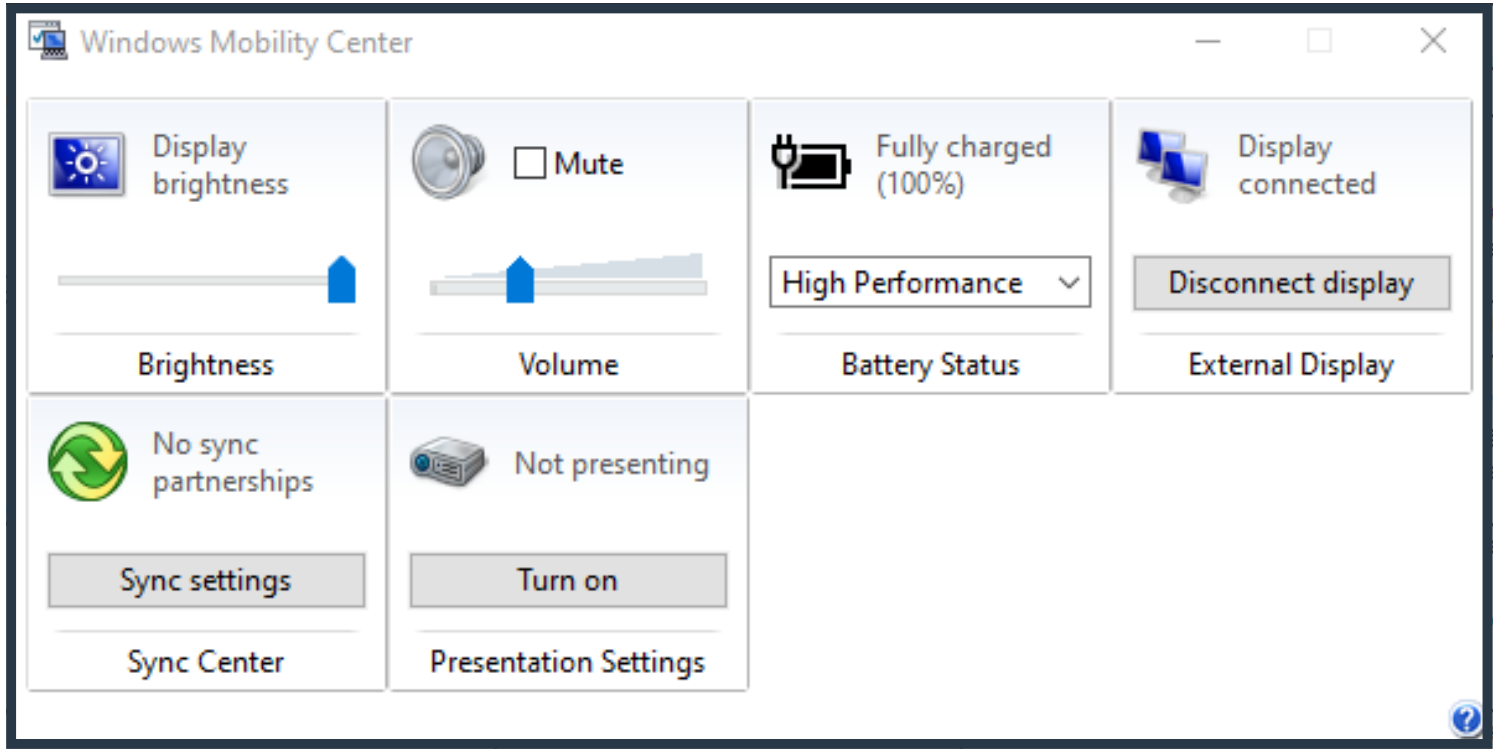
Disk Defragmenter is a function used when a computer is running slow, specifically slow drive performance. The computer will reorganize the scattered file segments on the hard drive to restore contiguous file segments.

“dfrgui.exe” is the command for Disk Defragmenter, now the Optimize Drives application.



