

Intro to Windows Security

Lecture 18 - ECS198F SQ26



Plan of the Day



About Windows

- What's the difference between different versions of Windows?
- What are some overarching themes we see in Windows's design?

Built-In Utilities

- How is security implemented in Windows?
- What are the security utilities that can be used to secure Windows?

Other Useful Tools

- What other utilities are useful for Windows security but do not come installed by default?



1. Windows Versioning and Design

The Stuff You Probably Know



Windows is:

- Designed and maintained by Microsoft
- Releases ~~step~~ major numbered versions every “few” years
 - XP, Vista, 7, 8, 9, 10, 11
 - Recently started subversioning out 10 and 11

https://en.wikipedia.org/wiki/List_of_Microsoft_Windows_versions#Personal_computer_versions



Image From:

<https://www.youtube.com/watch?v=e843erV5qXg>

Stuff You Didn't Care About Before



Each “release” of Windows has 3 versions for different types of users!

- **Windows Home** - Most basic version sold on consumer computers, contains some features
- **Windows Pro** - “Business”-grade general OS; essentially Home but with extra security features for management
- **Windows Server** - Server OS dedicated to hosting services; has different update schedule and support compared to Home/Pro

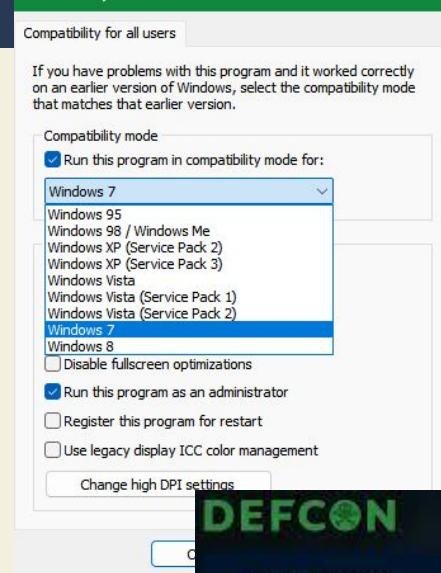
Feature	Windows 11 Home	Windows 11 Pro
BitLocker Drive Encryption If your device is lost or stolen, BitLocker puts everything on lockdown, so no one else can access your systems or data. 11		<input checked="" type="checkbox"/>
Device encryption If you turn on device encryption, only authorized individuals will be able to access your device and data. 12	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Find my device Keep track of your devices—even your digital pen!	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Firewall and network protection Your Windows device comes with built-in security features to help safeguard against viruses, malware, and ransomware.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Internet protection App & browser control in Windows Security helps protect your device from potentially dangerous apps, files, websites, and downloads. 13	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Parental controls and protection Manage screen time, limit access to mature content, and control online purchases when you connect your family's Microsoft accounts.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Secure boot Helps prevent malicious software applications and unauthorized operating systems from loading during the system start-up process.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Windows Hello Uses facial recognition, fingerprint, or PIN, for a fast, secure, and password-free way to unlock your compatible Windows devices. 14	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Backwards Compatibility



Windows as an operating system first and foremost is:

- ~~Secure~~
- **USABLE!**
 - That means making sure old programs can run on newer systems!
 - That means supporting old features *in case* you want to use them!
 - That means allowing you to **downgrade** your security for compatibility purposes!

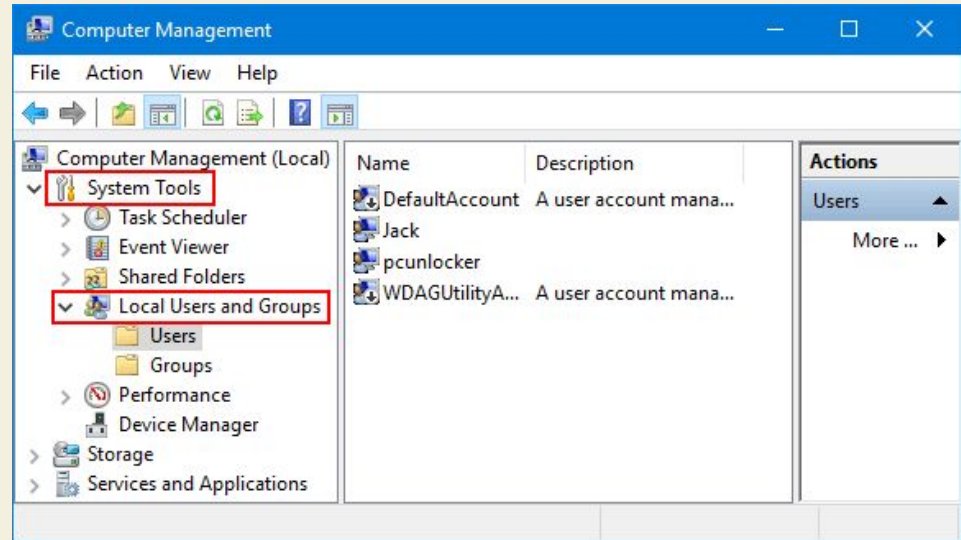


Administration Style



Welcome back GUI Management!

