

Sun City Computer Club

Windows SIG

June 14, 2022

**Questions, Comments, Suggestions welcomed at
any time**

Even Now

- [Audio Recording of this session](#)
- Use the link above to access MP4 audio recording
- Audio Recording in Progress
- SIG attendees are required to be members of the chartered club sponsoring that SIG.
Sun City Community Association By-law
- Sig leader – anyone?
- Topic Suggestions – plea(se)
- Your suggestions future presentations
- In person meetings

- 60 vulnerabilities 3 critical
- NOT Follina
- 9.8 RCE NFS & Hyper-V



Microsoft Patch Tuesday June 2022

Windows Malicious Software Removal Tool x64 - v5.102 (KB890830)

Installing - 0%

2022-06 Cumulative Update for Windows 11 for x64-based Systems (KB5014697)

Downloading - 4%



Windows Web Experience Pack
Microsoft Windows

Apps

Modified moments ago



Microsoft Whiteboard
Microsoft Corporation

Apps

Modified moments ago



Evernote
Evernote

Apps

Modified moments ago

Microsoft Update Tuesday

2022-06 Cumulative Update for Windows 10 Version 21H2 for x64-based Systems (KB5014699)

Status: Installing - 0%

Microsoft Patch Tuesday Windows 10

- Live captions
Settings > Accessibility > Captions
Live captions
At top, near most web cams - or move
fonts, size, color, background, etc.
generated on device – privacy
- Voice access
Settings > Accessibility > Speech
- Narrator
Settings > Accessibility > Narrator
Sight challenged, multi-tasking, ...

Windows 11 Accessibilities

ANNOUNCEMENTS

- Williamson county officials reporting jury scam calls
- Chromium Based Browser Updates around June 10
- June 16 Next Cyber Security SIG Presentation via zoom

- Windows 10

[2022-05 Cumulative Update Preview for .NET Framework 3.5 and 4.8 for Windows 10 Version 21H2 for x64 \(KB5013887\)](#)

Successfully installed on 6/5/2022

[2022-05 Cumulative Update Preview for Windows 10 Version 21H2 for x64-based Systems \(KB5014023\)](#)

Successfully installed on 6/3/2022

Recent Optional Quality Updates

- Windows 11

2022-05 Cumulative Update Preview for .NET Framework 3.5 and 4.8 for Windows 11 for x64 (KB5013889)
Successfully installed on 5/26/2022

2022-05 Cumulative Update for Windows 11 for x64-based Systems (KB5014019)
Successfully installed on 5/26/2022

Recent Optional Quality Updates



Settings

Personalization > Background

Find a setting

- System
- Bluetooth & devices
- Network & internet
- Personalization**
- Apps
- Accounts
- Time & language
- Gaming
- Accessibility
- Privacy & security
- Windows Update

Personalize your background
 A picture background applies to your current desktop. Solid color or slideshow backgrounds apply to all your desktops. Windows spotlight

Related settings

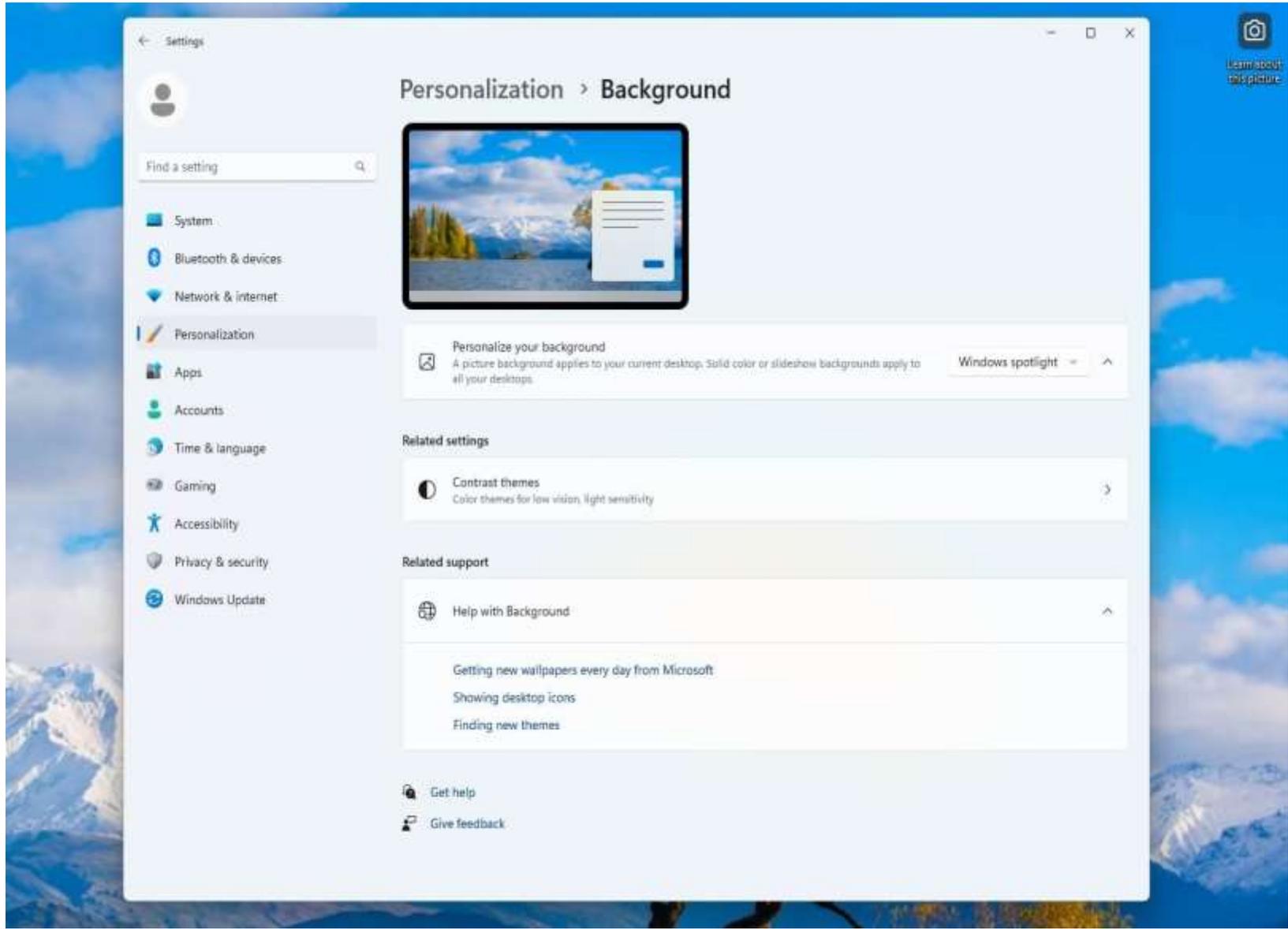
Contrast themes
 Color themes for low vision, light sensitivity

Related support

Help with Background

Getting new wallpapers every day from Microsoft
 Showing desktop icons
 Finding new themes

Get help
 Give feedback



- Microsoft fixed an issue where searchindexer.exe could affect shapes in Microsoft Visio.
- Microsoft fixed an issue where adding a trusted user, group or computer could result in the error message "The object selected doesn't match the type of destination source".
- Microsoft fixed an issue that could affect the brightness of displays after you change the display mode.
- Microsoft fixed an issue that crashes apps using d3d9.dll with certain graphics cards.
- Microsoft fixed an issue that causes some users to see a black screen.
- Microsoft fixed an issue that causes print failures.

