# Windows File System & Permissions

Modern Windows systems use NTFS (New Technology File System) as the default file system.

Before NTFS, Windows used FAT16/FAT32 (File Allocation Table) and HPFS (High Performance File System)

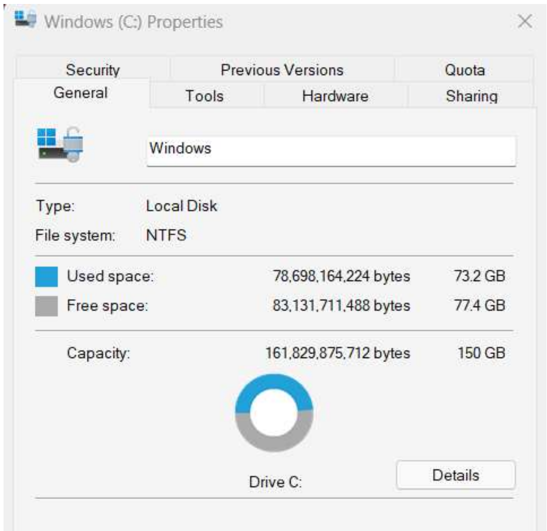
FAT is still used today in:

- USB drives
- Memory cards
- External devices

NTFS is a journaling file system.

- It keeps logs of file changes
- If system crashes → NTFS can repair files automatically
- Supports files larger than 4GB
- Allows file and folder permissions
- Supports compression
- Supports encryption (EFS)
- More stable and secure

To check your Windows file system:
Right click C drive → Properties → File system (NTFS/FAT)



Windows

| | | | |
|---|---|---|---|
| Type: | Local Disk | | |
| File system: | NTFS | | |
| 🟦 Used space: | | 78,698,164,224 bytes | 73.2 GB |
| ▨ Free space: | | 83,131,711,488 bytes | 77.4 GB |
| Capacity: | | 161,829,875,712 bytes | 150 GB |

Drive C:

## NTFS Permissions

NTFS allows controlling who can access files and folders.

Main Permission Types:

1. Full Control: Allows everything
2. Modify: Allows Read, Write and Delete files
3. Read & Execute: Allows opening files and running programs
4. List Folder Contents: Allows viewing files inside folder
5. Read: Allows viewing files and listing folder contents
6. Write: Allows creating files and editing files

# Alternate Data Streams (ADS)

ADS is a feature of NTFS that allows:

- A file to contain hidden data
- Multiple data streams inside one file

ADS can be used to:

- Hide malicious data
- Store hidden scripts
- Hide malware inside normal files

Example:
A normal image file can contain hidden malicious code.

Windows uses ADS to:

- Mark downloaded files from internet
- Store metadata

Example:
When you download a file → Windows marks it as downloaded from the internet using ADS.

## **Windows Directory & System32**

Windows Folder Overview:
The Windows folder (usually located at C:\Windows) is the main directory that contains the Windows operating system files.

Environment Variables:
Environment variables store important information about the operating system.

- They contain system paths, temp locations, processor info, etc.
- The system environment variable for Windows directory is: %windir%

## **Windows User Accounts & Permissions**

| | |
|---|---|
| 1. Administrator<br>● Full control over system<br>● Can install/uninstall programs<br>● Add/remove users<br>● Modify system settings<br>● Access all files | 2. Standard User<br>● Limited permissions<br>● Can use apps & change personal files only<br>● Cannot install system-level software<br>● Cannot modify system settings |

## Viewing User Accounts:

| | |
|---|---|
| 1. GUI method:<br>Start Menu → Settings → Accounts → Other users | 2. Using Run command:<br>lusrmgr.msc |

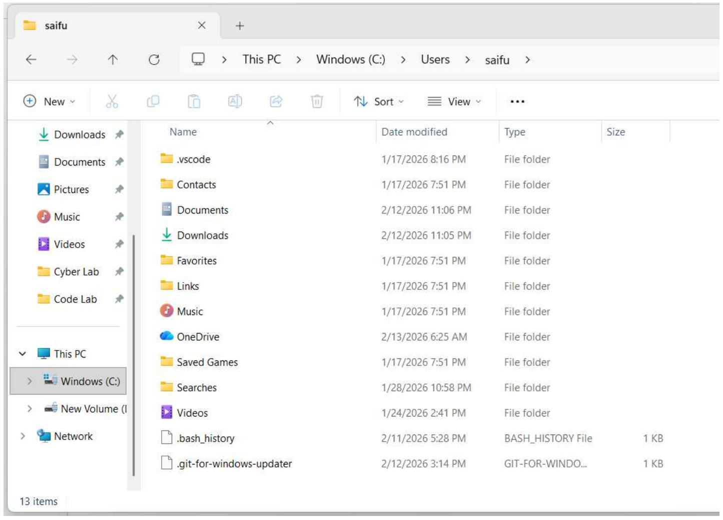
## User Profile Location:

Each user has profile folder:
C:\Users\username

Contains:

- Desktop
- Downloads
- Documents
- Pictures
- App data

Created when the user logs in for the first time.



| Name | Date modified | Type | Size |
|---|---|---|---|
| .vscode | 1/17/2026 8:16 PM | File folder | |
| Contacts | 1/17/2026 7:51 PM | File folder | |
| Documents | 2/12/2026 11:06 PM | File folder | |
| Downloads | 2/12/2026 11:05 PM | File folder | |
| Favorites | 1/17/2026 7:51 PM | File folder | |
| Links | 1/17/2026 7:51 PM | File folder | |
| Music | 1/17/2026 7:51 PM | File folder | |
| OneDrive | 2/13/2026 6:25 AM | File folder | |
| Saved Games | 1/17/2026 7:51 PM | File folder | |
| Searches | 1/28/2026 10:58 PM | File folder | |
| Videos | 1/24/2026 2:41 PM | File folder | |
| .bash_history | 2/11/2026 5:28 PM | BASH_HISTORY File | 1 KB |
| .git-for-windows-updater | 2/12/2026 3:14 PM | GIT-FOR-WINDO... | 1 KB |

13 items

## Groups in Windows

A group is a collection of users with same permissions

- Administrators → full control
- Users → normal access
- Guests → very limited

Users inherit permissions from groups.
A user can belong to multiple groups.

## Windows UAC (User Account Control)

UAC is a security feature in Windows that:

- Prevents unauthorized system changes
- Stops malware from auto-installing
- Asks permission before admin-level actions

Even if the user is an Administrator, programs run with normal privileges until approved.

## Startup Programs in Windows Server

On normal Windows (Windows 10/11):
You can see startup programs in Task Manager → Startup tab

**But on Windows Server:**
Startup tab may not appear in Task Manager or in msconfig

The reliable way is through the Startup folder by entering “shell:startup” in run command

This folder contains:

- Shortcuts to programs
- Scripts or executables

Any file placed here will run automatically when the user logs in

## MSConfig Tools Tab (Windows Utilities)

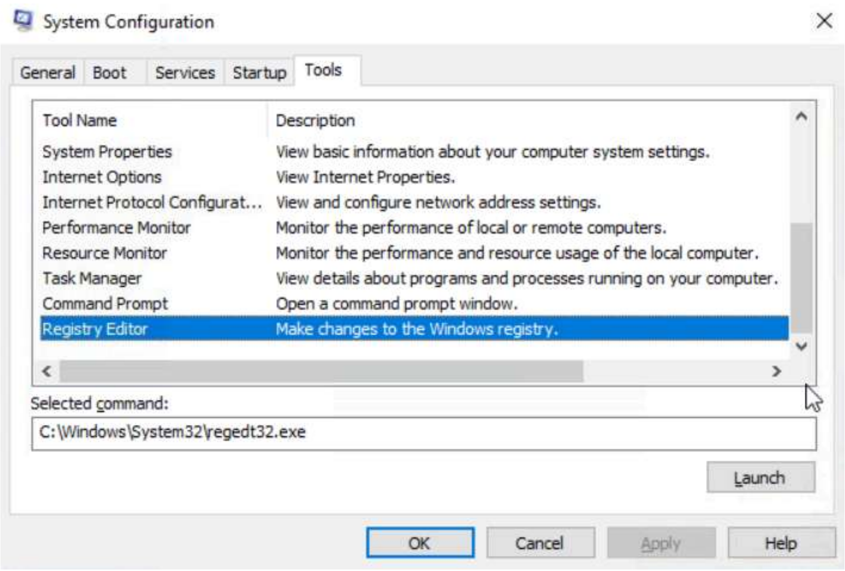
MSConfig (System Configuration) is a Windows utility used to configure and troubleshoot the operating system.

Inside MSConfig, there is a Tools tab that contains many useful Windows utilities. The Tools tab provides a list of important system tools that help you:

- Configure system settings
- Monitor system performance
- Troubleshoot problems
- Manage Windows features

Each tool includes:

1. Tool name
2. Short description
3. Command used to open it



| Tool Name | Description |
|---|---|
| System Properties | View basic information about your computer system settings. |
| Internet Options | View Internet Properties. |
| Internet Protocol Configurat... | View and configure network address settings. |
| Performance Monitor | Monitor the performance of local or remote computers. |
| Resource Monitor | Monitor the performance and resource usage of the local computer. |
| Task Manager | View details about programs and processes running on your computer. |
| Command Prompt | Open a command prompt window. |
| Registry Editor | Make changes to the Windows registry. |

Selected command:

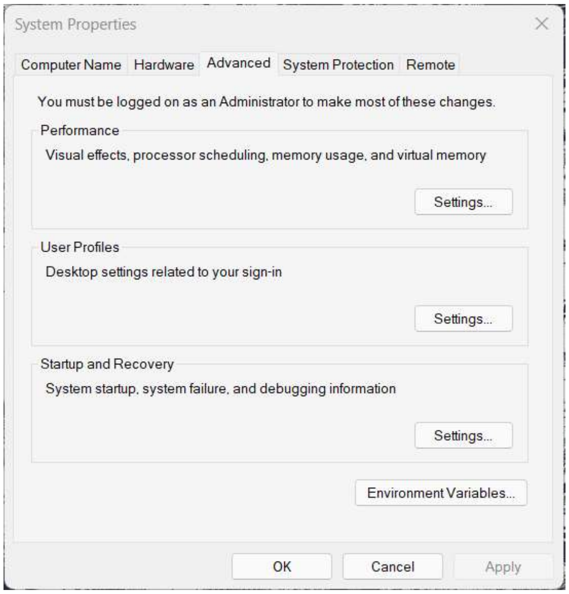
```
C:\Windows\System32\regedt32.exe
```

# Advanced System Settings

Search in Windows:
View advanced system settings

This opens the System Properties window.
This section controls:

- Performance
- Virtual memory (page file)
- Startup & recovery
- Environment variables



You must be logged on as an Administrator to make most of these changes.