- Pretty much all management tasks can be done by clicking through menus!
 - User management, firewall policies, setting rules, add or removing programs, etc. etc.
- Command-line options still available...



The Windows “Command Line”



You have “2” options for administering Windows through the command line:

- **Command Prompt**
 - Dates back to the late 80’s
 - Heritage of the original DOS
 - Very different commands!
- **PowerShell**
 - Introduced with Windows 7
 - Shell + scripting language!

```
Administrator: Command Prompt - dir /s *.pdf /p
Volume in drive C is NOTENDELL
Volume Serial Number is 6A8A-3332

Directory of C:\cygwin\usr\share\doc\bzip2
10/17/2011  03:59 AM                256,905 manual.pdf
              1 File(s)                256,905 bytes

Directory of C:\cygwin\usr\share\doc\cygwin-2.1.0
07/30/2015  03:48 PM                178,957 cygwin-api.pdf
07/30/2015  03:48 PM                548,458 cygwin-ug-net.pdf
              2 File(s)                727,415 bytes

Directory of C:\cygwin\usr\share\doc\groff\examples\nom
07/30/2015  03:47 PM                4,945 letter.pdf
07/30/2015  03:47 PM                56,426 mom-pdf.pdf
07/30/2015  03:47 PM                17,507 penguin.pdf
07/30/2015  03:47 PM                38,273 sample_docs.pdf
07/30/2015  03:47 PM                40,767 typesetting.pdf
              5 File(s)                157,918 bytes

Directory of C:\cygwin\usr\share\doc\groff\pdf
07/30/2015  03:47 PM                 56 mom-pdf.pdf
07/30/2015  03:47 PM                120,892 p
              2 File(s)                120,948
```

```
Windows PowerShell
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Users\Ted> gci

Directory: C:\Users\Ted

Mode                LastWriteTime         Length Name
----                -
d-----         4/1/2016 9:12 AM                .oracle_jre_usage
d-----         3/11/2016 5:19 PM                .ssh
d-----         3/3/2016 3:47 AM                Contacts
d-----         4/1/2016 10:19 PM                Desktop
d-----         3/13/2016 11:15 AM                Documents
d-----         4/3/2016 11:00 PM                Downloads
d-----         3/3/2016 3:47 AM                Favorites
d-----         3/20/2016 10:35 AM                ForReal
d-----         4/1/2016 3:16 PM                FunWithPowerShell
d-----         3/3/2016 3:47 AM                Links
d-----         3/3/2016 3:47 AM                Music
d-----         3/10/2016 5:51 PM                OneDrive
d-----         4/4/2016 3:03 PM                Pictures
d-----         3/3/2016 3:47 AM                Saved Games
d-----         3/3/2016 3:47 AM                Searches
d-----         2/20/2016 12:15 PM                temp
d-----         8/30/2015 7:48 PM                Tracing
d-----         3/3/2016 3:47 AM                Videos
d-----         4/3/2016 7:34 AM                wget-activehistory
-a-----         4/1/2016 9:42 PM                1505 .bash_history
-a-----         4/3/2016 1:13 PM                155 .gitconfig
-a-----         2/10/2016 11:29 AM                69 .node_repl_history
-a-----         2/25/2016 10:45 AM                599 .viminfo

PS C:\Users\Ted> _
```

About PowerShell



- The one that gets bundled into computers is **PowerShell 5.1!** (Newest version is 7)
- Object-based (Kinda like Python)
 - Queries return objects, and you can process those objects
 - Not text-based like bash!

Example: How do you get a list of users in Bash and PowerShell?

- `cut -d: -f1 /etc/passwd` (Bash)
- `Get-ADUser -Filter * | Select-Object (property)`

```
Administrator: Windows PowerShell
PS C:\> Get-Process | Select-Object name, id, @{L='LoadProfile';E={$_.StartInfo.LoadUserProfile}} | get-member

    TypeName: Selected.System.Diagnostics.Process

-----
Name           MemberType Definition
-----
Equals         Method      bool Equals(System.Object obj)
GetHashCode    Method      int GetHashCode()
GetType        Method      type GetType()
ToString       Method      string ToString()
Id             NoteProperty System.Int32 Id=3284
LoadProfile    NoteProperty System.Boolean LoadProfile=False
Name           NoteProperty System.String Name=alg

PS C:\> _
```