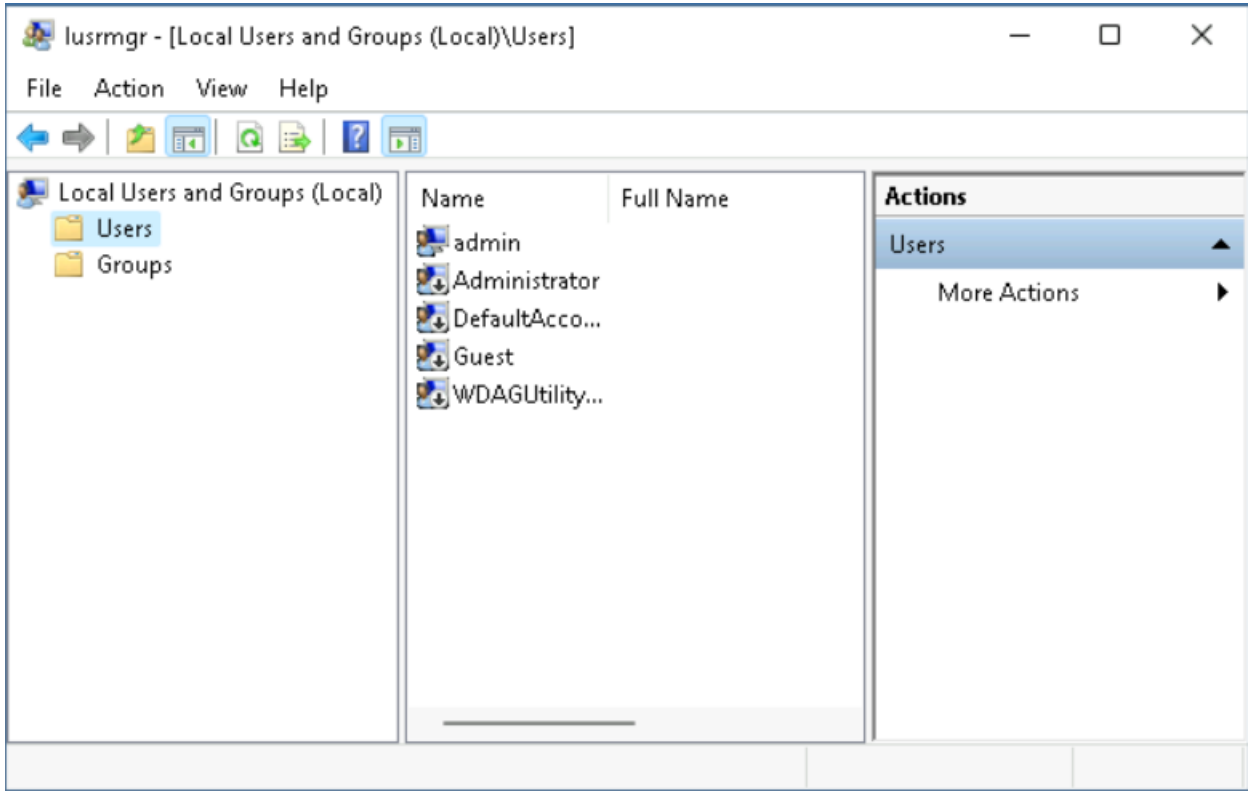
Mobility Center

The Mobility Center menu has Display Brightness, Sound, Battery, Monitor Connections, and Sync options — these are just generic, quick-access settings; you may need to go to the actual settings for more options.



Local Users and Groups

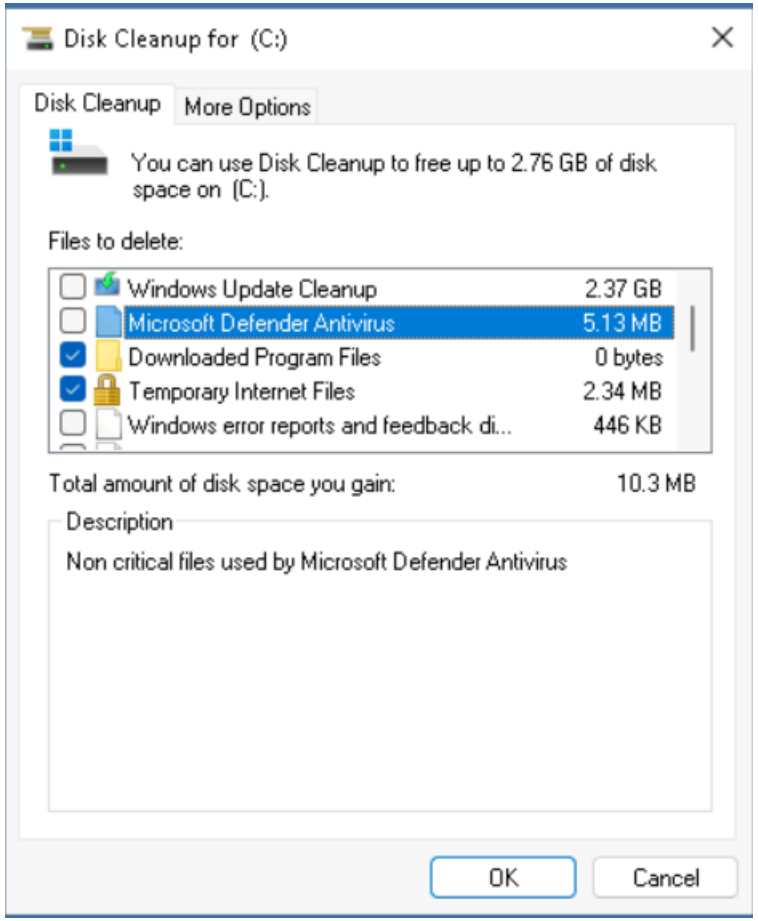
The lusrmgr.msc command is used to open the MMC snap-in for Local Users and Groups.
Local Users and Groups snap-in is used to manage the local user that has access to the device. It is used to create local users and groups and can also be used to manage user passwords.