Visual effects, processor scheduling, memory usage, and virtual memory

Desktop settings related to your sign-in

System startup, system failure, and debugging information

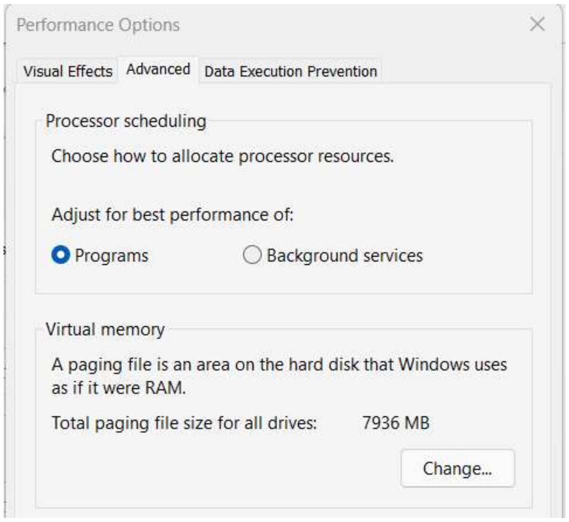
## Performance Settings & Virtual Memory:

Windows uses page files as extra virtual RAM when real RAM is full.

Inside Performance:

- Visual effects
- Processor scheduling
- Virtual memory
- Virtual memory (Page file)

Acts like backup RAM stored on disk.



Choose how to allocate processor resources.

Adjust for best performance of:

● Programs ○ Background services

A paging file is an area on the hard disk that Windows uses as if it were RAM.

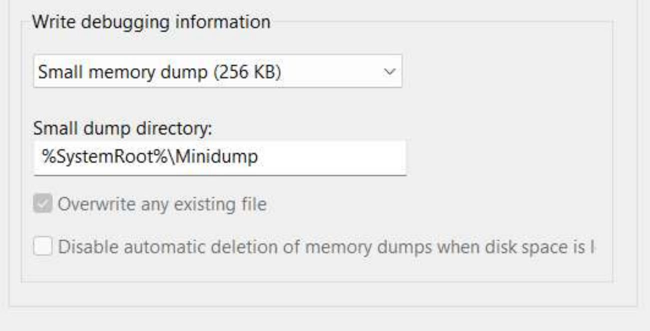
Total paging file size for all drives: 7936 MB

## Startup & Recovery Settings:

Advanced tab → Startup and Recovery → Settings

Controls what happens when Windows crashes.

Crash dump
When a system crashes (BSOD), Windows creates a dump file to analyze the problem.



Small memory dump (256 KB)

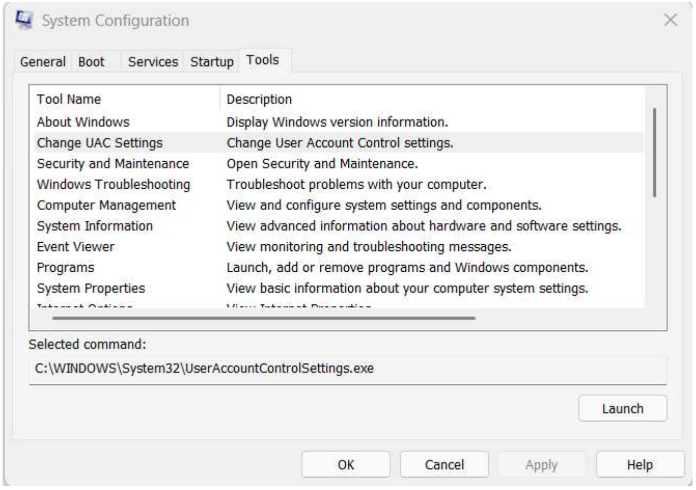
Small dump directory:
%SystemRoot%\Minidump

☑ Overwrite any existing file

☐ Disable automatic deletion of memory dumps when disk space is l

# UAC Security Levels

Windows provides 4 security levels using a slider:


System Configuration

General | Boot | Services | Startup | Tools

| Tool Name | Description |
|---|---|
| About Windows | Display Windows version information. |
| Change UAC Settings | Change User Account Control settings. |
| Security and Maintenance | Open Security and Maintenance. |
| Windows Troubleshooting | Troubleshoot problems with your computer. |
| Computer Management | View and configure system settings and components. |
| System Information | View advanced information about hardware and software settings. |
| Event Viewer | View monitoring and troubleshooting messages. |
| Programs | Launch, add or remove programs and Windows components. |
| System Properties | View basic information about your computer system settings. |

Selected command:
C:\WINDOWS\System32\UserAccountControlSettings.exe

1. Always Notify (Highest Security)

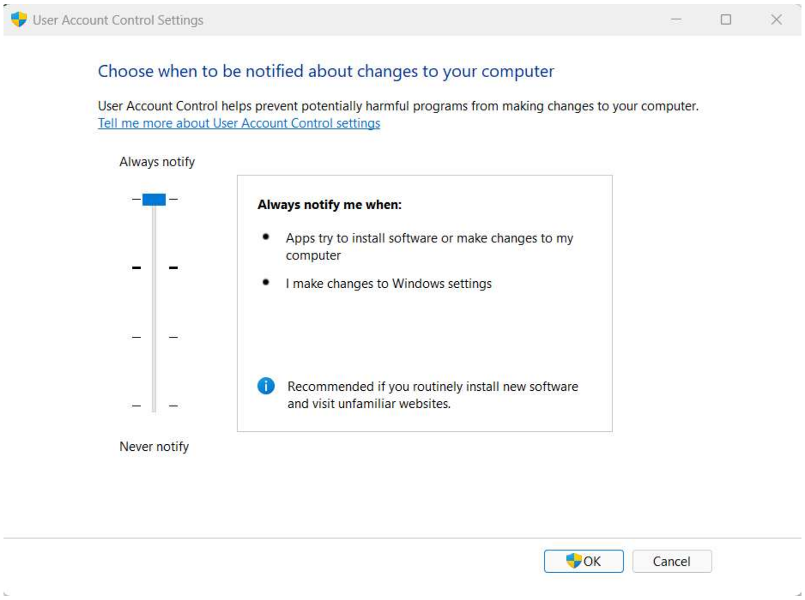
Notifies whenever:

- Apps try to install/change system
- You change Windows settings
- Screen dims (Secure Desktop)
- Requires confirmation

2. Notify for Apps Only (Default)

- Notifies only when apps try to make changes
- Does NOT notify when you change Windows settings

Screen dims


User Account Control Settings

Choose when to be notified about changes to your computer

User Account Control helps prevent potentially harmful programs from making changes to your computer.
Tell me more about User Account Control settings

Always notify

Always notify me when:

- Apps try to install software or make changes to my computer
- I make changes to Windows settings

Recommended if you routinely install new software and visit unfamiliar websites.

Never notify

3. Notify Without Dimming

- Same as default
- But screen does NOT dim
- Slightly less secure
- Malware could interact with screen

4. Never Notify (Lowest Security)

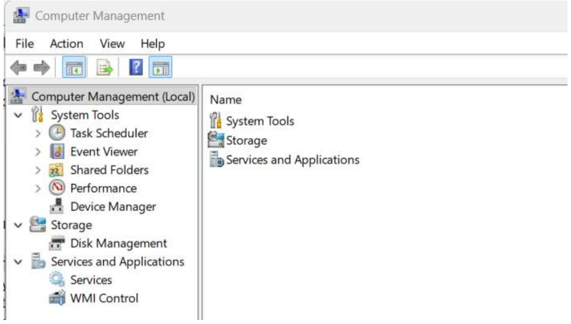
- No warnings at all
- Apps can make system changes silently

# Computer Management

Computer Management is a built-in Windows admin tool used to manage and monitor the system.

It has 3 main sections:

1. System Tools
2. Storage
3. Services and Applications


Computer Management

- Computer Management (Local)
  - System Tools
    - Task Scheduler
    - Event Viewer
    - Shared Folders
    - Performance
    - Device Manager
  - Storage
    - Disk Management
  - Services and Applications
    - Services
    - WMI Control

Name
- System Tools
- Storage
- Services and Applications

## 1. System Tools:

### TASK SCHEDULER:

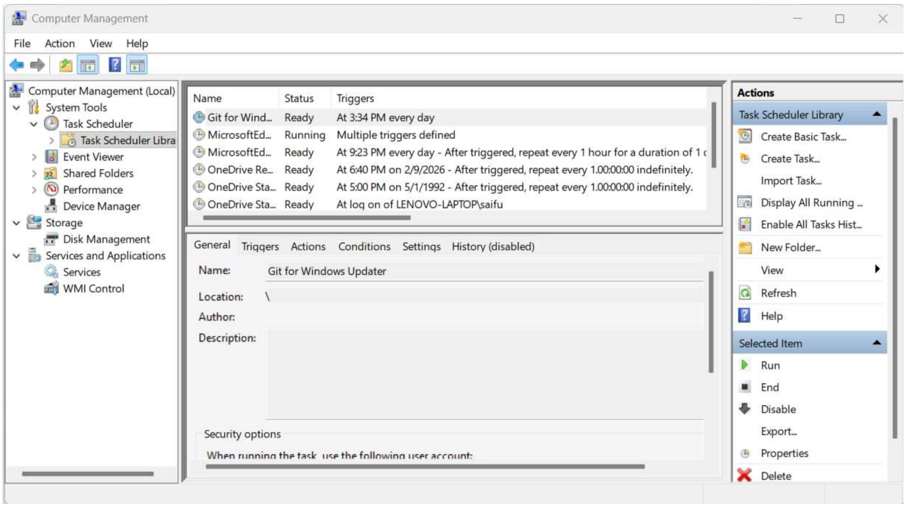
Task Scheduler allows Windows to run tasks automatically.

A task can:

- Run a program
- Run a script
- Run PowerShell command
- Run malware

Tasks can run:

- At system startup
- At user login/logoff
- At specific time (daily, weekly etc)
- Once at specific time
- Every few minutes



| Name | Status | Triggers |
|---|---|---|
| Git for Wind... | Ready | At 3:34 PM every day |
| MicrosoftEd... | Running | Multiple triggers defined |
| MicrosoftEd... | Ready | At 9:23 PM every day - After triggered, repeat every 1 hour for a duration of 1 ( |
| OneDrive Re... | Ready | At 6:40 PM on 2/9/2026 - After triggered, repeat every 1.00:00:00 indefinitely. |
| OneDrive Sta... | Ready | At 5:00 PM on 5/1/1992 - After triggered, repeat every 1.00:00:00 indefinitely. |
| OneDrive Sta... | Ready | At log on of LENOVO-LAPTOP\saifu |

Name: Git for Windows Updater

Location: \

Author:

Description:

Security options

When running the task, use the following user account:

### EVENT VIEWER:

Event Viewer shows everything happening in Windows.