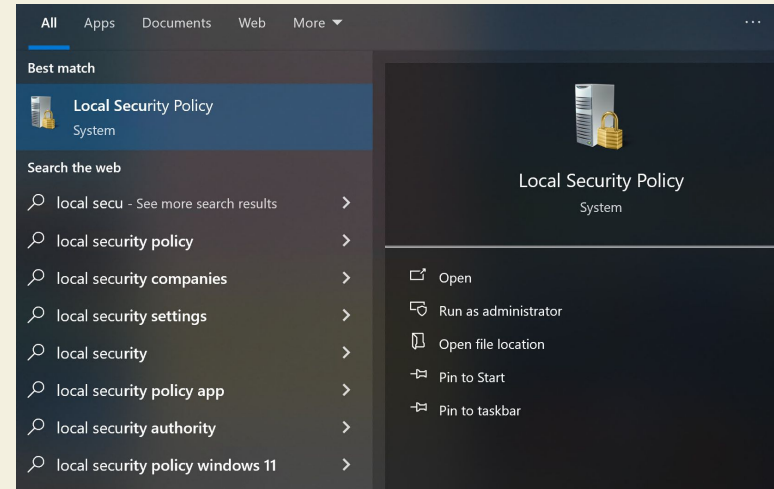
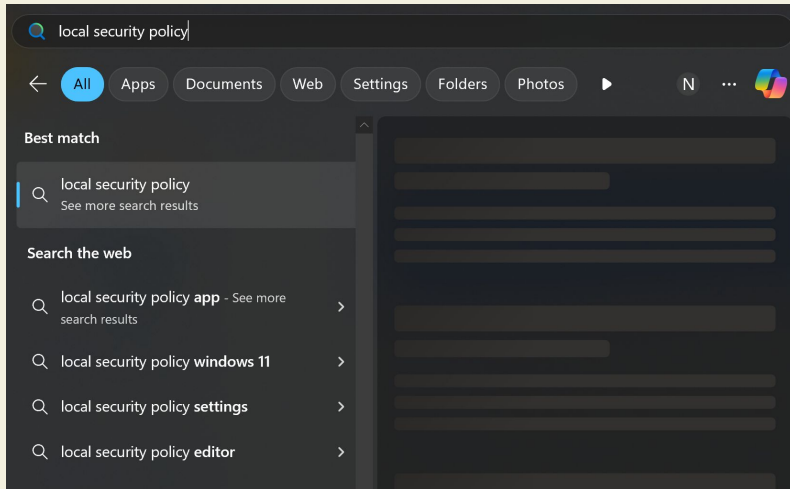


2. Windows Security Tools

Notes



DISCLAIMER: Some of the tools I'm about to mention do not appear in Windows Home editions, only in Pro / Enterprise / Education

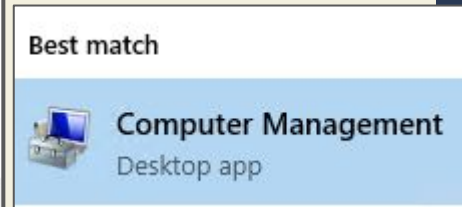
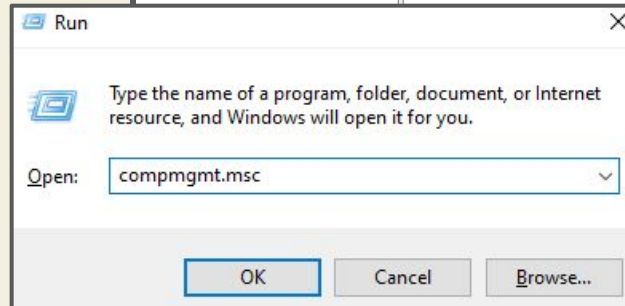
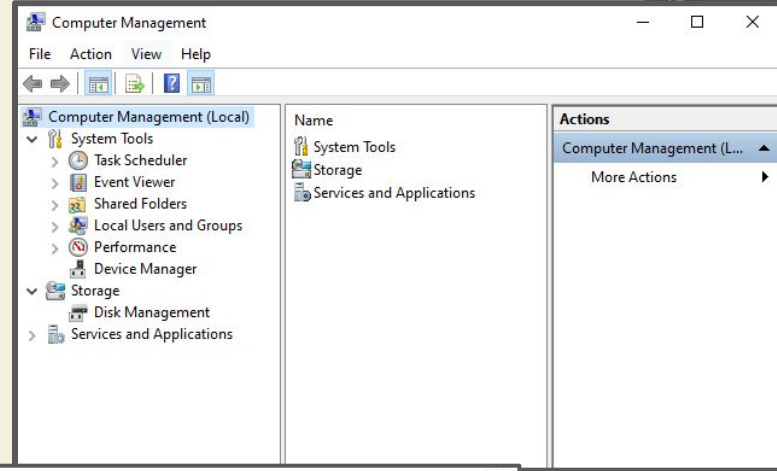


compmgmt.msc



Computer Management

- Interface for performing common administrative tasks
- Control Panel on steroids
- Links to other common administrative tools



Task Scheduler



- Windows utility for scheduling programs to run at certain times
- Triggers:
 - Times / Dates
 - When certain system events occur (logon, Event IDs, etc.)