Varied fixes Windows 11 Optional Update

- October release?
- Stickers
- Add to desktop - survives wallpaper change



Windows 11 22H2 features?

← Settings

Personalization > Background

Find a setting

- System
- Bluetooth & devices
- Network & internet
- Personalization**
- Apps
- Accounts
- Time & language
- Gaming
- Accessibility
- Privacy & security
- Windows Update



Personalize your background
A picture background applies to your current desktop. Solid color or slideshow backgrounds apply to all your desktops. Windows spotlight

Choose stickers for your wallpaper Add stickers

Related settings

- Contrast themes**
Color themes for low vision, light sensitivity

Related support

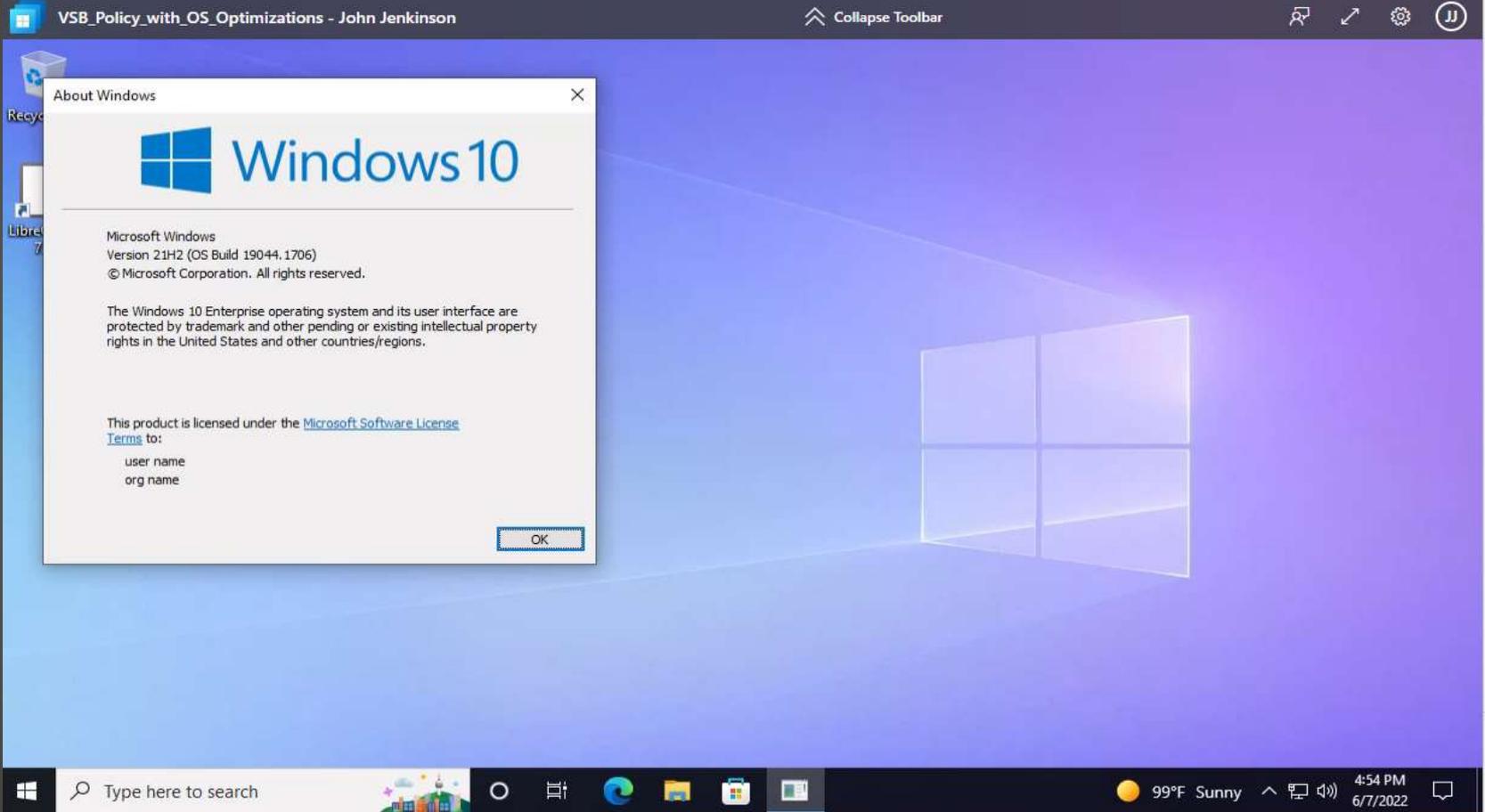
- Help with Background**

Getting new wallpapers every day from Microsoft
Showing desktop icons
Finding new themes

- Public preview
- Enterprise E3 or greater
- Tenant concept

Windows Autopatch

Windows 10 Version 21H2 19044.1706



Windows 365



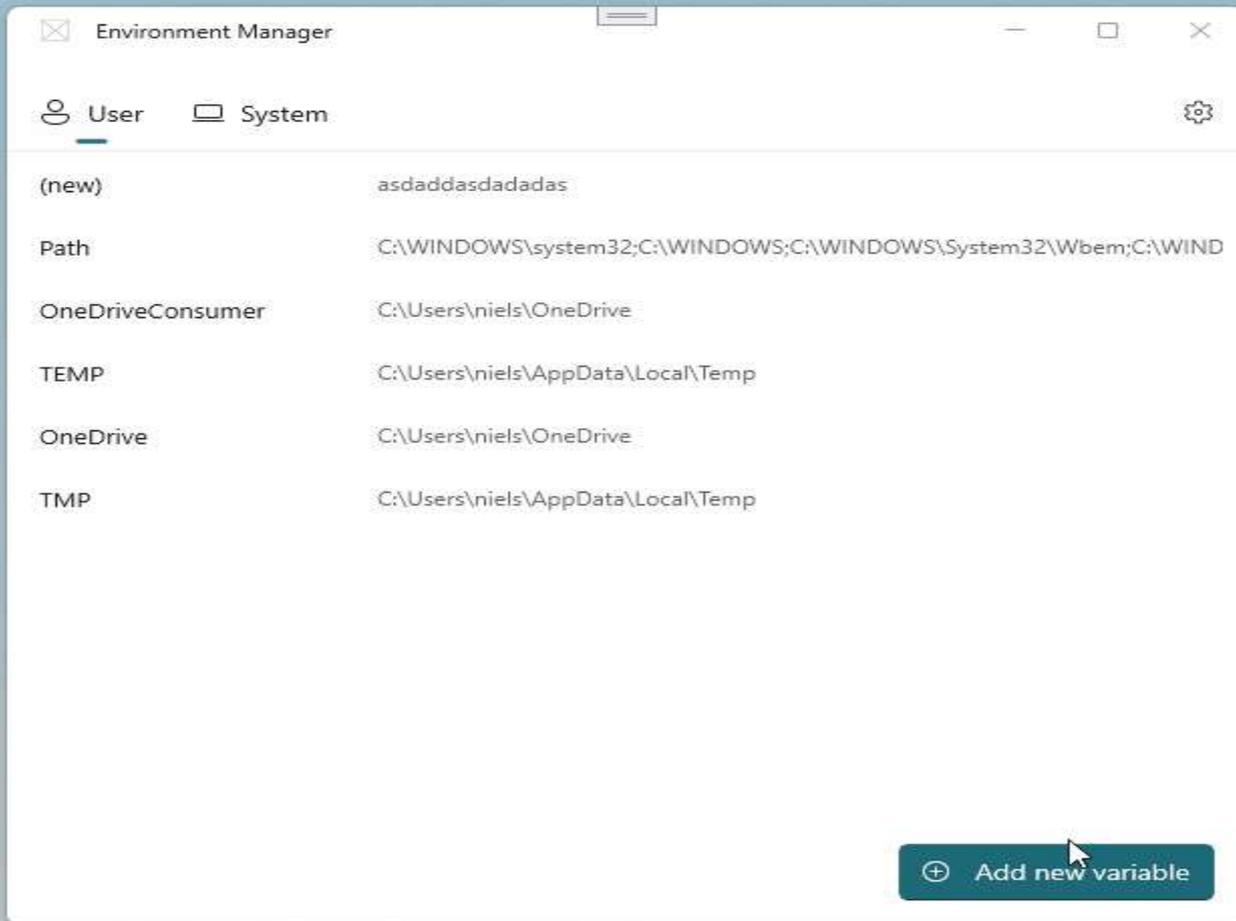
- Windows Insider Dev channel 25126
- RTM (Release to Manufacturing) 22621