It records:

- Login attempts
- Errors
- Software activity
- System changes
- Attacks

Types of Event Logs:

| | |
|---|---|
| 1. Error:<br>Serious problem in the system. | Example:<br>● Service crashed<br>● System failed to boot<br>● Software crash |
| 2. Warning:<br>Not serious now but may cause problem later. | Example:<br>● Low disk space<br>● Driver issue<br>● High memory usage |
| 3. Information:<br>Normal successful operation. | Example:<br>● Service started successfully<br>● Driver loaded<br>● System booted |

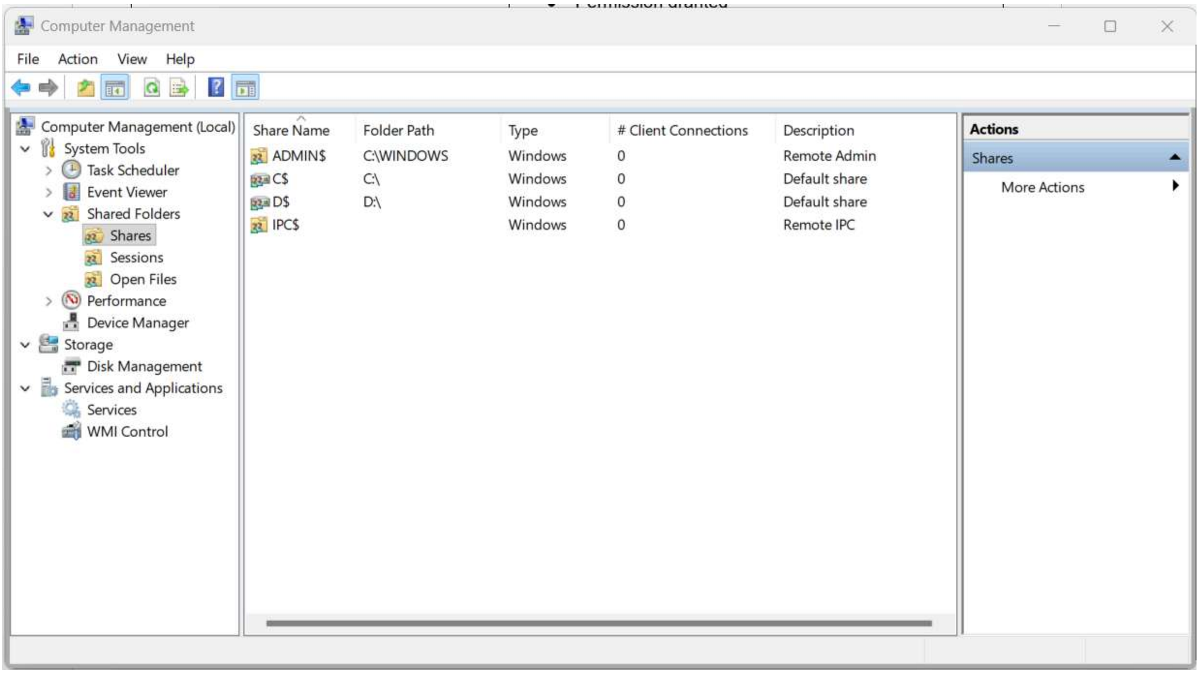
| | |
|---|---|
| 4. Success Audit:<br>Security success log. | Example:<br>● Successful login<br>● User accessed system<br>● Permission granted |
| 5. Failure Audit:<br>Security failure log. | Example:<br>● Wrong password login<br>● Unauthorized access attempt<br>● Blocked access |

**SHARED FOLDERS:**

Shared folders allow other users/systems to access resources remotely.

Common default administrative shares:

- ADMIN$ → Remote admin access to Windows folder
- C$ → Entire C drive shared for admin
- D$ → Entire D drive shared for admin
- IPC$ → Inter-process communication (used for remote connections)



| Share Name | Folder Path | Type | # Client Connections | Description |
|---|---|---|---|---|
| ADMIN$ | C:\WINDOWS | Windows | 0 | Remote Admin |
| C$ | C:\ | Windows | 0 | Default share |
| D$ | D:\ | Windows | 0 | Default share |
| IPC$ | | Windows | 0 | Remote IPC |

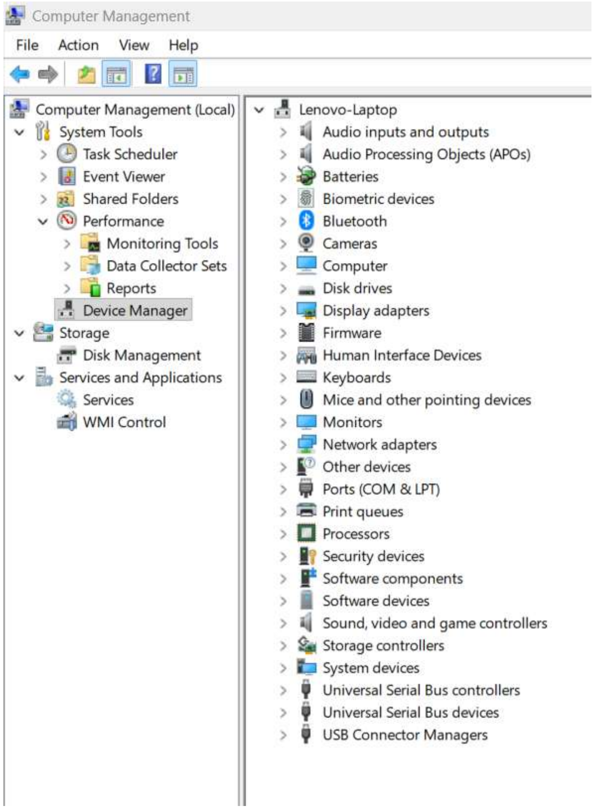
**PERFORMANCE MONITOR (perfmon):**

- Shows system performance in real-time
- Can load saved logs
- Useful for diagnosing:
- CPU usage
- Memory usage
- Disk activity
- Network activity

Device Manager

Used to:

- View hardware devices
- Enable/disable hardware
- Update drivers
- Troubleshoot hardware issues



- Computer Management (Local)
  - System Tools
    - Task Scheduler
    - Event Viewer
    - Shared Folders
    - Performance
      - Monitoring Tools
      - Data Collector Sets
      - Reports
    - Device Manager
  - Storage
    - Disk Management
  - Services and Applications
    - Services
    - WMI Control

- Lenovo-Laptop
  - Audio inputs and outputs
  - Audio Processing Objects (APOs)
  - Batteries
  - Biometric devices
  - Bluetooth
  - Cameras
  - Computer
  - Disk drives
  - Display adapters
  - Firmware
  - Human Interface Devices
  - Keyboards
  - Mice and other pointing devices
  - Monitors
  - Network adapters
  - Other devices
  - Ports (COM & LPT)
  - Print queues
  - Processors
  - Security devices
  - Software components
  - Software devices
  - Sound, video and game controllers
  - Storage controllers
  - System devices
  - Universal Serial Bus controllers
  - Universal Serial Bus devices
  - USB Connector Managers

## 2. Storage:

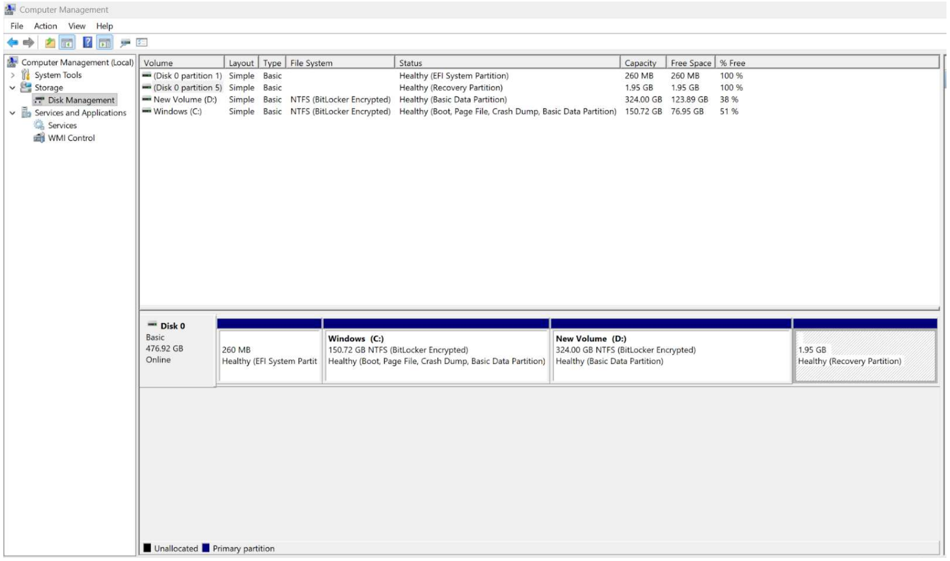
Disk Management:
Disk Management is a Windows built-in utility used to manage storage, disks, and partitions.
It allows administrators to perform advanced storage configuration.