Name	Status	Triggers
npcapwatchdog	Ready	At system startup
NvDriverUpdateCheckDaily_{B2FE1952-...	Ready	At 12:25 PM every day
NVIDIA GeForce Experience SelfUpdat...	Ready	On event - Log: Application, Source: NVIDIA GeForce Experience SelfUp...
NvNodeLauncher_{B2FE1952-0186-46-...	Ready	At log on of any user - After triggered, repeat every 1.00:00:00 indefinitel
NvProfileUpdaterDaily_{B2FE1952-018...	Ready	At 12:25 PM every day
NvProfileUpdaterOnLogon_{B2FE1952-...	Ready	At log on of any user
NvTmRep_CrashReport1_{B2FE1952-0-...	Ready	At 12:25 PM every day
NvTmRep_CrashReport2_{B2FE1952-0-...	Ready	At 6:25 PM every day
NvTmRep_CrashReport3_{B2FE1952-0-...	Ready	At 12:25 AM every day
NvTmRep_CrashReport4_{B2FE1952-0-...	Ready	At 6:25 AM every day
OneDrive Reporting Task-S-1-5-21-26...	Ready	At 11:06 PM on 12/15/2024 - After triggered, repeat every 1.00:00:00 inde
OneDrive Standalone Update Task-S-1...	Ready	At 10:00 PM on 5/1/1992 - After triggered, repeat every 1.00:00:00 indefir
WS4W Private Network (bc87228e-afd...	Ready	At system startup
WS4W Set NetIPAddress (1048541f-d0...	Ready	At system startup
ZoomUpdateTaskUser-S-1-5-21-26328...	Ready	At 12:57 AM every day - After triggered, repeat every 12:00:00 for a durat

Event Viewer



- “Logging service” of Windows
- Keeps track of events that Windows or other installed software reports to it
- Set what Windows logs in *Local Security Policy*

The screenshot shows the Windows Event Viewer interface. The left pane displays a tree view of event logs, with 'Windows Logs' expanded to show 'Application'. The main pane shows a table of events with columns for Level, Date and Time, Source, Event ID, and Task Category. The event with ID 16384 is selected and highlighted in blue. Below the table, the details for event 16384 are shown, including a 'General' tab with a message about a successful software protection service re-start.

Level	Date and Time	Source	Event ID	Task Category
Information	1/6/2025 12:07:37 PM	Security-SPP	16384	None
Information	1/6/2025 12:07:07 PM	Security-SPP	16394	None
Information	1/6/2025 12:02:28 PM	VSS	8224	None
Information	1/6/2025 11:59:33 AM	System-Restore	8302	None
Information	1/6/2025 11:59:33 AM	System-Restore	8301	None
Information	1/6/2025 11:59:28 AM	System Restore	8216	None
Information	1/6/2025 11:59:20 AM	System Restore	8300	None
Information	1/6/2025 11:59:10 AM	Security-SPP	16384	None
Information	1/6/2025 11:59:09 AM	System Restore	8194	None
Information	1/6/2025 11:58:04 AM	Security-SPP	16394	None
Information	1/6/2025 11:53:02 AM	edgeupdate	0	None
Information	1/6/2025 11:52:04 AM	Winlogon	6000	None
Information	1/6/2025 11:52:03 AM	Winlogon	6003	None
Information	1/6/2025 12:46:47 AM	Winlogon	6000	None
Information	1/6/2025 12:46:47 AM	Winlogon	6000	None