“cleanmgr.exe” is the command used to open Disk Cleanup application.

The Disk Cleanup application removes temporary files from a Windows device and can be used to free up drive space.

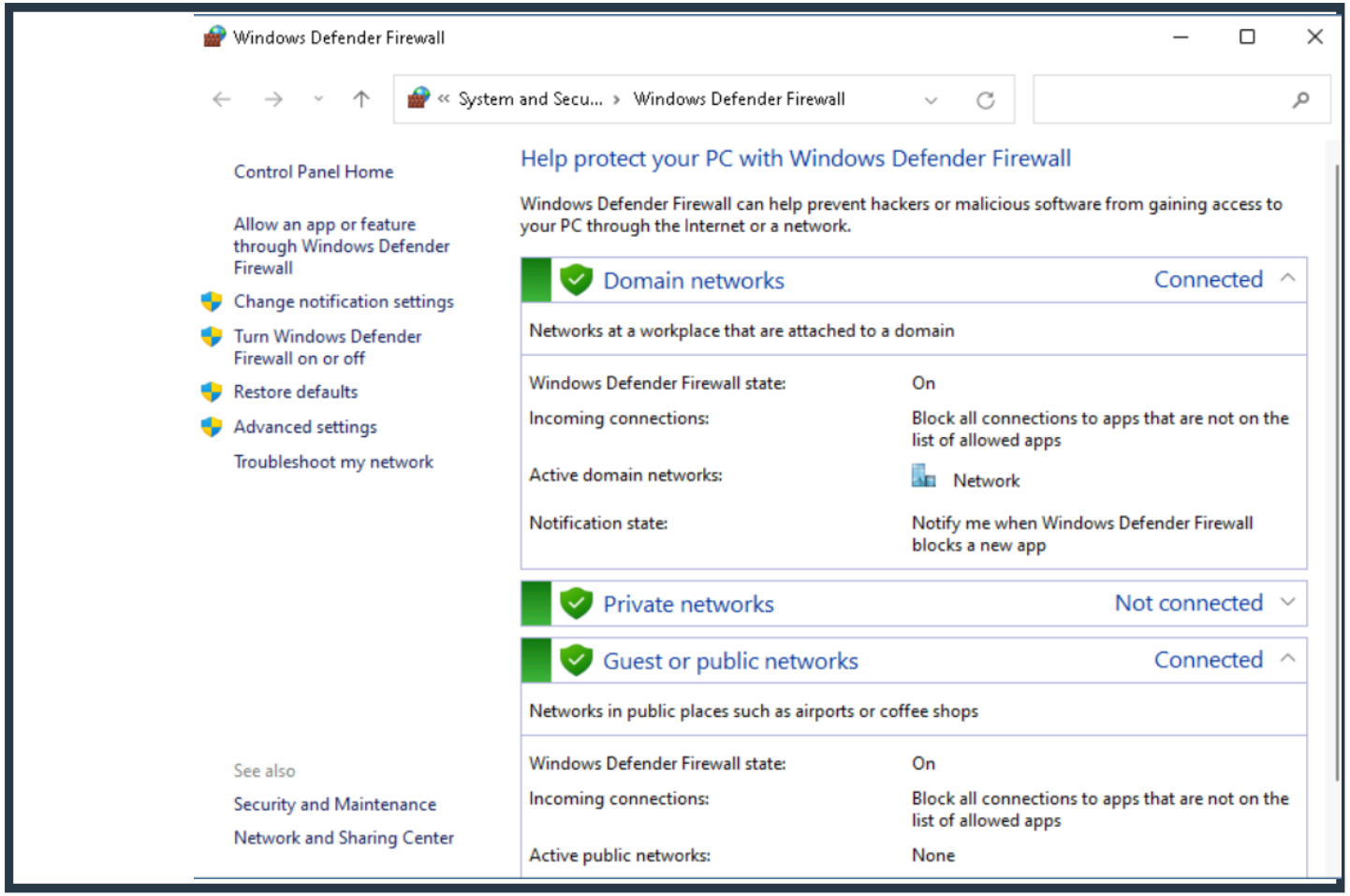
Disk Cleanup



Windows Defender Firewall

Windows Defender Firewall is a native component of the Windows Operating System and is used to filter network traffic on the device.

The Windows Defender Firewall application can be used to open or close ports on the device or allow a specific application to access the device.