Important partition types:

1. System Reserved
2. C: Drive

Main Functions of Disk Management:

1. Set up a new drive
2. Extend a partition
3. Shrink a partition
4. Assign or change drive letter



- Computer Management (Local)
  - System Tools
  - Storage
    - Disk Management
  - Services and Applications
    - Services
    - WMI Control

| Volume | Layout | Type | File System | Status | Capacity | Free Space | % Free |
|---|---|---|---|---|---|---|---|
| (Disk 0 partition 1) | Simple | Basic | | Healthy (EFI System Partition) | 260 MB | 260 MB | 100 % |
| (Disk 0 partition 5) | Simple | Basic | | Healthy (Recovery Partition) | 1.95 GB | 1.95 GB | 100 % |
| New Volume (D:) | Simple | Basic | NTFS (BitLocker Encrypted) | Healthy (Basic Data Partition) | 324.00 GB | 123.89 GB | 38 % |
| Windows (C:) | Simple | Basic | NTFS (BitLocker Encrypted) | Healthy (Boot, Page File, Crash Dump, Basic Data Partition) | 150.72 GB | 76.95 GB | 51 % |

| Disk 0<br>Basic<br>476.92 GB<br>Online | 260 MB<br>Healthy (EFI System Partit | **Windows (C:)**<br>150.72 GB NTFS (BitLocker Encrypted)<br>Healthy (Boot, Page File, Crash Dump, Basic Data Partition) | **New Volume (D:)**<br>324.00 GB NTFS (BitLocker Encrypted)<br>Healthy (Basic Data Partition) | 1.95 GB<br>Healthy (Recovery Partition) |
|---|---|---|---|---|

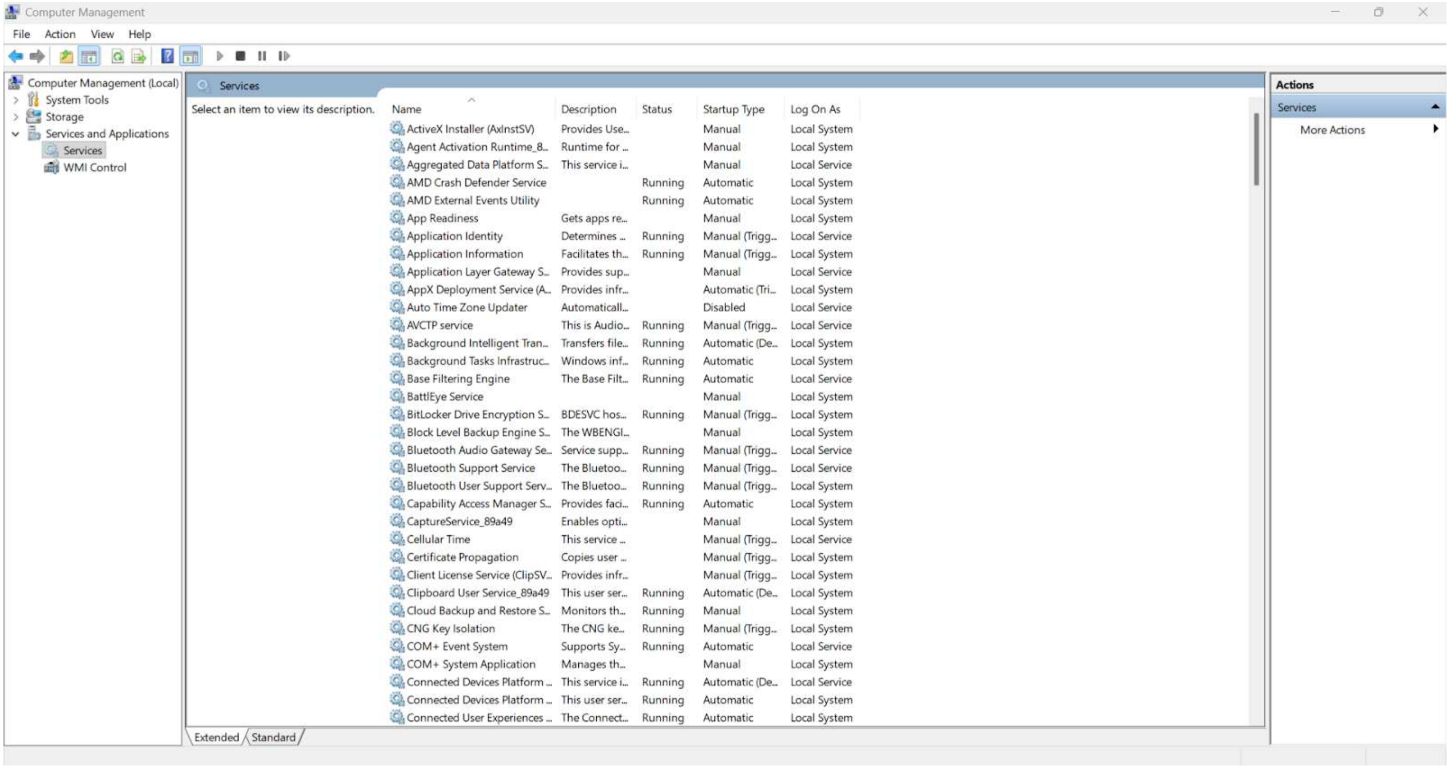
■ Unallocated ■ Primary partition

## 3. Services and Applications:

Services are some programs running in the background.

Each service has:

1. Name
2. Status (Running/Stopped)
3. Startup type
4. Path to executable



Select an item to view its description.

| Name | Description | Status | Startup Type | Log On As |
|---|---|---|---|---|
| ActiveX Installer (AxInstSV) | Provides Use... | | Manual | Local System |
| Agent Activation Runtime_8... | Runtime for ... | | Manual | Local System |
| Aggregated Data Platform S... | This service i... | | Manual | Local Service |
| AMD Crash Defender Service | | Running | Automatic | Local System |
| AMD External Events Utility | | Running | Automatic | Local System |
| App Readiness | Gets apps re... | | Manual | Local System |
| Application Identity | Determines ... | Running | Manual (Trigg... | Local Service |
| Application Information | Facilitates th... | Running | Manual (Trigg... | Local System |
| Application Layer Gateway S... | Provides sup... | | Manual | Local Service |
| AppX Deployment Service (A... | Provides infr... | | Automatic (Tri... | Local System |
| Auto Time Zone Updater | Automaticall... | | Disabled | Local Service |
| AVCTP service | This is Audio... | Running | Manual (Trigg... | Local Service |
| Background Intelligent Tran... | Transfers file... | Running | Automatic (De... | Local System |
| Background Tasks Infrastruc... | Windows inf... | Running | Automatic | Local System |
| Base Filtering Engine | The Base Filt... | Running | Automatic | Local Service |
| BattlEye Service | | | Manual | Local System |
| BitLocker Drive Encryption S... | BDESVC hos... | Running | Manual (Trigg... | Local System |
| Block Level Backup Engine S... | The WBENGI... | | Manual | Local System |
| Bluetooth Audio Gateway Se... | Service supp... | Running | Manual (Trigg... | Local Service |
| Bluetooth Support Service | The Bluetoo... | Running | Manual (Trigg... | Local Service |
| Bluetooth User Support Serv... | The Bluetoo... | Running | Manual (Trigg... | Local System |
| Capability Access Manager S... | Provides faci... | Running | Automatic | Local System |
| CaptureService_89a49 | Enables opti... | | Manual | Local System |
| Cellular Time | This service ... | | Manual (Trigg... | Local Service |
| Certificate Propagation | Copies user ... | | Manual (Trigg... | Local System |
| Client License Service (ClipSV... | Provides infr... | | Manual (Trigg... | Local System |
| Clipboard User Service_89a49 | This user ser... | Running | Automatic (De... | Local System |
| Cloud Backup and Restore S... | Monitors th... | Running | Manual | Local System |
| CNG Key Isolation | The CNG ke... | Running | Manual (Trigg... | Local System |
| COM+ Event System | Supports Sy... | Running | Automatic | Local Service |
| COM+ System Application | Manages th... | | Manual | Local System |
| Connected Devices Platform ... | This service i... | Running | Automatic (De... | Local Service |
| Connected Devices Platform ... | This user ser... | Running | Automatic | Local System |
| Connected User Experiences ... | The Connect... | Running | Automatic | Local System |

Startup types:

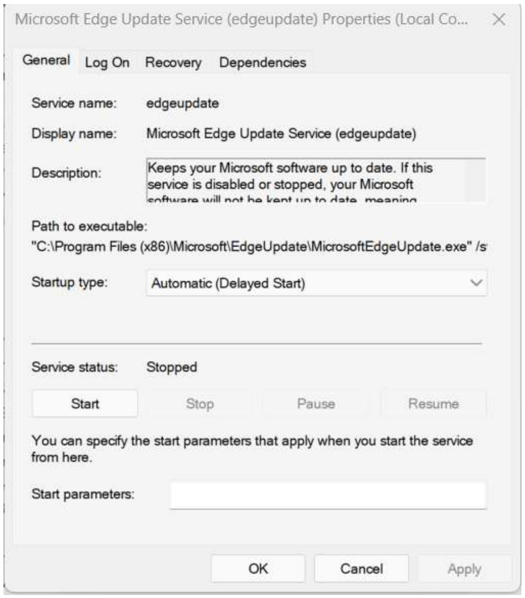
- Automatic → starts at boot
- Manual → starts when needed
- Disabled → never runs

WMI (Windows Management Instrumentation)

WMI controls and manages Windows systems.

Used for:

- Automation
- Remote management
- System info gathering
- PowerShell scripting


Microsoft Edge Update Service (edgeupdate) Properties (Local Co...
General
Log On
Recovery
Dependencies
Start
Stop
Pause
Resume
OK
Cancel
Apply

Service name: edgeupdate

Display name: Microsoft Edge Update Service (edgeupdate)

Description: Keeps your Microsoft software up to date. If this service is disabled or stopped, your Microsoft software will not be kept up to date, meaning

Path to executable:
"C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe" /s

Startup type: Automatic (Delayed Start)

Service status: Stopped

You can specify the start parameters that apply when you start the service from here.

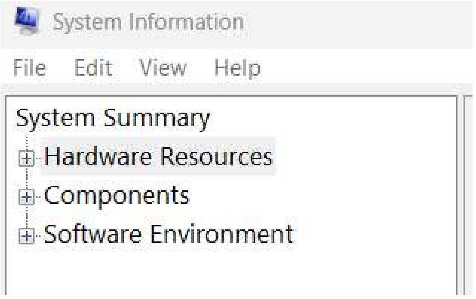
Start parameters:

# System Information Tool (msinfo32)

System Information (msinfo32) is a built-in Windows tool that shows complete details about your computer.

It provides a full overview of:

1. Hardware
2. System components
3. Software environment

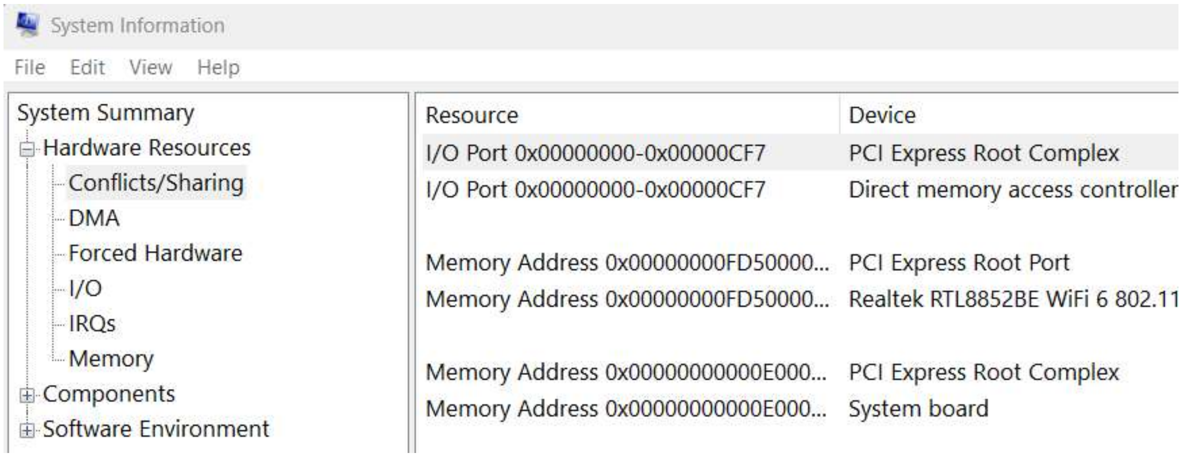


## 1. Hardware Resources

Shows low-level hardware details of the system.
This section is mostly for advanced users or system engineers, not average users.