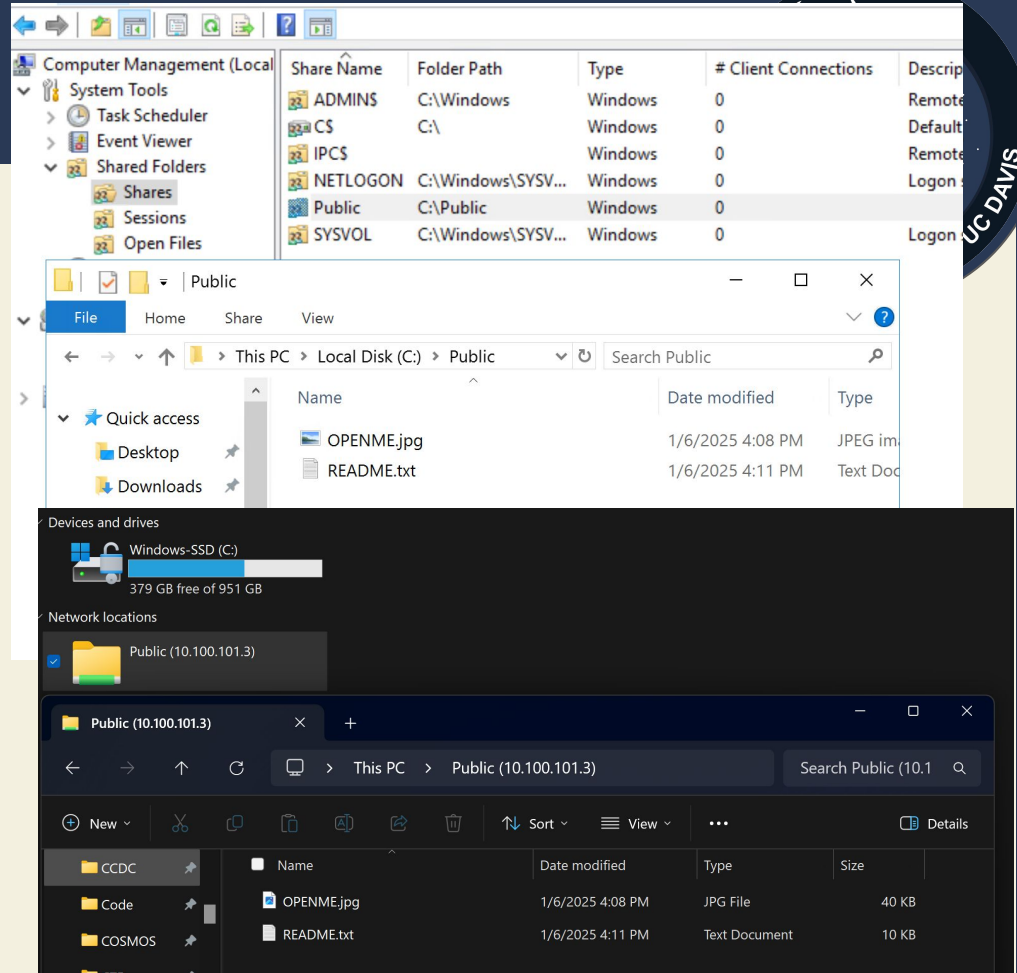
Event 16384, Security-SPP

General Details

Successfully scheduled Software Protection service for re-start at 2124-12-13T20:07:37Z. Reason: RulesEngine.

Shared Folders

- Folders on your hard drive can be shared with other computers over the SMB Protocol!
- Shares with '\$' at the end are there by default and hidden from normal users
- If you don't need it, disable it!
 - (And if you do, don't)



Local Users and Groups



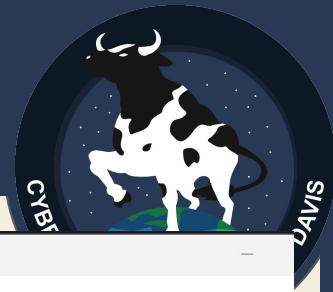
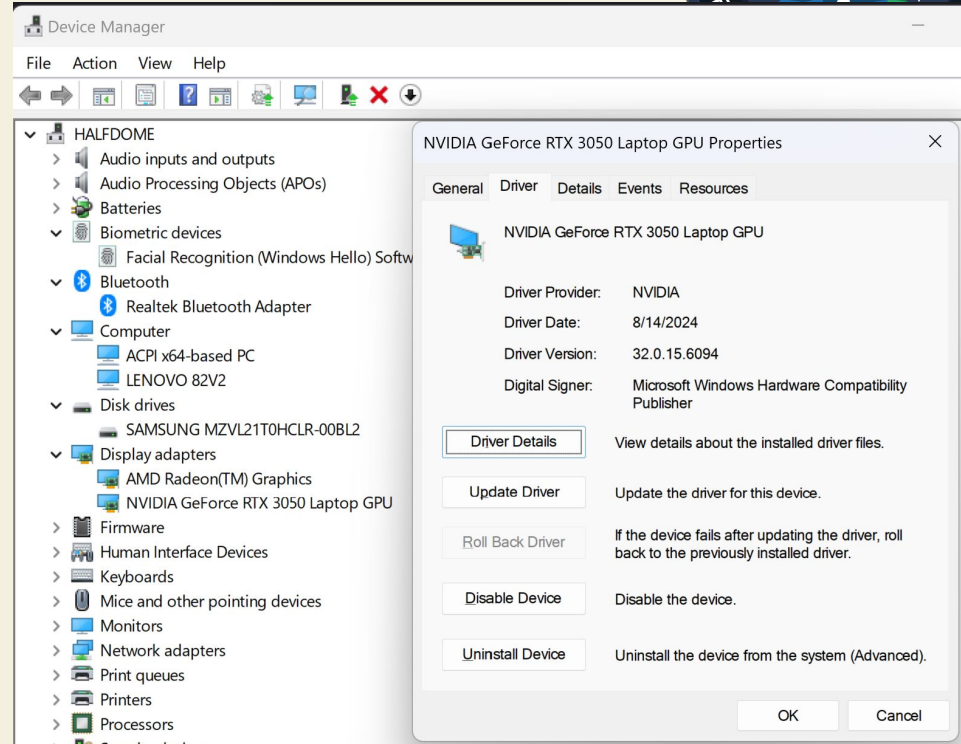
- Fast interface for managing...you guessed it
- Create / delete accounts, manage their properties and what groups they belong to
- Probably exists in Settings/Control Panel as well but this gives you more control

The screenshot shows the Windows Computer Management console. The left pane shows the tree view with 'Local Users and Groups' expanded, and 'Users' selected. The right pane shows a list of users: DefaultAccount, Home, Mr. North, NuclearFizzler, reptilelegit, and WDAGUtility... The 'Home' user is selected. A 'Home Properties' dialog box is open, showing the 'General' tab. The dialog has a 'Full name' text box, a 'Description' text box, and several checkboxes: 'User must change password at next logon', 'User cannot change password', 'Password never expires' (checked), 'Account is disabled', and 'Account is locked out'. The 'OK', 'Cancel', 'Apply', and 'Help' buttons are at the bottom.