Topic:
Control Panel Utilities

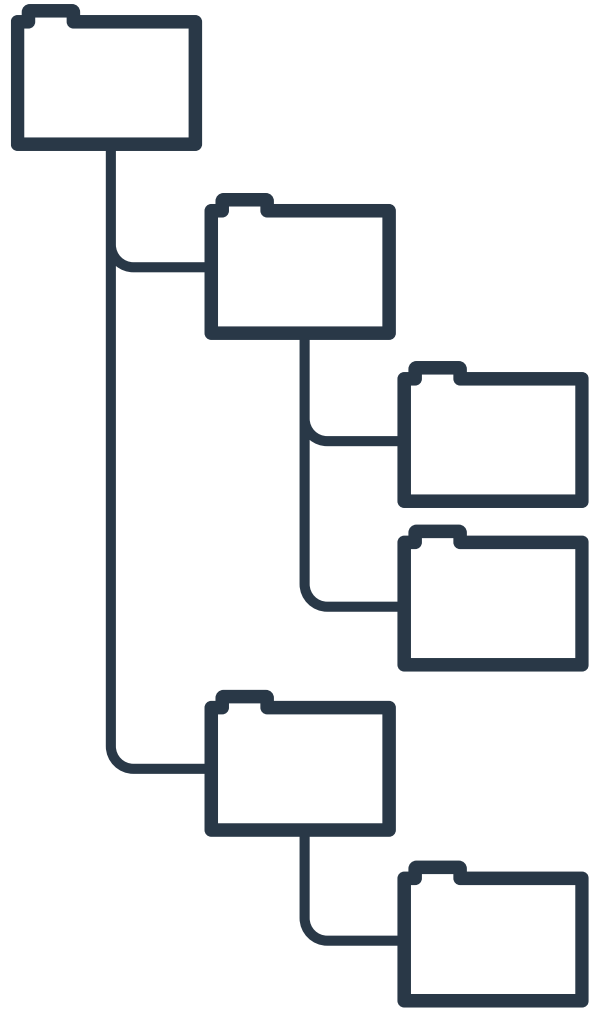
In this section, we will cover:

- File Explorer Options
- Network and Sharing Center
- Administrative Tools
- Power and Sleep Options