Includes:

- IRQs (Interrupt requests)
- DMA (Direct Memory Access)
- I/O ports
- Memory addresses
- Hardware conflicts/sharing



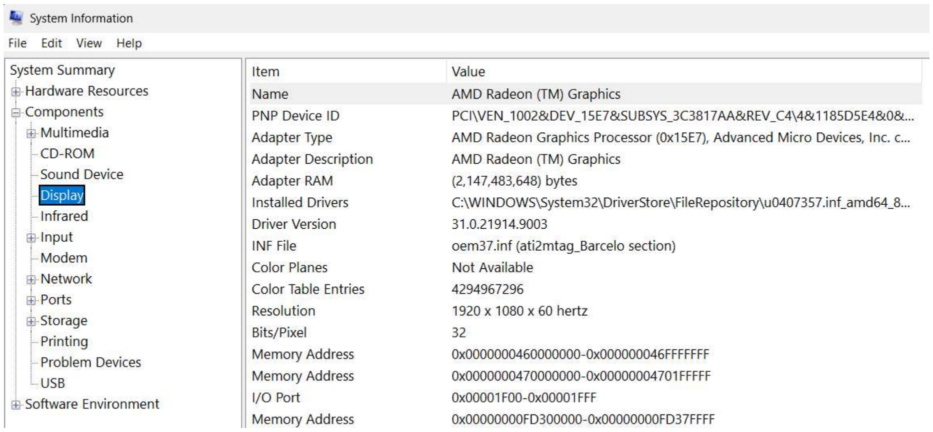
| Resource | Device |
|---|---|
| I/O Port 0x00000000-0x00000CF7 | PCI Express Root Complex |
| I/O Port 0x00000000-0x00000CF7 | Direct memory access controller |
| | |
| Memory Address 0x00000000FD50000... | PCI Express Root Port |
| Memory Address 0x00000000FD50000... | Realtek RTL8852BE WiFi 6 802.11 |
| | |
| Memory Address 0x00000000000E000... | PCI Express Root Complex |
| Memory Address 0x00000000000E000... | System board |

## 2. Components

Shows details about installed hardware components.

Examples:

- Display (GPU info)
- Sound devices
- Network adapters
- Storage devices
- USB devices



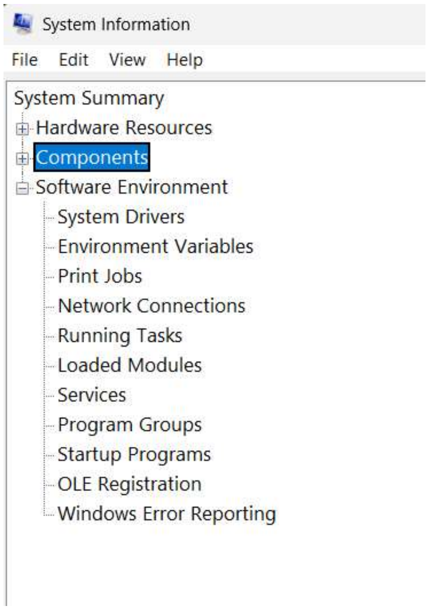
| Item | Value |
|---|---|
| Name | AMD Radeon (TM) Graphics |
| PNP Device ID | PCI\VEN_1002&DEV_15E7&SUBSYS_3C3817AA&REV_C4\4&1185D5E4&0&... |
| Adapter Type | AMD Radeon Graphics Processor (0x15E7), Advanced Micro Devices, Inc. c... |
| Adapter Description | AMD Radeon (TM) Graphics |
| Adapter RAM | (2,147,483,648) bytes |
| Installed Drivers | C:\WINDOWS\System32\DriverStore\FileRepository\u0407357.inf_amd64_8... |
| Driver Version | 31.0.21914.9003 |
| INF File | oem37.inf (ati2mtag_Barcelo section) |
| Color Planes | Not Available |
| Color Table Entries | 4294967296 |
| Resolution | 1920 x 1080 x 60 hertz |
| Bits/Pixel | 32 |
| Memory Address | 0x0000000460000000-0x000000046FFFFFFF |
| Memory Address | 0x0000000470000000-0x00000004701FFFFF |
| I/O Port | 0x00001F00-0x00001FFF |
| Memory Address | 0x00000000FD300000-0x00000000FD37FFFF |

## 3. Software environment

Shows OS-level software details.

Includes:

- Installed software
- Running processes
- System drivers
- Startup programs
- Services
- Environment variables
- Network connections



Two Types of Environment Variables

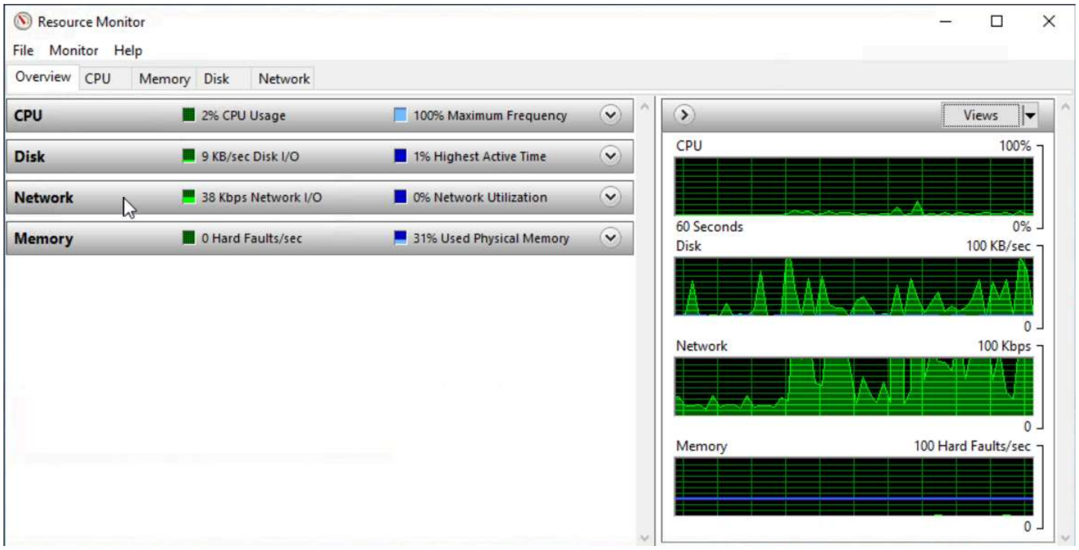
1. User Variables
   - Only for current user
   - Example: user TEMP folder
   - Can be edited without affecting whole system

2. System Variables
   - Apply to entire system
   - Used by OS and all users
   - Example: system PATH

## Resource Monitor (resmon)

Resource Monitor (resmon) shows real-time usage of:

1. CPU
2. RAM
3. Disk
4. Network



| | |
|---|---|
| **1. CPU**<br>Shows:<br>● Running processes<br>● CPU usage per process<br>● Services running<br>● Threads<br>● Handles | **2. Memory**<br>Shows:<br>● RAM usage<br>● Per-process memory usage<br>● Hard faults<br>● Free vs used memory |
| **3. Disk**<br>Shows:<br>● Disk read/write speed<br>● Active processes using disk<br>● File paths being accessed<br>● Storage usage | **4. Network**<br>Shows:<br>● Network usage per process<br>● IP addresses<br>● Open ports<br>● TCP connections<br>● Send/receive speed |

## Command Prompt (cmd)

- Command Prompt (cmd) is a text-based interface used to interact with the operating system.
- Before GUI existed, command line was the main way to control computers.
- Even today, many system and troubleshooting tasks can be done using cmd.

### Basic Commands

1. hostname

Purpose: Shows the computer name.

2. whoami

Purpose: Shows current logged-in user.

3. ipconfig

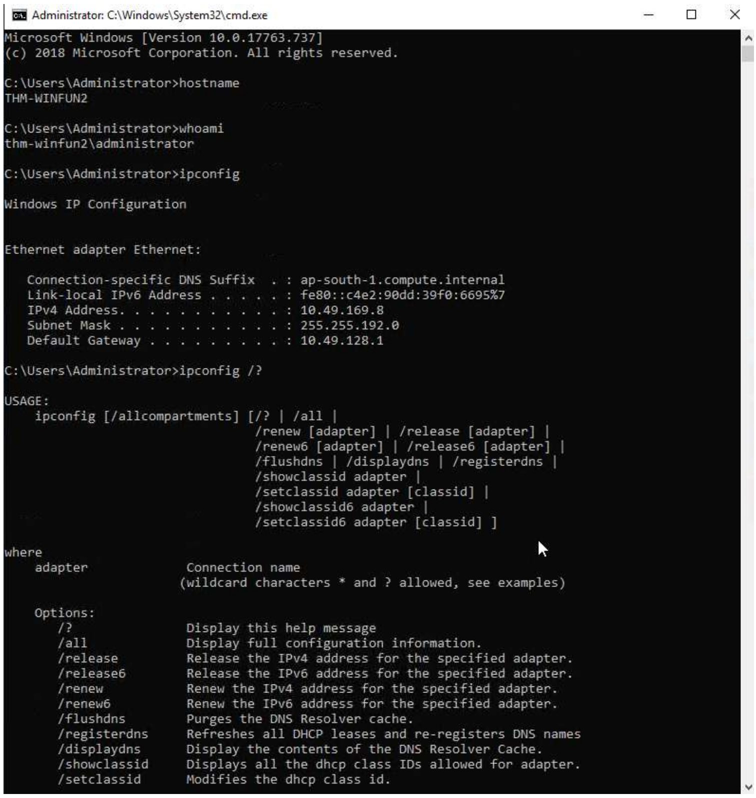
Purpose: Displays network configuration of the system.

4. cls

Purpose: Clears command prompt screen.