Device Manager

- Settings for devices connected to your computer

See also: msinfo32.exe



Local Security Policy



- The “main” Windows security settings
- EX: Windows password requirements, Windows logging settings, force CTRL-ALT-DEL, etc.
- A lot! of policies
- See also: Local Group Policy

Security Settings	
Name	Description
> Account Policies	Password and account lockout policies
> Local Policies	Auditing, user rights and security options policies
> Windows Defender Firewall with Advanced Security	Windows Defender Firewall with Advanced Security
> Network List Manager Policies	Network name, icon and location group policies.
> Public Key Policies	
> Software Restriction Policies	
> Application Control Policies	Application Control Policies
> IP Security Policies on Local Computer	Internet Protocol Security (IPsec) Administration ...
> Advanced Audit Policy Configuration	Advanced Audit Policy Configuration

Windows Updates



- You should download them...but you already know how it is
- Certain variants of Windows allow Windows Updates to be controlled via Security Policy

A screenshot of the Windows Update settings page. The title "Windows Update" is at the top. Below it, a red message states "*Some settings are managed by your organization" with a link to "View configured update policies". A yellow mouse cursor points to a refresh icon. Below that, a notification says "You're not up to date" with a red exclamation mark icon and "Last checked: Today, 08:52 AM". A "Check for updates" button is visible. At the bottom, there is a section titled "Adjust active hours to reduce disruptions" with a message about automatic updates during active hours.

Windows Update

*Some settings are managed by your organization
[View configured update policies](#)

You're not up to date
Last checked: Today, 08:52 AM

Your device is missing important security and quality fixes.

[Check for updates](#)

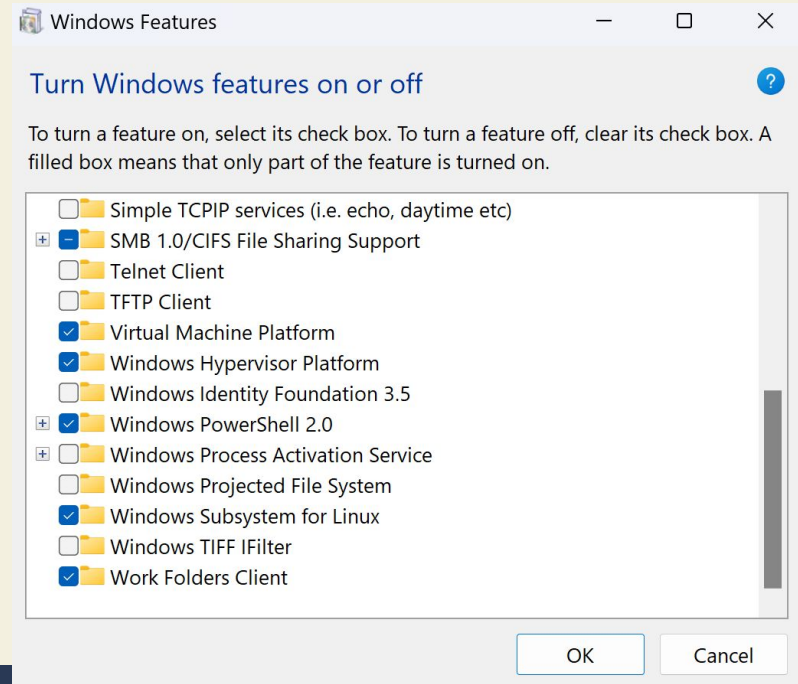
Adjust active hours to reduce disruptions

We noticed you regularly use your device between 10:00 AM and 11:00 PM. Would you like Windows to automatically update your active hours to match your activity? We won't restart for updates during this time.