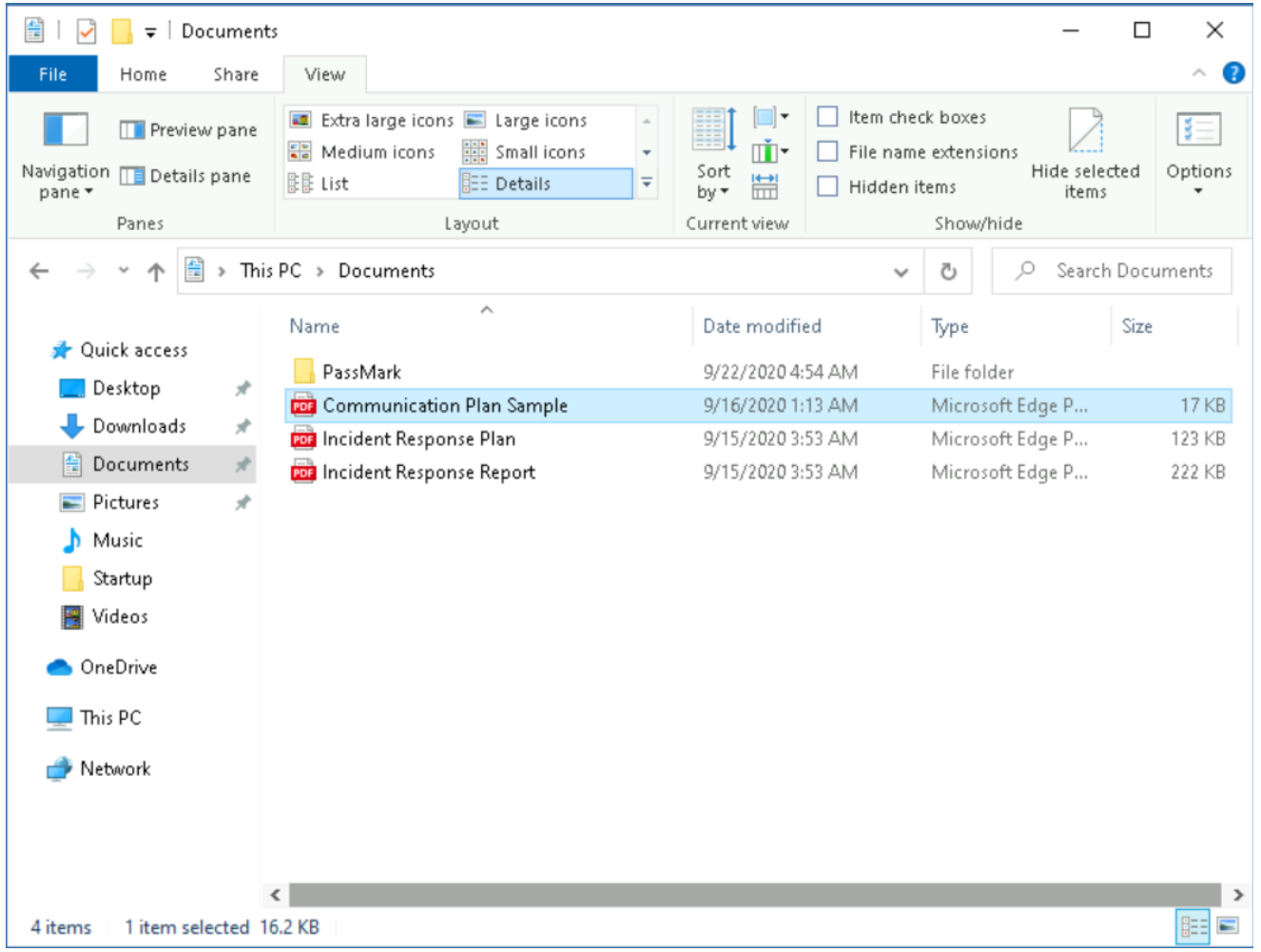
File Explorer Options

File Explorer is a native Windows application that can be used to manage files and folders on the device.

Some of the functionality is showing hidden files, hiding file extensions or displaying the properties of a file or folder.