September, October?

Windows 11 22H2 Sun Valley 2

- Advanced tool for environment variables
e.g. \$PATH

**PowerToys tool
Environment Manager**



- Android 12.1
- Advanced networking Same network as PC
- Better Windows integration
- Improved mouse scroll
- Camera improvements
 - camera orientation, preview, feed
- Improved VP8 & VP9 codecs
- Better settings app
- Current version 2203.40000.3.0
- Dev channel version 2204.40000.19.0

Windows Subsystem for Android

- Task Manager
- taskkill shortcut
Right-click desktop empty space
New > Shortcut
taskkill /f /fi "status eq not responding"
/f – force
/fi - filter
Name shortcut
Finish

Keyboard shortcut?

Force Quit – another method

- MS Office remote template feature
HTML file from remote server
ms-msdt://URI scheme
load code & PowerShell
EVEN tho macros disabled!!
bypass Protected view using RTF extension

Current workaround:

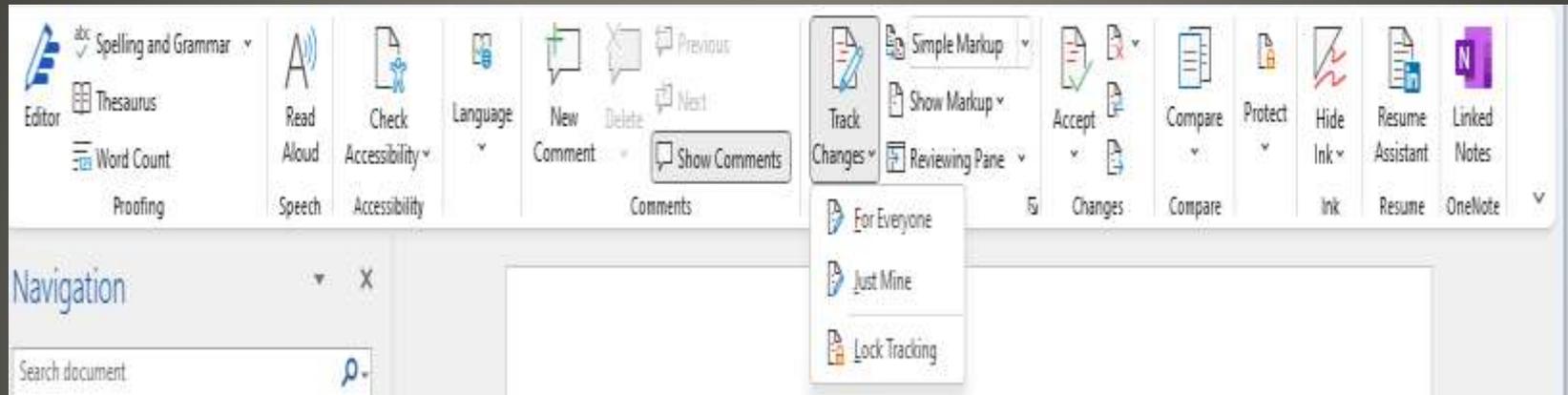
CMD prompt as Administrator

```
"reg delete HKEY_CLASSES_ROOT\ms-msdt /f"
```

NOT detected by Windows Defender

MSDT Follina

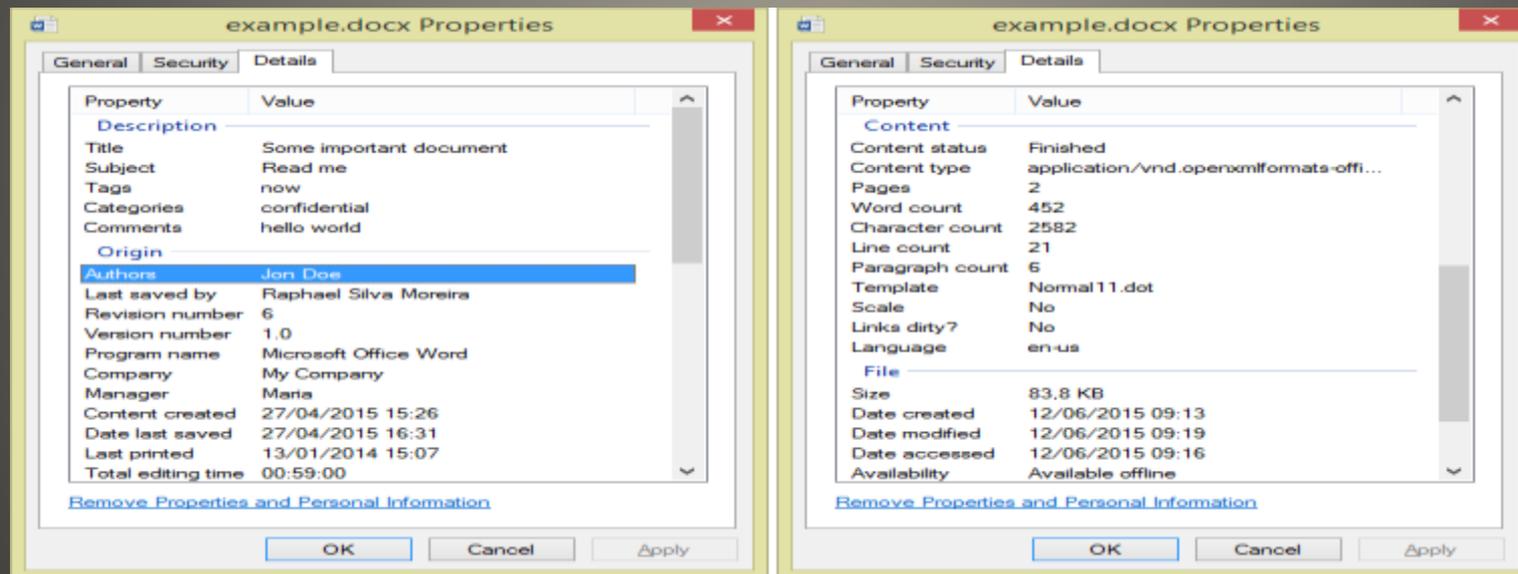
- Office files with Track Changes



Windows Metadata

- File Metadata

Right click > Properties > Details > Remove Properties and Personal Information



Windows Metadata

- Create a copy with all possible properties removed
- Remove the following properties from this file
- Helpful <> Harmful
- Backup / archive

Windows Metadata

- Windows Subsystem for Linux (WSL) malware steals browser auth cookies
- WSL malware increasing
Using telegraph to communicate
standard RAT capabilities
- Free & low costs VPN revenue
Ads
Cookies
Tracking pixels
Freemium
VPN logs
Sell the data

Current Issues

Been there...