Windows Features

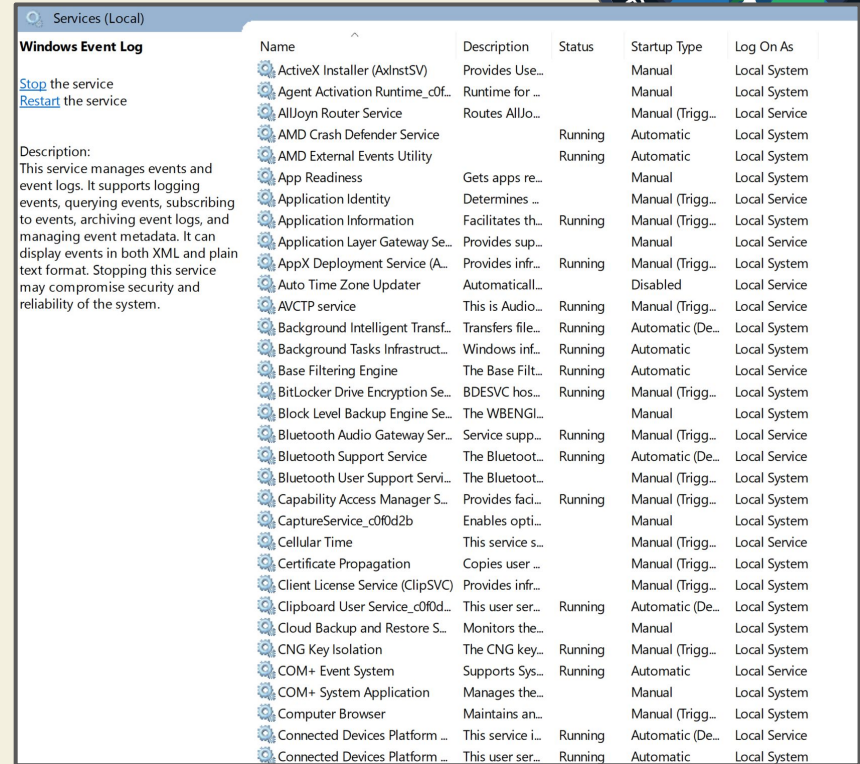


- Additions to Windows that can be installed separately from the operating system
- WSL, HyperV/Virtualization support, IIS (Web servers), etc.
- Again, add/remove at your discretion



Services

- List of all processes/programs on the computer that may run in the background continuously
- Does not describe if it's running (Task Manager) but its overall status and permissions
- “Things that need to run constantly vs periodically” Services vs Task Scheduler



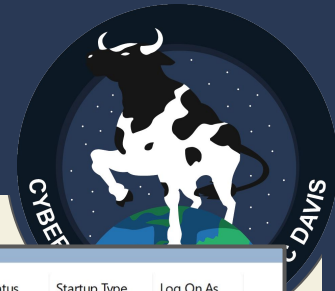
Services (Local)

Windows Event Log

[Stop](#) the service
[Restart](#) the service

Description:
This service manages events and event logs. It supports logging events, querying events, subscribing to events, archiving event logs, and managing event metadata. It can display events in both XML and plain text format. Stopping this service may compromise security and reliability of the system.

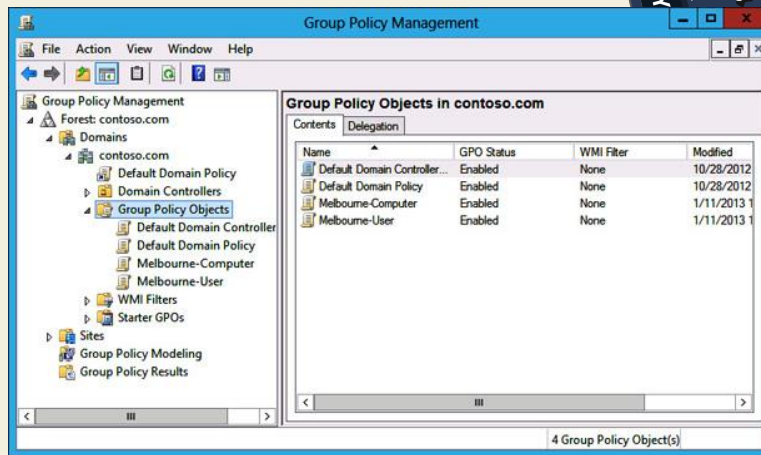
Name	Description	Status	Startup Type	Log On As
ActiveX Installer (AxInstSV)	Provides Use...		Manual	Local System
Agent Activation Runtime_cof...	Runtime for ...		Manual	Local System
AllJoyn Router Service	Routes AllJo...		Manual (Trigg...	Local Service
AMD Crash Defender Service		Running	Automatic	Local System
AMD External Events Utility		Running	Automatic	Local System
App Readiness	Gets apps re...		Manual	Local System
Application Identity	Determines ...		Manual (Trigg...	Local Service
Application Information	Facilitates th...	Running	Manual (Trigg...	Local System
Application Layer Gateway Se...	Provides sup...		Manual	Local Service
AppX Deployment Service (A...	Provides infr...	Running	Manual (Trigg...	Local System
Auto Time Zone Updater	Automaticall...		Disabled	Local Service
AV/CTP service	This is Audio...	Running	Manual (Trigg...	Local Service
Background Intelligent Transf...	Transfers file...	Running	Automatic (De...	Local System
Background Tasks Infrastruct...	Windows inf...	Running	Automatic	Local System
Base Filtering Engine	The Base Fil...	Running	Automatic	Local Service
BitLocker Drive Encryption Se...	BDESVC hos...	Running	Manual (Trigg...	Local System
Block Level Backup Engine Se...	The WBENGL...		Manual	Local System
Bluetooth Audio Gateway Ser...	Service supp...	Running	Manual (Trigg...	Local Service
Bluetooth Support Service	The Bluetooth...	Running	Automatic (De...	Local Service
Bluetooth User Support Servi...	The Bluetooth...		Manual (Trigg...	Local System
Capability Access Manager S...	Provides faci...	Running	Manual (Trigg...	Local System
CaptureService_c0f0d2b	Enables opti...		Manual	Local System
Cellular Time	This service s...		Manual (Trigg...	Local Service
Certificate Propagation	Copies user ...		Manual (Trigg...	Local System
Client License Service (ClipSVC)	Provides infr...		Manual (Trigg...	Local System
Clipboard User Service_c0f0d...	This user ser...	Running	Automatic (De...	Local System
Cloud Backup and Restore S...	Monitors the...		Manual	Local System
CNG Key Isolation	The CNG key...	Running	Manual (Trigg...	Local System
COM+ Event System	Supports Sys...	Running	Automatic	Local Service
COM+ System Application	Manages the...		Manual	Local System
Computer Browser	Maintains an...		Manual (Trigg...	Local System
Connected Devices Platform ...	This service i...	Running	Automatic (De...	Local Service
Connected Devices Platform ...	This user ser...	Running	Automatic	Local System