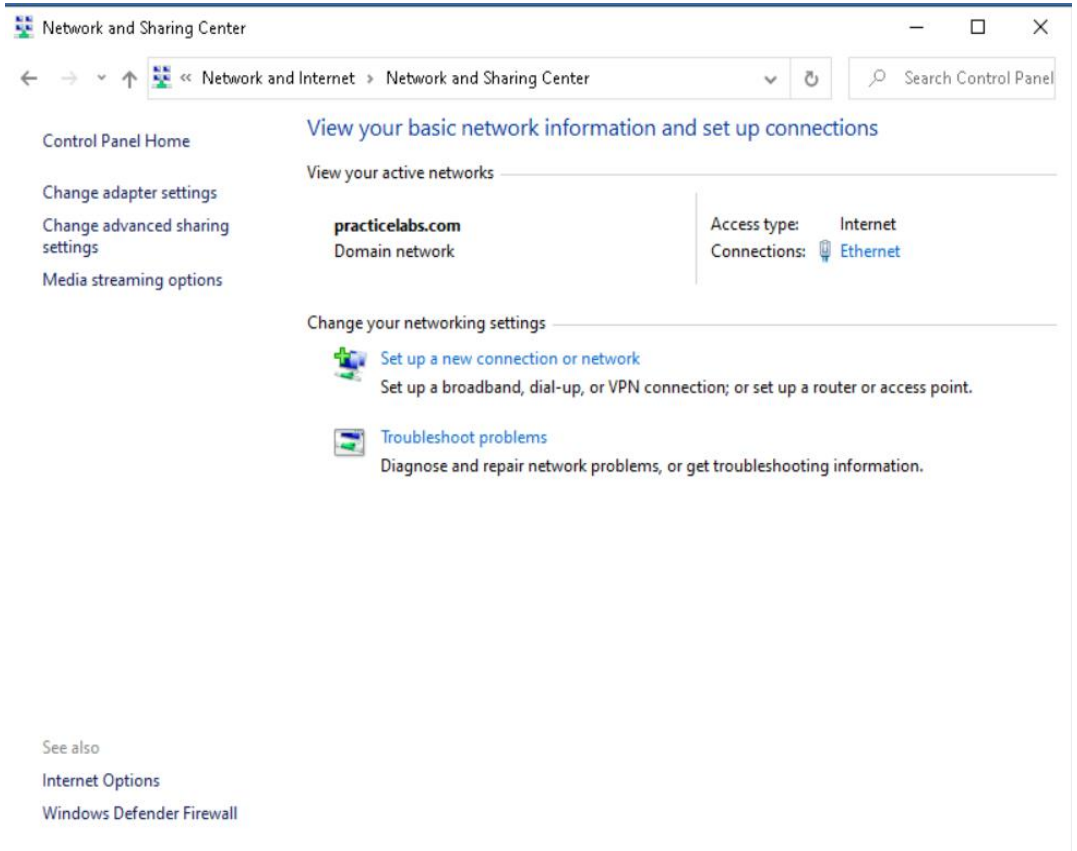
File Explorer options



Network and Sharing Center

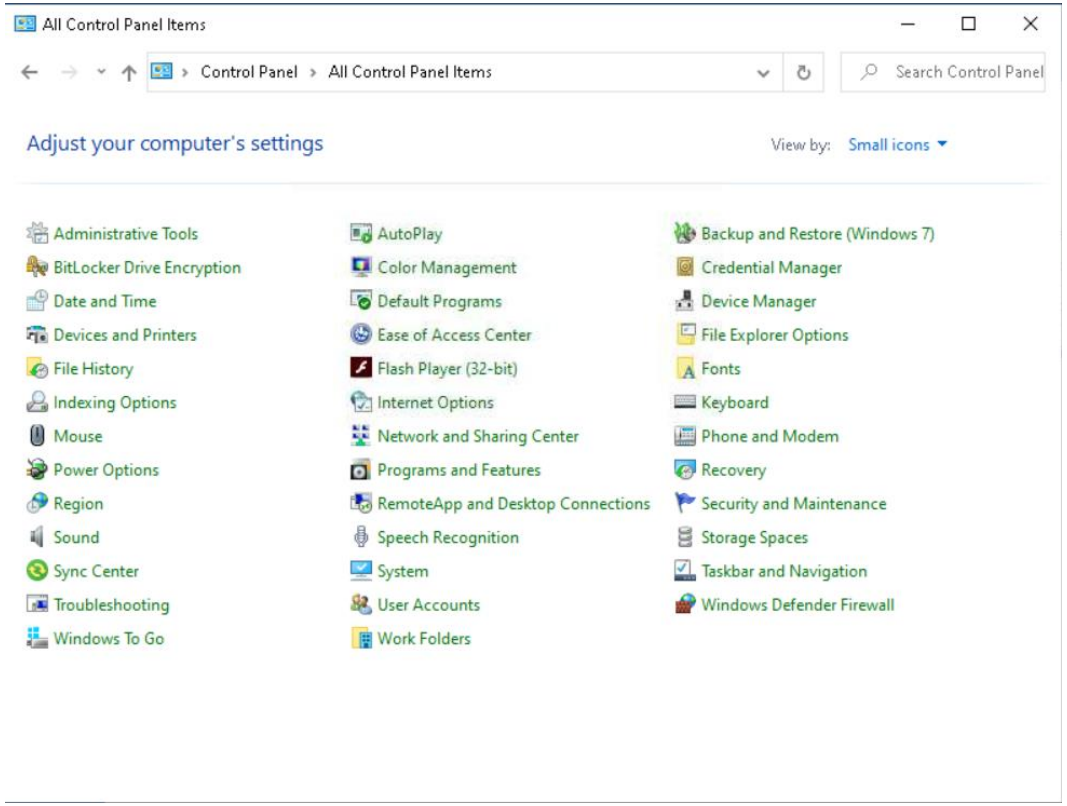
Network and Sharing Center is a system property window that is used to view the basic network information of the device.

Different configurations are available, which include changing the network adapter settings, viewing the network connection settings and managing the sharing settings of the device.