FRIDAY EVENING



PERFECT!
I'LL FINISH
THIS ON
MONDAY



MONDAY MORNING...

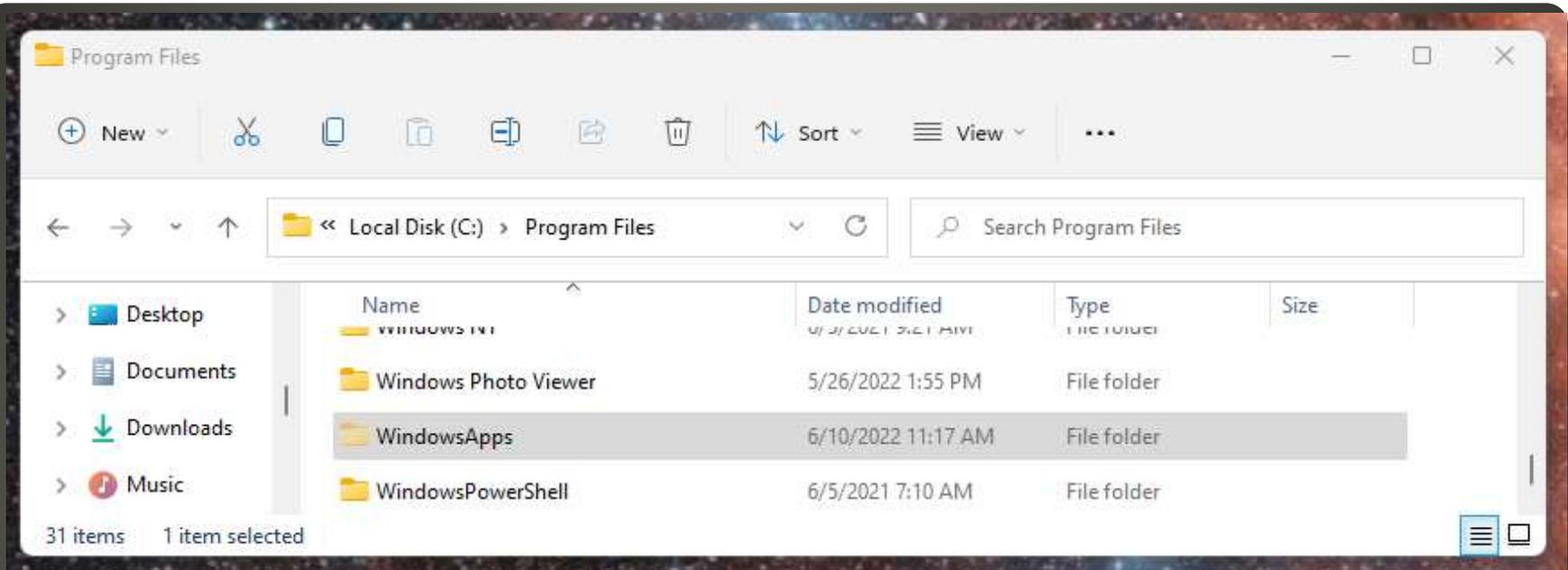


WHAT DOES
THIS MEAN!?!?

- DuckDuckGo
- NOT a windows browser
- Can be search engine
- Can be default search engine
- Browser on iOS, Android, macOS (beta)
- Privacy reputation - yeahbut
- Blocks ads & trackers - to a degree
- ALLOWS Microsoft tracking
Bing & LinkedIn

Bing on Amazon

Current Issues



WindowsApps folder

Program Files

New | Sort | View

<< Local Disk (C:) > Program Files

- > Desktop
- > Documents
- > Downloads
- > Music

Name
Windows 10
Windows Photo Viewer
WindowsApps
WindowsPowerShell

31 items 1 item selected

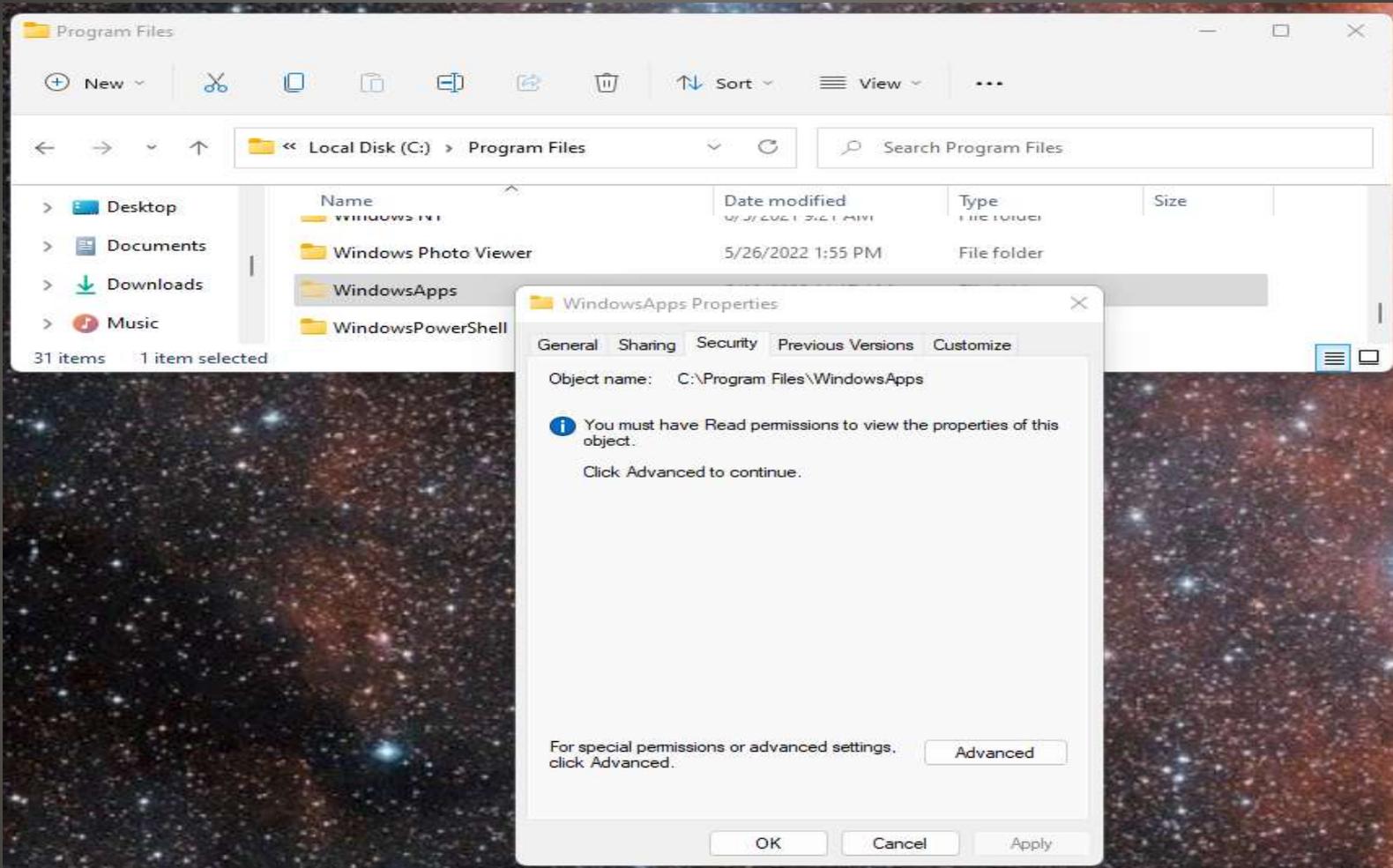
- Extra large icons
- Large icons
- Medium icons
- Small icons
- List
- Details
- Tiles
- Content
- Compact view