5. netstat

Purpose: Shows network statistics and active TCP/IP connections



```
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>hostname
THM-WINFUN2

C:\Users\Administrator>whoami
thm-winfun2\administrator

C:\Users\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : ap-south-1.compute.internal
   Link-local IPv6 Address . . . . . : fe80::c4e2:90dd:39f0:6695%7
   IPv4 Address. . . . . . . . . . . : 10.49.169.8
   Subnet Mask . . . . . . . . . . . : 255.255.192.0
   Default Gateway . . . . . . . . . : 10.49.128.1

C:\Users\Administrator>ipconfig /?

USAGE:
    ipconfig [/allcompartments] [/? | /all |
                                 /renew [adapter] | /release [adapter] |
                                 /renew6 [adapter] | /release6 [adapter] |
                                 /flushdns | /displaydns | /registerdns |
                                 /showclassid adapter |
                                 /setclassid adapter [classid] |
                                 /showclassid6 adapter |
                                 /setclassid6 adapter [classid] ]

where
    adapter             Connection name
                       (wildcard characters * and ? allowed, see examples)

    Options:
       /?               Display this help message
       /all             Display full configuration information.
       /release         Release the IPv4 address for the specified adapter.
       /release6        Release the IPv6 address for the specified adapter.
       /renew           Renew the IPv4 address for the specified adapter.
       /renew6          Renew the IPv6 address for the specified adapter.
       /flushdns        Purges the DNS Resolver cache.
       /registerdns     Refreshes all DHCP leases and re-registers DNS names
       /displaydns      Display the contents of the DNS Resolver Cache.
       /showclassid     Displays all the dhcp class IDs allowed for adapter.
       /setclassid      Modifies the dhcp class id.
```

Common net subcommands

- net user → manage users
- net localgroup → manage groups
- net share → manage shared folders
- net session → view active sessions
- net use → manage network connections
- net start/stop → control services

Help Manual for Commands

Every command has a help manual.

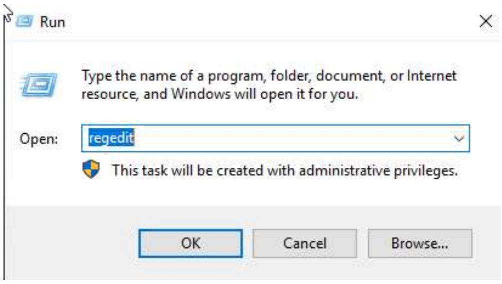
Syntax: command /?

# Windows Registry

The Windows Registry is a central hierarchical database in Windows.

It stores important configuration data needed for:

- Operating system
- Applications
- Hardware devices
- User settings



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: regedit

This task will be created with administrative privileges.

Windows constantly reads this database during system operation.

Registry contains system and user configuration such as:

1. User Information

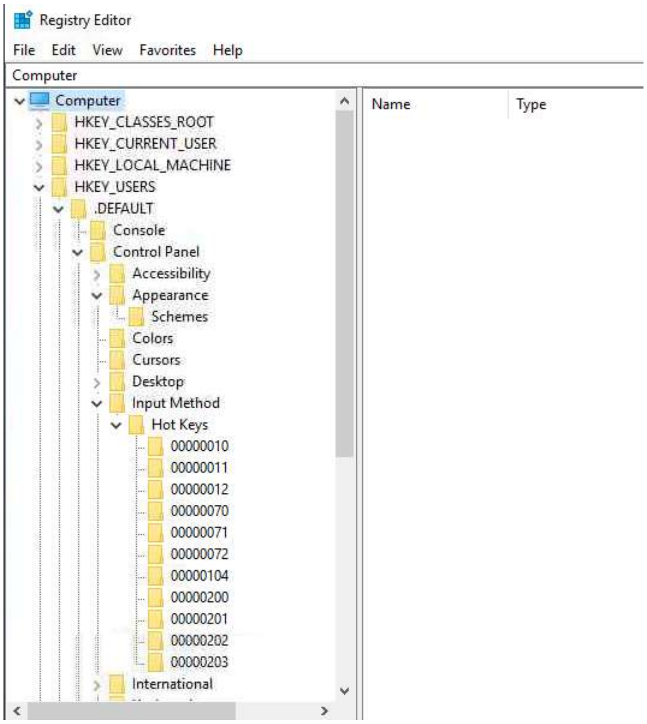
- Profiles for each user
- User-specific settings

2. Applications

- Installed programs
- File types each program can open
- Application settings

3. System Properties

- Folder settings
- Application icons
- System configuration



4. Hardware Info

- Hardware installed on system
- Drivers and configurations

5. Network & Ports

- Ports being used
- Network-related settings

## Windows Security

Windows Security is the built-in protection system in Windows that helps protect:

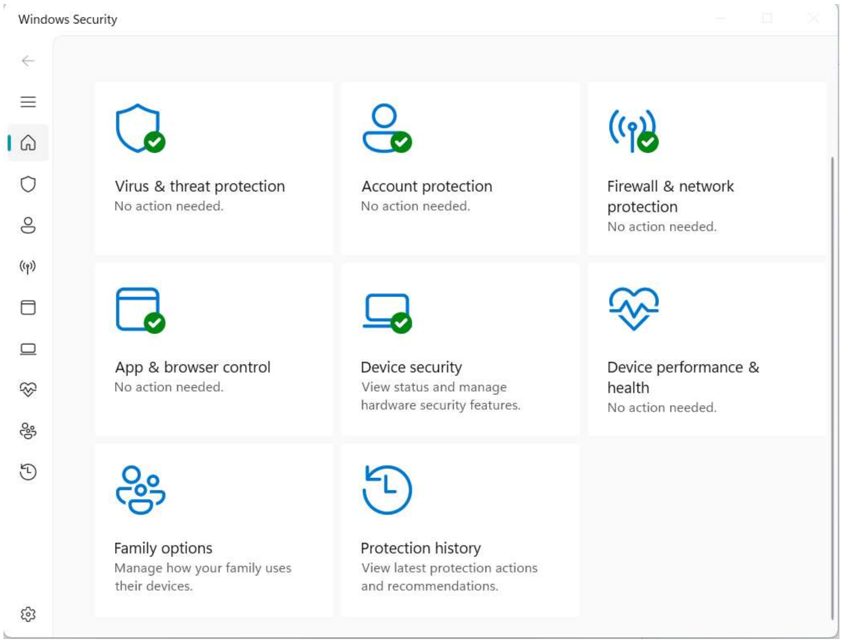
- Device (PC/server)
- Files & data
- Network
- Apps & browser

**Main Protection Areas:**

1. Virus & threat protection
2. Firewall & network protection
3. App & browser control
4. Device security

Inside Windows Security you'll see colored icons:

- Green → Fully protected
- Yellow → Recommendation available
- Red → Immediate action needed (danger)



Windows Security

Virus & threat protection
No action needed.

Account protection
No action needed.

Firewall & network protection
No action needed.

App & browser control
No action needed.

Device security
View status and manage hardware security features.

Device performance & health
No action needed.

Family options
Manage how your family uses their devices.

Protection history
View latest protection actions and recommendations.

### 1. Virus & Threat Protection:

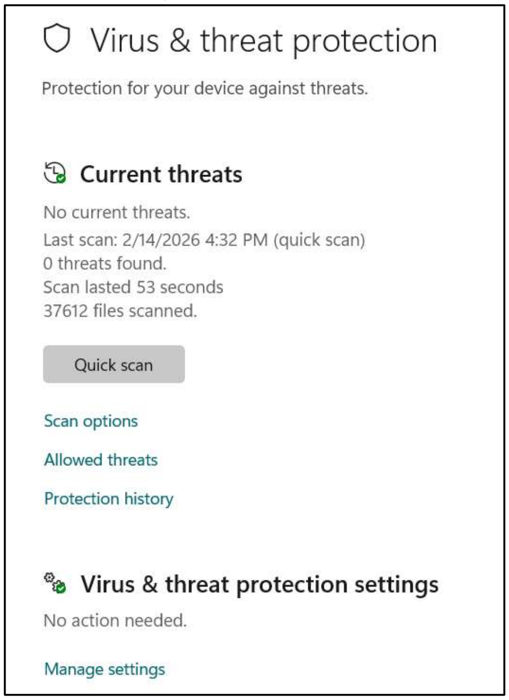
Windows Virus & Threat Protection is part of Windows Security that protects the system from malware, viruses, ransomware, and other threats.

Two main sections:

1. Current threats
2. Virus & threat protection settings

**1. Current threats:**

This shows the real-time status of threats in the system.



Virus & threat protection

Protection for your device against threats.

Current threats

No current threats.
Last scan: 2/14/2026 4:32 PM (quick scan)
0 threats found.
Scan lasted 53 seconds
37612 files scanned.

Virus & threat protection settings

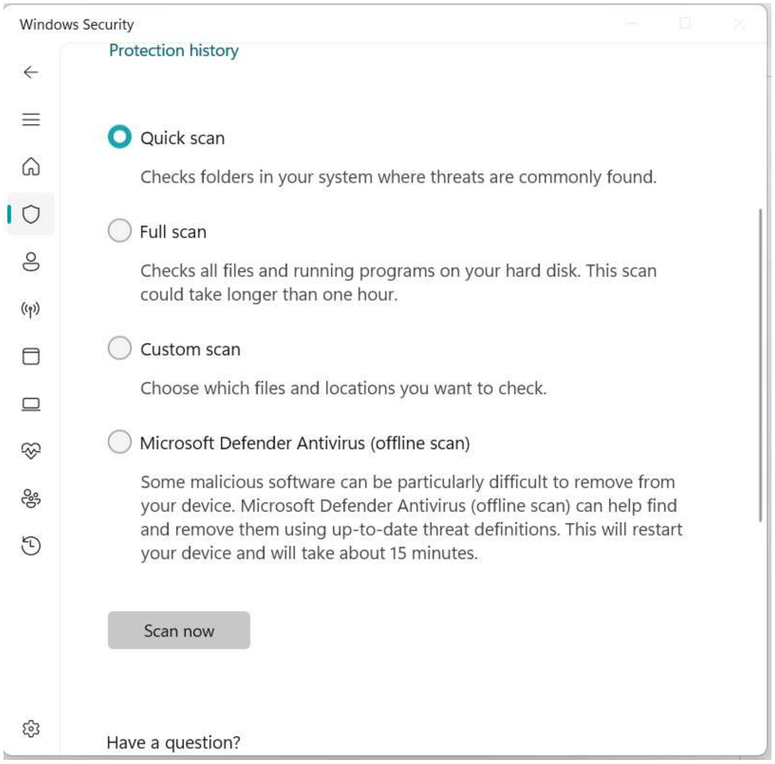
No action needed.

Displays:

- If any virus/malware detected
- Last scan time
- Number of threats found
- Files scanned
- Scan duration

Scan Options:

Used to manually scan the system.



Windows Security

Protection history

● Quick scan

Checks folders in your system where threats are commonly found.