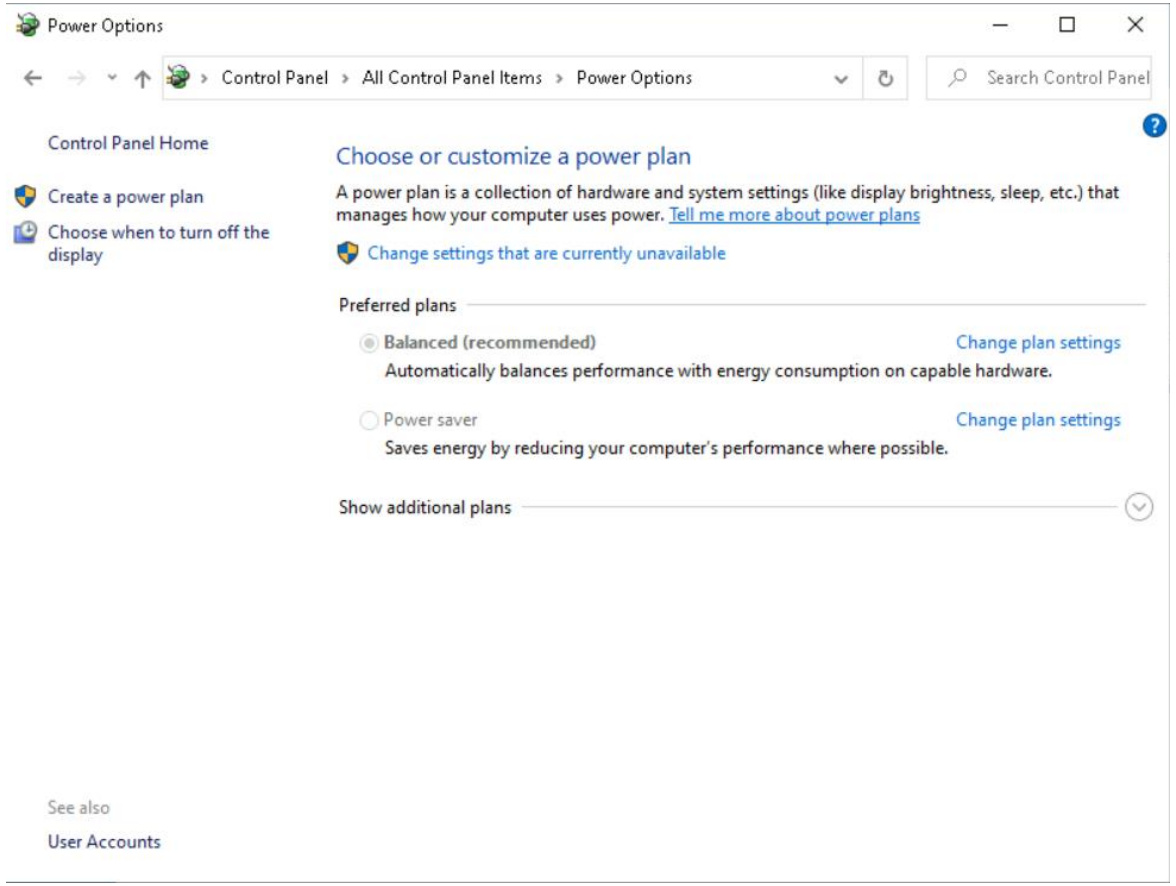
Administrative Tools

The Administrative Tools window is accessible through the Control Panel and enables easy access to several configuration tools used for managing the device.



Power Options

The Power Options window accessible through the Control Panel is used to manage the power utilization options for the device.



Topic: macOS Features and Tools

In this section, we will cover:

- Time Machine
- Mission Control
- Spotlight
- Keychain
- iCloud
- Finder
- Boot Camp

Time Machine (macOS)

Time Machine is an Apple system configuration application used for backing up data on the computer.

Time Machine is used if a system update fails and can be used to restore the system.

Mission Control (macOS)

Mission Control is a feature that allows a user to have multiple desktops on an Apple computer.

Using Mission Control, you can have multiple desktops that help keep your work separated and organized.

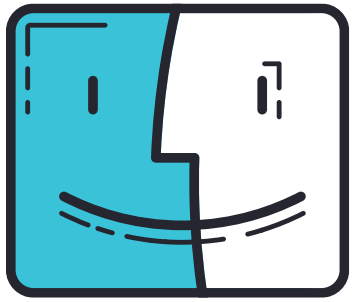
Spotlight (macOS)

Spotlight (macOS) is a feature that allows a user to search for anything on their Mac.

Spotlight (macOS) is a search bar option to search for emails, applications, folders, etc., on the entire system.

Click on the magnifying glass on the search bar or use the Command key and tap the space bar.

Finder (macOS)



Finder (macOS) is a place to view and organize files.

Finder (macOS) allows you to create, delete, or even modify the properties of folders and files.

You can click on the Finder icon to open a window.

Keychain (macOS)

Keychain is used for single sign-on purposes when browsing websites on an Apple computer; it stores username and password information directly on the computer.

When you browse to a website, you have the chance to save your login credentials to the Keychain, so you don't have to re-enter it every time you sign into a website.

You can use Spotlight to search Keychain Access.

iCloud (macOS)

iCloud is cloud storage for folders and files.

With iCloud, you can pay to have more online storage space. Click "Manage" to get an overview of what is stored on the Cloud.

Click System Preferences > Apple ID > iCloud.

Boot Camp (macOS)

Boot Camp (macOS) allows you to put the Windows OS on a Mac device.

Boot Camp (macOS) is a way to be able to have a dual boot option so you can enter the Mac or Windows OS.

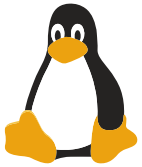
Search "Boot Camp Assistant."

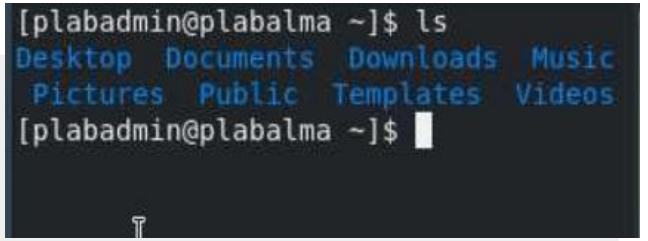
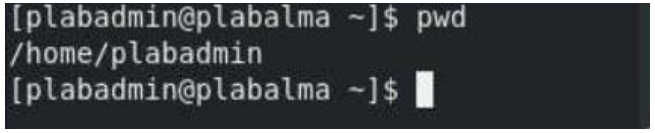
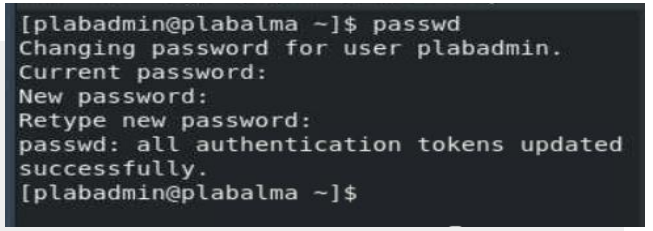
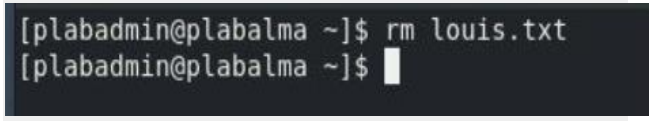
Topic: Linux Features and Tools