Show >

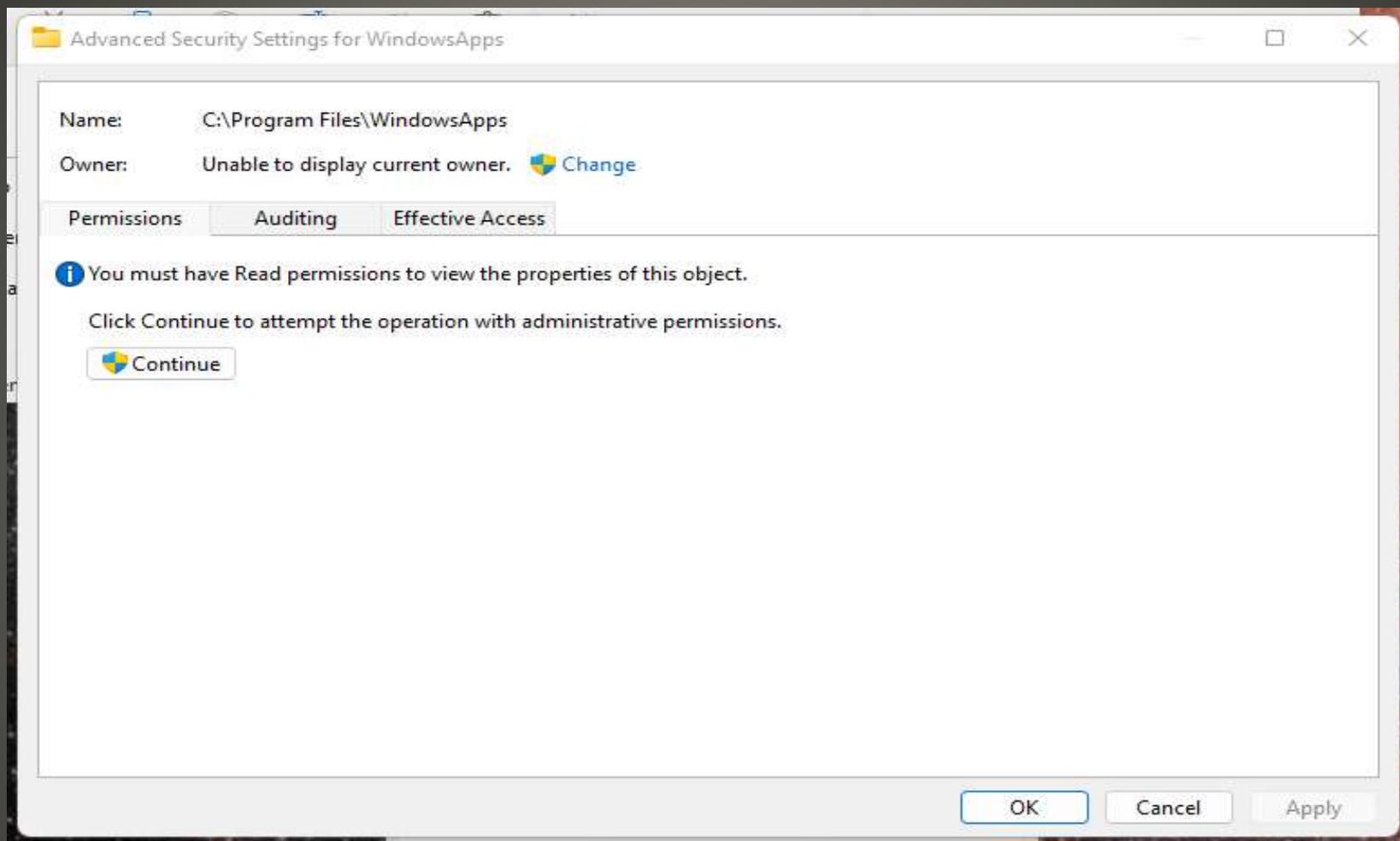
- Navigation pane
- Details pane
- Preview pane
- Item check boxes
- Hidden items

Show or hide the files and folders that are marked as hidden.