Command Line Automation



- Everything I just mentioned can be done via PowerShell or Command Prompt!
- Hardening scripts / Policy automation!
 - Deploy Group Policy templates
 - Deploy scripts to set settings and run utilities automatically!



```
[*] 9/4/2022 8:54:12 AM - Starting HardeningKitty

[*] 9/4/2022 8:54:12 AM - Getting user information
[*] Hostname: DESKTOP-DG83TOD
[*] Domain: WORKGROUP

...

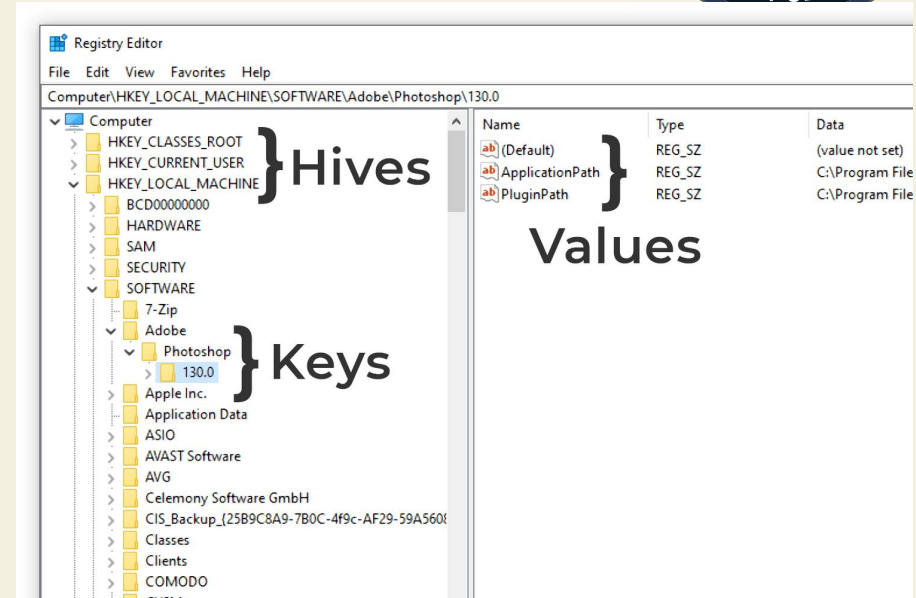
[*] [*] 9/4/2022 8:54:12 AM - Starting Category Account Policies
[👉] ID 1103, Store passwords using reversible encryption, Result=0, Severity=Passed
[👉] ID 1100, Account lockout threshold, Result=10, Severity=Passed
[👉] ID 1101, Account lockout duration, Result=30, Severity=Passed

...
```

Registry



- All of these menus and GUIs are “front ends” for databases containing security rules!
 - Registry - Stores operating system settings and config data! (Think the **etc** folder!)
 - Authentication / User data databases



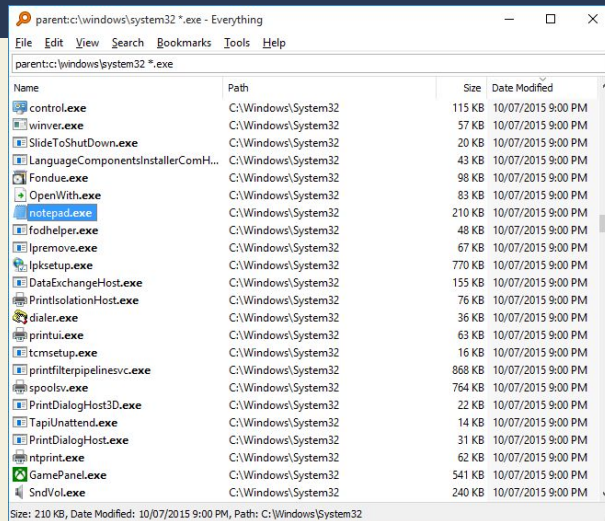


3. Other Security Tools

Random Useful Things



- Windows Package Managers
 - Chocolatey, Winget
- Everything
 - Fast file searcher
- Ninite
 - Installer bundler for quickly installing software



Let's install [Notepad++](#).

1. Open a command line as an administrator.
2. Type `choco install notepadplusplus` and press Enter.
3. That's it. Pretty simple but powerful little concept!