In this section, we will cover:

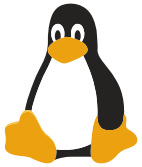
- Commands

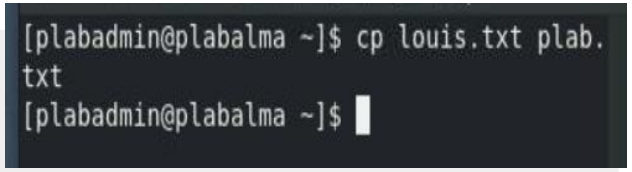
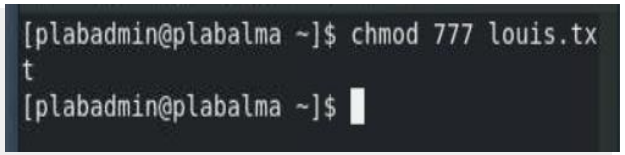
Linux Commands



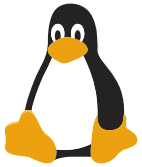
Command	Description	Application
ls	The ls command is used to list all directories and files in the current directory.	
pwd	pwd is used to display (print) the working/current directory.	
passwd	The passwd command is used to change the password of a user's account.	
rm	The rm command is used to delete a file from the device.	

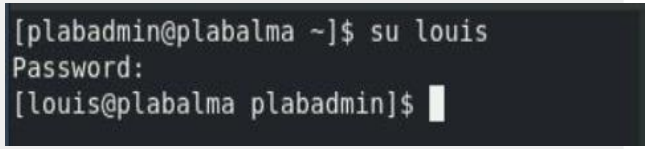
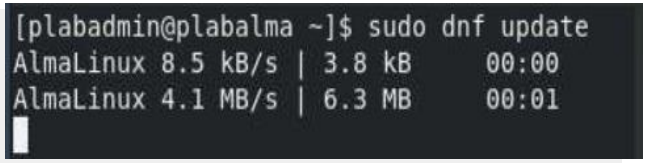
Linux Commands



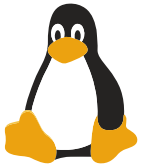
Command	Description	Application
cp	"cp" (command) is used when you want to copy a file or folder. Objects can be renamed during the copy.	
chmod	"chmod" is used to change file mode (permissions) of a file or folder.	
chown	"chown" is used to change ownership of a file or folder.	The "chown" command can be used as chown root:root report.txt.
dd	"dd" (command) is used to copy/convert files at the Byte or block level, rather than files.	Use the "if" and "of" arguments for input file and output file.

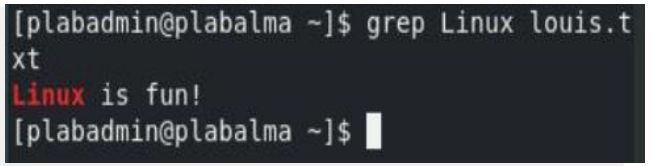
Linux Commands



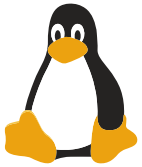
Command	Description	Application
su	"su" is used to switch to a different user account. Default is root.	
sudo	"sudo" runs a command as the specified user account. The default is root.	
vi	"vi" opens a command line text editor with a new document or the specified file.	vi <filename>
nano	"nano" is a text editor, like vi.	nano <filename>

Linux Commands



Command	Description	Application
grep	"grep" (command) searches for text patterns in a file.	
apt (apt-get)	"apt" (command) is used to interface with software repositories to install, upgrade, repair, and uninstall software Packages on Debian distributions of Linux.	sudo apt-get install <package> sudo apt-get install firefox
yum	"yum" (command) is used to get updates from the Internet on Red Hat distributions.	yum install <package name> yum install kazaam
kill	"kill" (command) stops processes that are unresponsive	The "kill" command can be used as kill "switch" "process id."

Linux Commands



Command	Description	Application
ip	**ip** is a powerful NIC management tool. IP addresses, MAC addresses, and DNS configurations.	**ip** addr
ifconfig	Predecessor to **ip.** Similar to ipconfig in Windows.	ifconfig [interface]
iwconfig	is used to manage wireless NIC settings.	iwconfig [interface]

summary

In this module, we covered:

- Common Operating Systems
- File Systems
- Features and Tools of MS Windows 10
- Control Panel Utilities
- Linux Features and Tools