WindowsApps Folder

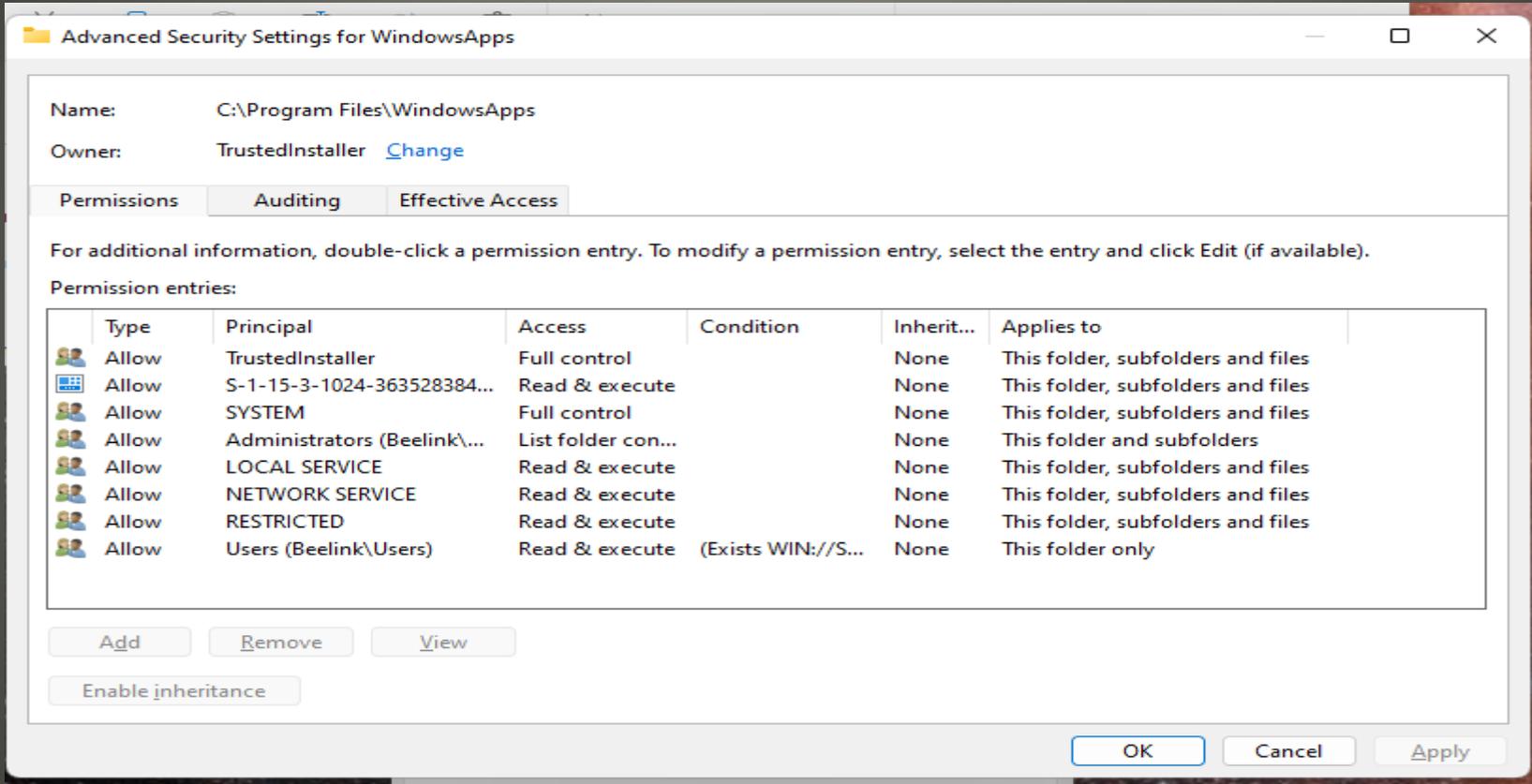


WindowsApps folder

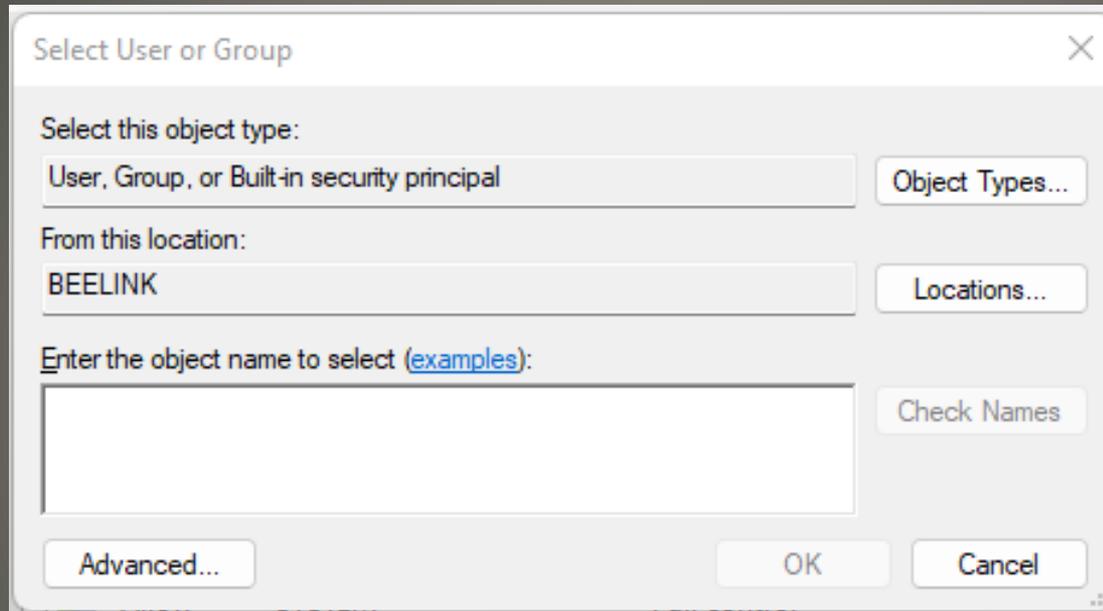


WindowsApp folder

• UAC - please



WindowsApp folder

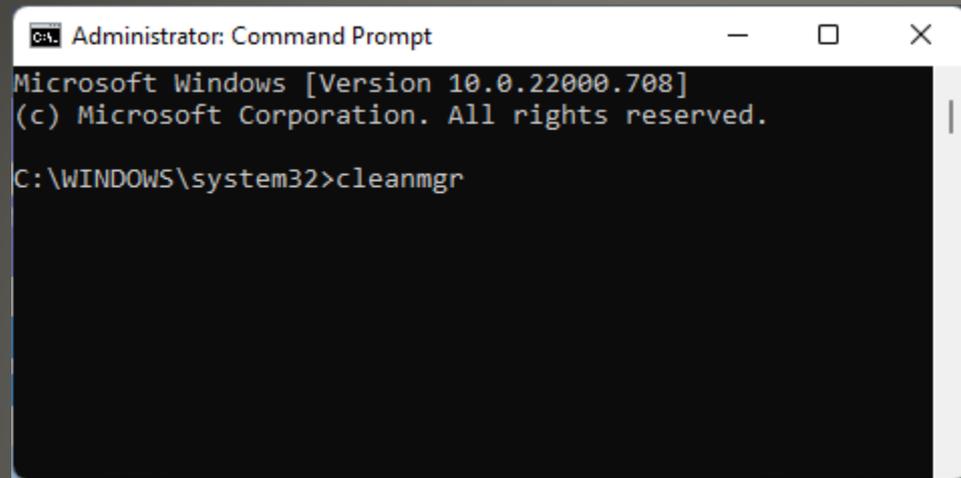


WindowsApp folder

- PowerShell As Administrator - please

```
takeown /f "C:\Program Files\WindowsApps" /r
```