○ Full scan

Checks all files and running programs on your hard disk. This scan could take longer than one hour.

○ Custom scan

Choose which files and locations you want to check.

○ Microsoft Defender Antivirus (offline scan)

Some malicious software can be particularly difficult to remove from your device. Microsoft Defender Antivirus (offline scan) can help find and remove them using up-to-date threat definitions. This will restart your device and will take about 15 minutes.

Quick Scan

- Scans common threat locations
- Fast (few minutes)
- Used for daily checking

Full Scan

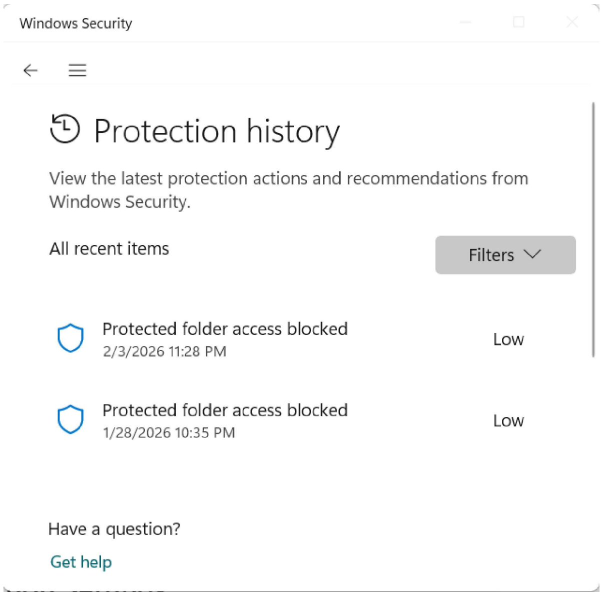
- Scans entire disk and running programs
- Very slow (can take 1+ hour)
- Deep check

Custom Scan

- User selects specific files/folders
- Useful for checking suspicious file

Threat History

Shows past detection records.



Windows Security

Protection history

View the latest protection actions and recommendations from Windows Security.

All recent items

| | |
|---|---|
| Protected folder access blocked<br>2/3/2026 11:28 PM | Low |
| Protected folder access blocked<br>1/28/2026 10:35 PM | Low |

Last Scan

- Shows last automatic scan result
- Windows Defender runs automatic scans

Quarantined Threats

- Infected files isolated
- Cannot run or harm system
- Usually auto-deleted later

Allowed Threats

- Threats user allowed manually
- Dangerous if allowed wrongly

## 2. Virus & Threat Protection Settings

### Real-time Protection

- Scans files instantly when opened/downloaded
- Stops malware before execution
- Protects system continuously

### Dev Drive Protection

- Scans developer drives (Dev Drive)
- Works asynchronously
- Reduces performance impact while coding

### Cloud-Delivered Protection

- Uses Microsoft cloud database
- Detects latest/new malware faster
- Provides stronger real-time detection

### Automatic Sample Submission

- Sends suspicious files to Microsoft
- Helps detect new threats globally
- Improves security for all users

### Tamper Protection

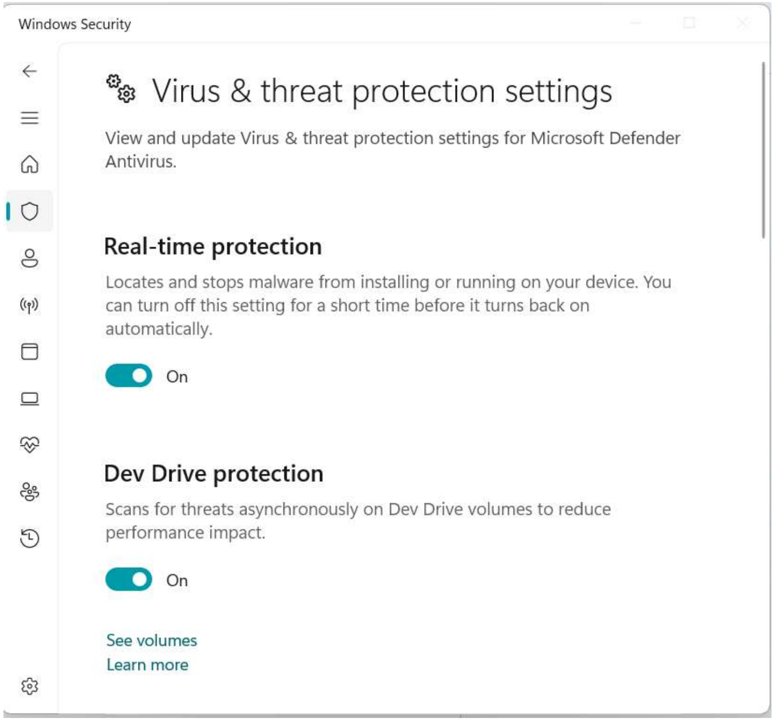
- Prevents malware/users from disabling Antivirus
- Stops attackers from turning off Defender.

### Controlled Folder Access

- Protects important folders from ransomware.
- Blocks unauthorized apps from Changing files

### Exclusions

- Exclude files/folders from antivirus scanning.
- Excluded files will NOT be scanned



Windows Security

Virus & threat protection settings

View and update Virus & threat protection settings for Microsoft Defender Antivirus.

Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

On

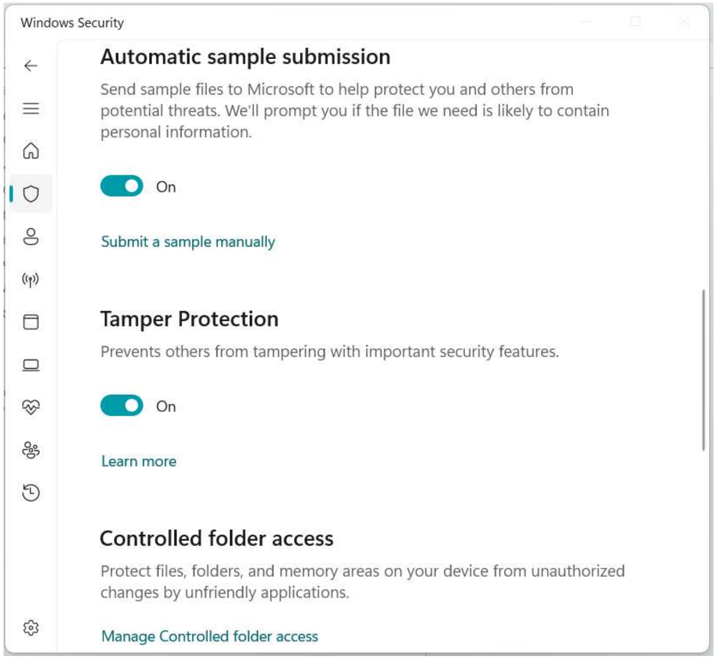
Dev Drive protection

Scans for threats asynchronously on Dev Drive volumes to reduce performance impact.

On

See volumes

Learn more



Windows Security

Automatic sample submission

Send sample files to Microsoft to help protect you and others from potential threats. We'll prompt you if the file we need is likely to contain personal information.

On

Submit a sample manually

Tamper Protection

Prevents others from tampering with important security features.

On

Learn more

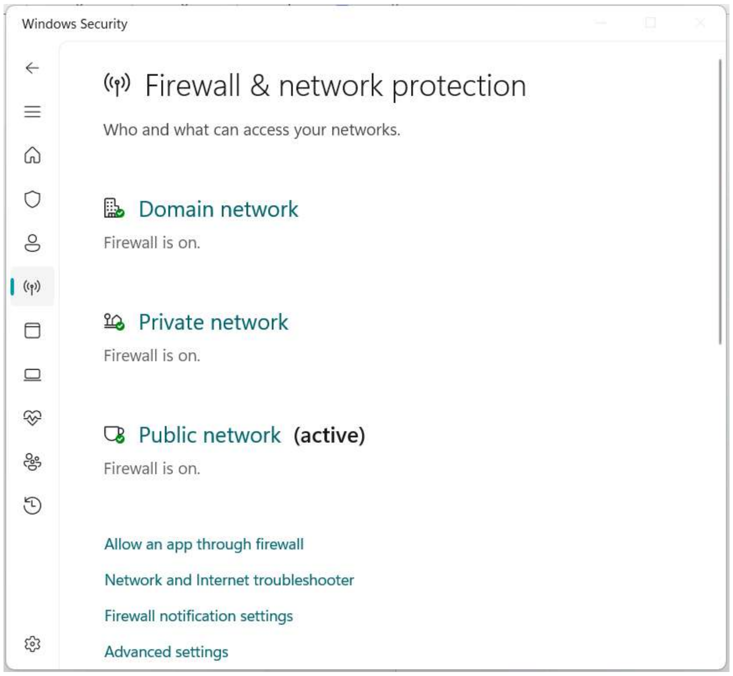
Controlled folder access

Protect files, folders, and memory areas on your device from unauthorized changes by unfriendly applications.

Manage Controlled folder access

## 2. Firewall & network protection

A firewall controls incoming and outgoing network traffic.



Windows Security

Firewall & network protection

Who and what can access your networks.

Domain network

Firewall is on.

Private network

Firewall is on.

Public network (active)

Firewall is on.

Allow an app through firewall
Network and Internet troubleshooter
Firewall notification settings
Advanced settings

There are three firewall profiles:

1. Domain network
2. Private network
3. Public network

Each can have separate firewall settings.

### 1. Domain Network

Used in:

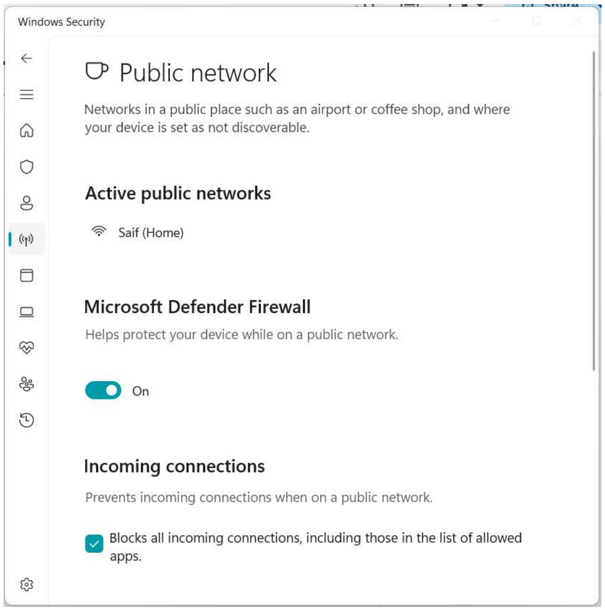
- Company/office networks
- Connected to domain controller (Active Directory)

### 2. Private Network

- Device is discoverable
- Can share files
- Can connect to other devices
- Firewall is still ON but less strict than public.