WindowsApp folder

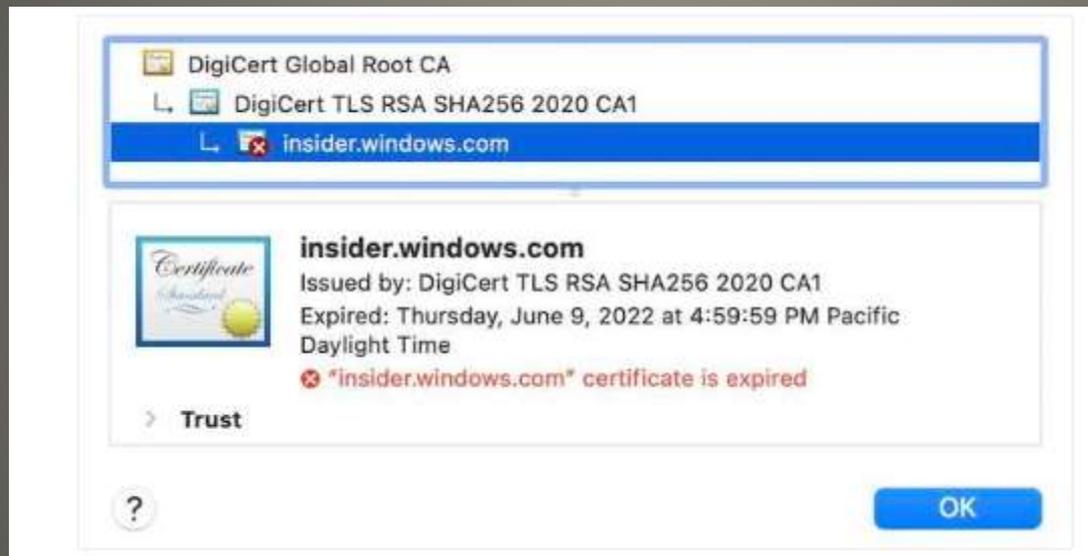


```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.22000.708]
(c) Microsoft Corporation. All rights reserved.

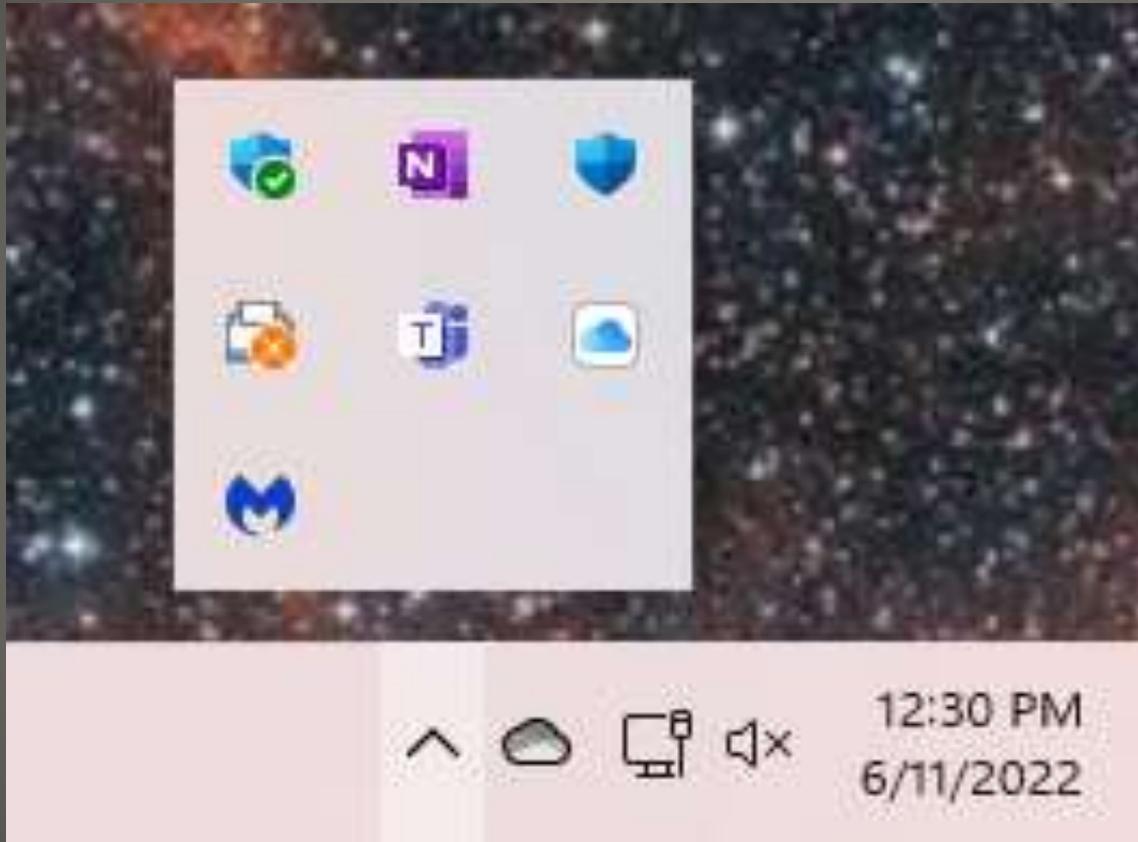
C:\WINDOWS\system32>cleanmgr
```

Clean Windows

- insider.windows.com



Microsoft Insiders Certificate expired



Windows Defender

- Full Scan
- Actions

The screenshot displays the Windows Security application window. On the left is a navigation pane with the following items: Home, Virus & threat protection (selected), Account protection, Firewall & network protection, App & browser control, Device security, Device performance & health, and Family options. The main content area is titled 'Virus & threat protection' and includes the subtitle 'Protection for your device against threats.' Below this is a section for 'Current threats' with the text 'Threats found. Start the recommended actions.' A list of four threats is shown, each with a severity level of 'Severe' and a timestamp of '2020-06-05 07:32 (Active)'. The first threat, 'Backdoor:MacOS/Mettle.AIMTB', has an expanded view showing 'Action options: Remove (selected), Quarantine, Allow on device' and a 'See details' link. The other three threats are 'Exploit:MSIL/CVE-2013-0074.A', 'VirTool:Java/Donk!rfrn', and 'Exploit:SWF/CVE-2015-5119'.

Threat Name	Severity
Backdoor:MacOS/Mettle.AIMTB 2020-06-05 07:32 (Active)	Severe
Exploit:MSIL/CVE-2013-0074.A 2020-06-05 07:32 (Active)	Severe
VirTool:Java/Donk!rfrn 2020-06-05 07:32 (Active)	Severe
Exploit:SWF/CVE-2015-5119 2020-06-05 07:32 (Active)	Severe

Windows Defender

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

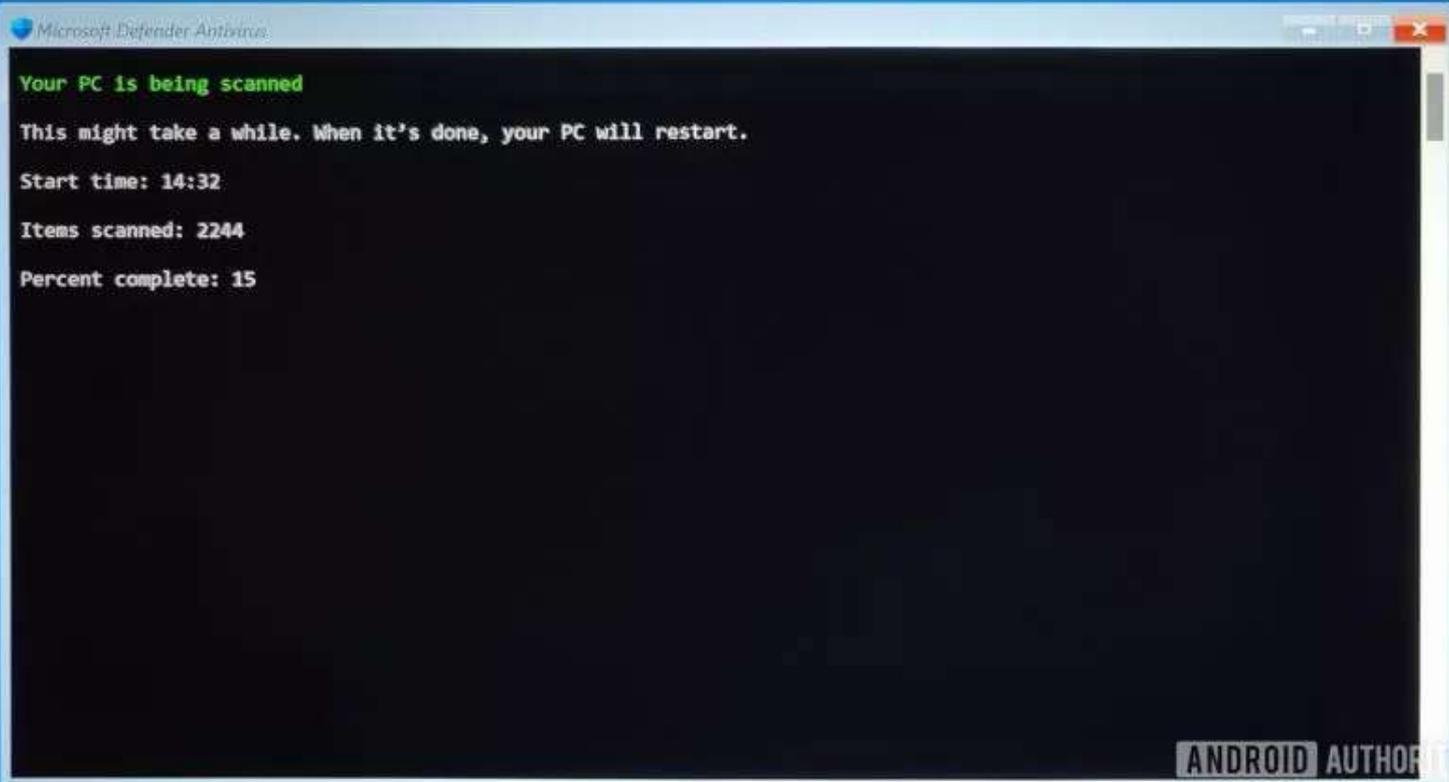
Choose which files and locations you want to check.

Microsoft Defender Offline scan

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

Scan now

Windows Defender



Windows Defender

- Media Creation Tool
- Cycle thru several
- Use Help Center
- Periodic Clean Install

Remove Virus

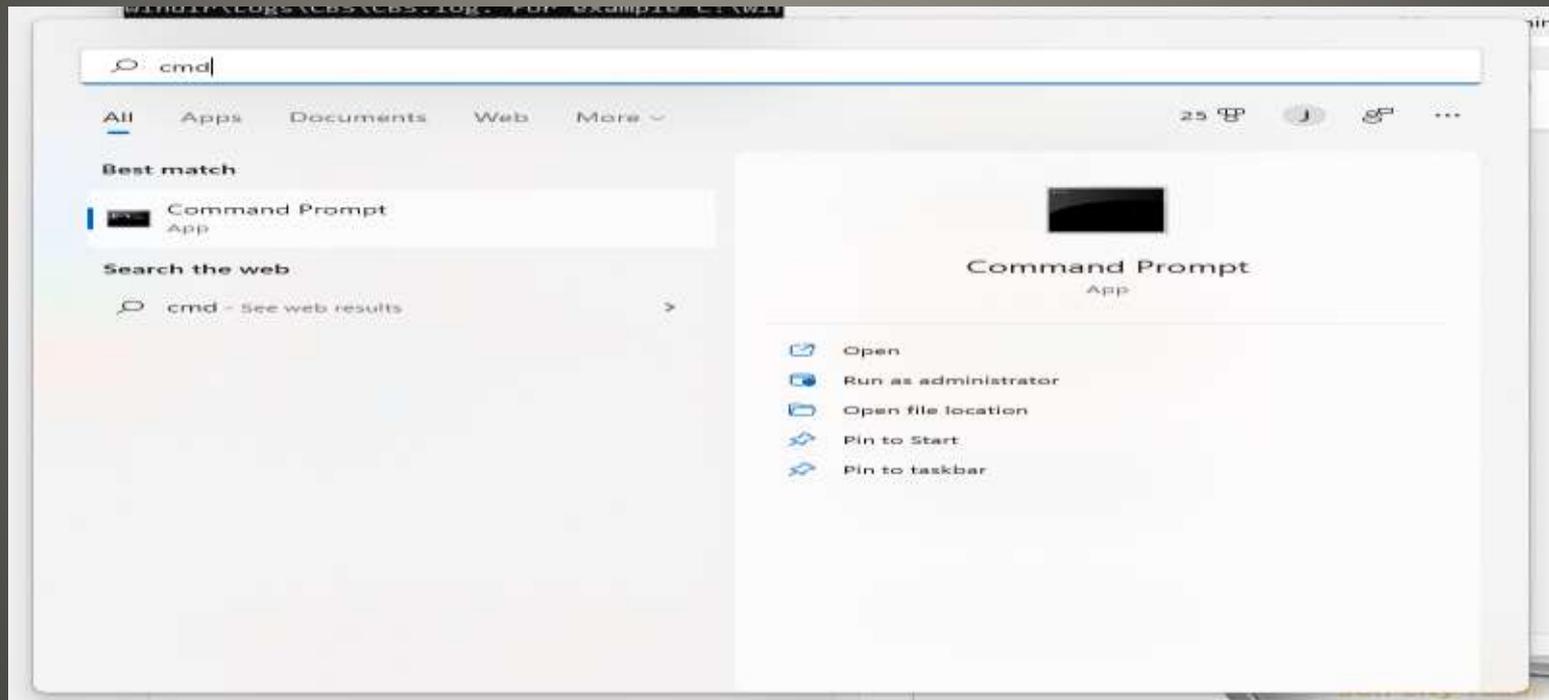
- Fit for purpose
 - OneDrive and iCloud support both
 - Google Drive, Dropbox, Verizon cloud, Box, Amazon Drive,
 - Network Sharing NAS, SMB
- Windows Show more options
Give Access To
Specific People
- macOS System Preferences
Sharing

Windows & macOS

- Clipboard shared CAUTION Private data
- Keyboard Mouse Trackpad Monitor sharing
- Office Suites Office 365, Libre Office
- Filesystem Formats
- Remote Desktops
- VMs Parallels

Windows & macOS

- System File Checker SFC
- Search CMD Run as Administrator PLEASE



Windows Filesystem

C:\ Administrator: Command Prompt

Microsoft Windows [Version 10.0.22000.708]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>SFC /scannow

Beginning system scan. This process will take some time.

Beginning verification phase of system scan.
Verification 100% complete.

Windows Resource Protection found corrupt files and successfully repaired them.
For online repairs, details are included in the CBS log file located at
windir\Logs\CBS\CBS.log. For example C:\Windows\Logs\CBS\CBS.log. For offline
repairs, details are included in the log file provided by the /OFFLOGFILE flag.

C:\WINDOWS\system32>

- Windows Resource Protection:
 - 1) did not find any integrity violations
 - 2) could not perform the requested operation
 - 3) found corrupt files and successfully repaired
 - 4) found corrupt files but was unable to fix some

Scan Results

The screenshot shows a Windows File Explorer window titled 'CBS'. The address bar indicates the path is 'Windows > Logs > CBS'. The left sidebar shows the 'Local Disk (C:)' with various folders like 'SWinREAgent', 'Aiseesoft Stuc', 'Aiseesoft Tem', 'Driver', 'Intel', 'OneDriveTem', and 'PerfLogs'. The main pane displays a list of files with columns for Name, Date modified, Type, and Size. The 'CBS' file is selected.

Name	Date modified	Type	Size
CBS	6/13/2022 1:42 PM	Text Document	9,221 KB
CbsPersist_20220426141027	4/26/2022 9:09 AM	Cabinet File	5,920 KB
CbsPersist_20220426142344	4/26/2022 9:21 AM	Cabinet File	4,619 KB
CbsPersist_20220510173240	5/10/2022 12:32 PM	Cabinet File	11,582 KB
CbsPersist_20220526184558	5/26/2022 1:45 PM	Cabinet File	7,552 KB
CbsPersist_20220526185613	5/26/2022 1:55 PM	Cabinet File	4,923 KB

6 items 1 item selected 9.00 MB

Access file Notepad or similar

- None of us are as experienced as all of us
- Awareness, Preparedness, Understanding
- Participate
- Topic Suggestions
- Questions: scccwindows@gmail.com