### 3. Public Network

- Most restrictive firewall rules.
- Device hidden from other computers



Windows Security

Public network

Networks in a public place such as an airport or coffee shop, and where your device is set as not discoverable.

Active public networks

Saif (Home)

Microsoft Defender Firewall

Helps protect your device while on a public network.

On

Incoming connections

Prevents incoming connections when on a public network.

☑ Blocks all incoming connections, including those in the list of allowed apps.

### Inside a Firewall Profile (Example: Public)

1. Turn Firewall ON/OFF

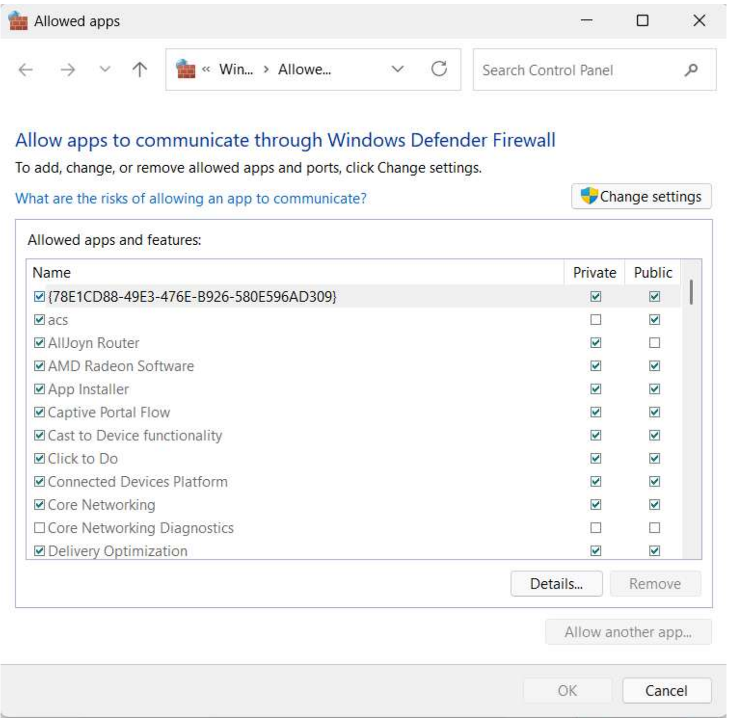
- Recommended: always ON
- OFF = system exposed to attacks

2. Block All Incoming Connections

- Blocks every incoming request
- Block even allowed apps
- Maximum security mode

## Allow an App Through Firewall

You can allow specific apps to pass the firewall.



Allowed apps

Allow apps to communicate through Windows Defender Firewall

To add, change, or remove allowed apps and ports, click Change settings.

What are the risks of allowing an app to communicate?

Allowed apps and features:

| Name | Private | Public |
|---|---|---|
| ☑ {78E1CD88-49E3-476E-B926-580E596AD309} | ☑ | ☑ |
| ☑ acs | □ | ☑ |
| ☑ AllJoyn Router | ☑ | □ |
| ☑ AMD Radeon Software | ☑ | ☑ |
| ☑ App Installer | ☑ | ☑ |
| ☑ Captive Portal Flow | ☑ | ☑ |
| ☑ Cast to Device functionality | ☑ | ☑ |
| ☑ Click to Do | ☑ | ☑ |
| ☑ Connected Devices Platform | ☑ | ☑ |
| ☑ Core Networking | ☑ | ☑ |
| □ Core Networking Diagnostics | □ | □ |
| ☑ Delivery Optimization | ☑ | ☑ |

Example:

- Browser
- Remote desktop
- Games
- Software tools

Allowed Apps Window:

- Shows list of apps allowed through firewall.
- Private ✓ allowed on home network
- Public ✓ allowed on public network

## Advanced Settings

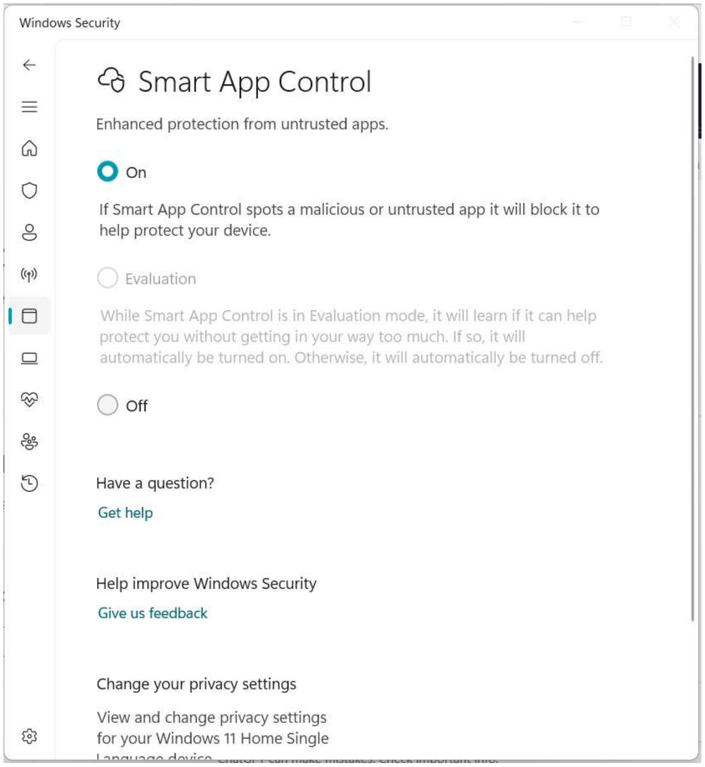
This is the advanced firewall control panel used by admin

Main Sections (Left Panel):

- Inbound Rules: Controls traffic coming INTO your computer.
- Outbound Rules: Controls traffic leaving FROM your computer.
- Connection Security Rules: Advanced secure communication rules.
- Monitoring: Shows real-time firewall activity.

## 3. App & browser control

It automatically blocks malicious apps, softwares before they run.



Windows Security

Smart App Control

Enhanced protection from untrusted apps.

● On

If Smart App Control spots a malicious or untrusted app it will block it to help protect your device.

○ Evaluation

While Smart App Control is in Evaluation mode, it will learn if it can help protect you without getting in your way too much. If so, it will automatically be turned on. Otherwise, it will automatically be turned off.

○ Off

Have a question?

Get help

Help improve Windows Security

Give us feedback

Change your privacy settings

View and change privacy settings for your Windows 11 Home Single Language device

## Smart App Control Modes:

ON (Recommended):

- Blocks malicious/untrusted apps automatically
- Strong protection
- Best security mode

Evaluation Mode:

- Temporary learning mode.
- System checks your app usage
- Checks whether protection will affect work
- Then automatically turns ON or OFF

OFF (Not recommended):

- No protection
- Apps run without Smart App Control checks

## 4. Device Security

Device Security protects hardware-level components of your computer. It uses built-in hardware and virtualization-based protection. This is one of the strongest security layers because it works below the operating system.

### Core Isolation:

Core isolation uses virtualization-based security (VBS) to protect critical system processes.
It isolates important system memory so malware cannot easily access it.

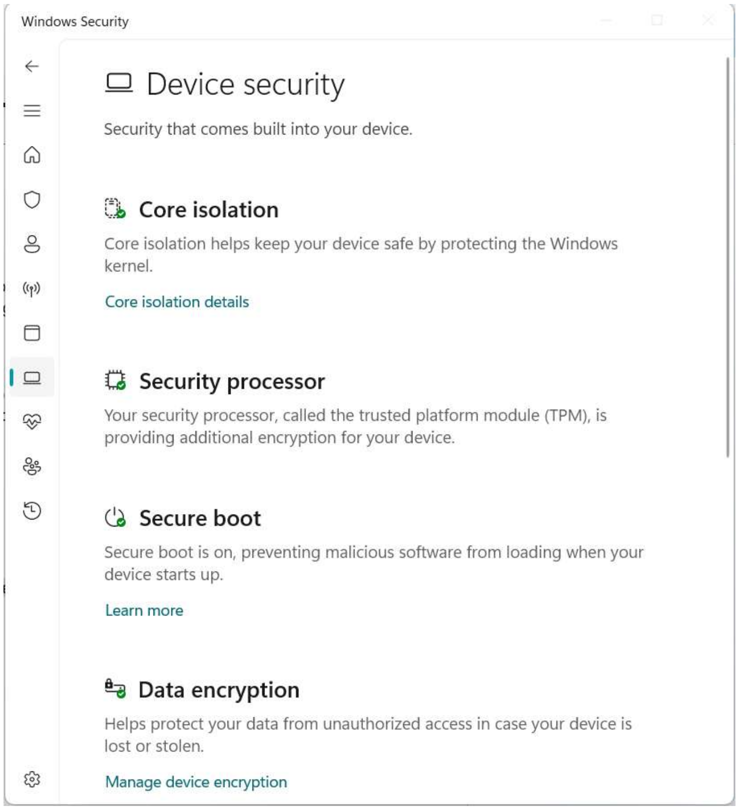
Memory Integrity (Inside Core Isolation):

- Prevents malicious code from inserting into:
- High-security processes
- System kernel
- Drivers

### Security Processor (TPM - Trusted Platform Module):

It is a hardware-based security processor.
Provides:

- Encryption
- Secure key storage
- Device authentication



Windows Security

Device security

Security that comes built into your device.

Core isolation

Core isolation helps keep your device safe by protecting the Windows kernel.

Core isolation details

Security processor

Your security processor, called the trusted platform module (TPM), is providing additional encryption for your device.

Secure boot

Secure boot is on, preventing malicious software from loading when your device starts up.

Learn more

Data encryption

Helps protect your data from unauthorized access in case your device is lost or stolen.

Manage device encryption

# BitLocker

BitLocker is a Windows feature used for disk encryption. It encrypts the entire drive so files cannot be accessed without proper authentication.

It protects data from:

- Theft
- Unauthorized access
- Lost or stolen computers
- Offline attacks

### How BitLocker Works

BitLocker encrypts:

- Entire disk (OS drive)
- Files & folders
- System data

Uses:

- Encryption keys
- Password/PIN
- TPM chip (best method)

**BitLocker works best with Trusted Platform Module (TPM)**

# Volume Shadow Copy Service (VSS)

Volume Shadow Copy Service (VSS) creates a snapshot (backup copy) of files or system at a specific time.

Used for:

- Backup
- Restore
- Recovery

VSS is very useful for:

- Recovering files after malware attack
- Restoring deleted data
- Undoing system damage