

Sun City Computer Club

Windows SIG

September 13, 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

- Ever want to be a presenter??

Presenter???

Windows Update



Updates available

Last checked: Today, 12:38 PM

Windows Malicious Software Removal Tool x64 - v5.105
(KB890830)

Status: Pending install

2022-09 .NET Core 3.1.29 Security Update for x64 Client
(KB5017903)

Status: Pending install

2022-09 Cumulative Update for .NET Framework 3.5, 4.8 and
4.8.1 for Windows 10 Version 21H2 for x64 (KB5017500)

Status: Pending install

2022-09 Cumulative Update for Windows 10 Version 21H2 for
x64-based Systems (KB5017308)

Status: Downloading - 1%

Microsoft Update Tuesday



Updates available

Last checked: Today, 8:21 AM

Download now

2022-08 Cumulative Update for Windows 11 for x64-based Systems (KB5016691)

Downloading - 4%



Updates available

Last checked: Today, 1:07 PM

Install now

Windows Malicious Software Removal Tool x64 - v5.105 (KB890830)

Installing - 0%

2022-09 Cumulative Update for Windows 11 for x64-based Systems (KB5017328)

Downloading - 4%

2022-09 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for Windows 11 for x64 (KB5017497)

Pending install

Windows 11

- 79 Vulnerabilities
- 5 Critical
- 2 Previously disclosed
- 1 Actively being exploited



Microsoft Windows Update Tuesday

- POST Power On Self Test
- BIOS -> UEFI
- BIOS Basic Input Output System
Master Boot Record
- UEFI Unified Extensible Firmware
More features GUID Partition table
Secure boot

BIOS UEFI

ASUS UEFI BIOS Utility - EZ Mode

08/03/2083 21:03 Tuesday English

Information
 PRIME B350-PLUS BIOS Ver. 5407
 AMD Ryzen 7 1700 Eight-Core Processor

Speed: 3000 MHz
 Memory: 4096 MB (DDR4 2133MHz)

DRAM Status
 DIMM_A1: N/A
 DIMM_A2: SK Hynix 4096MB 2133MHz
 DIMM_B1: N/A
 DIMM_B2: N/A

D.O.C.P.
 Disabled Disabled

FAN Profile
 CPU FAN 2089 RPM
 CHA1 FAN N/A
 CHA2 FAN N/A

CPU FAN
 47°C
 QFan Control

VDDCR CPU Voltage
 1.090 V

Motherboard Temperature
 37°C

SATA Information
 SATA6G_1: HGST HTS725050A7E630 (500.1GB)
 SATA6G_2: INTEL SSDSC2BW256H6 (256.0GB)
 SATA6G_3: HGST HTS541010A9E680 (1000.2GB)
 SATA6G_4: Samsung SSD 860 EVO 250GB (250.0GB)
 SATA6G_5: Micron 1100_MTFDDAK512TBN (126.8GB)
 SATA6G_6: SanDisk SSD U1110 128GB (126.8GB)
 M.2: N/A

Copyright (C) 1984-1999 Award

Features
 Features
 Chipset Features
 Peripherals
 Management Setup
 Configurations
 Health Status

Frequency/Volts
 Load Fail-Safe
 Load Optimizer
 Set Supervisory
 Set User Password
 Save & Exit
 Exit Without Saving

Quit
 Save & Exit Setup

Time, Date, Hard Disk Type...

UEFI / BIOS

- Global Partition Table (GPT)
- Windows 11 Secure Boot and TPM
TPM – Trusted Platform Module

Convert MBR & BIOS -> UEFI

- Option 1

Start menu Power Button

Shift + Restart





















Accessing BIOS

Type here to search


Pinned

All apps >

 Edge	 Mail	 Calendar	 Microsoft Store	 Photos	 Settings
 Office	 Solitaire	 Adobe Express	 Spotify	 WhatsApp	 Twitter
 Clipchamp	 Prime Video	 TikTok	 Instagram	 Facebook	 Calculator

Recommended

To show your recent files and new apps, turn them on in [Start settings](#)

-  Disconnect
-  Shut down
-  Restart

 Ham

Microsoft Store

1



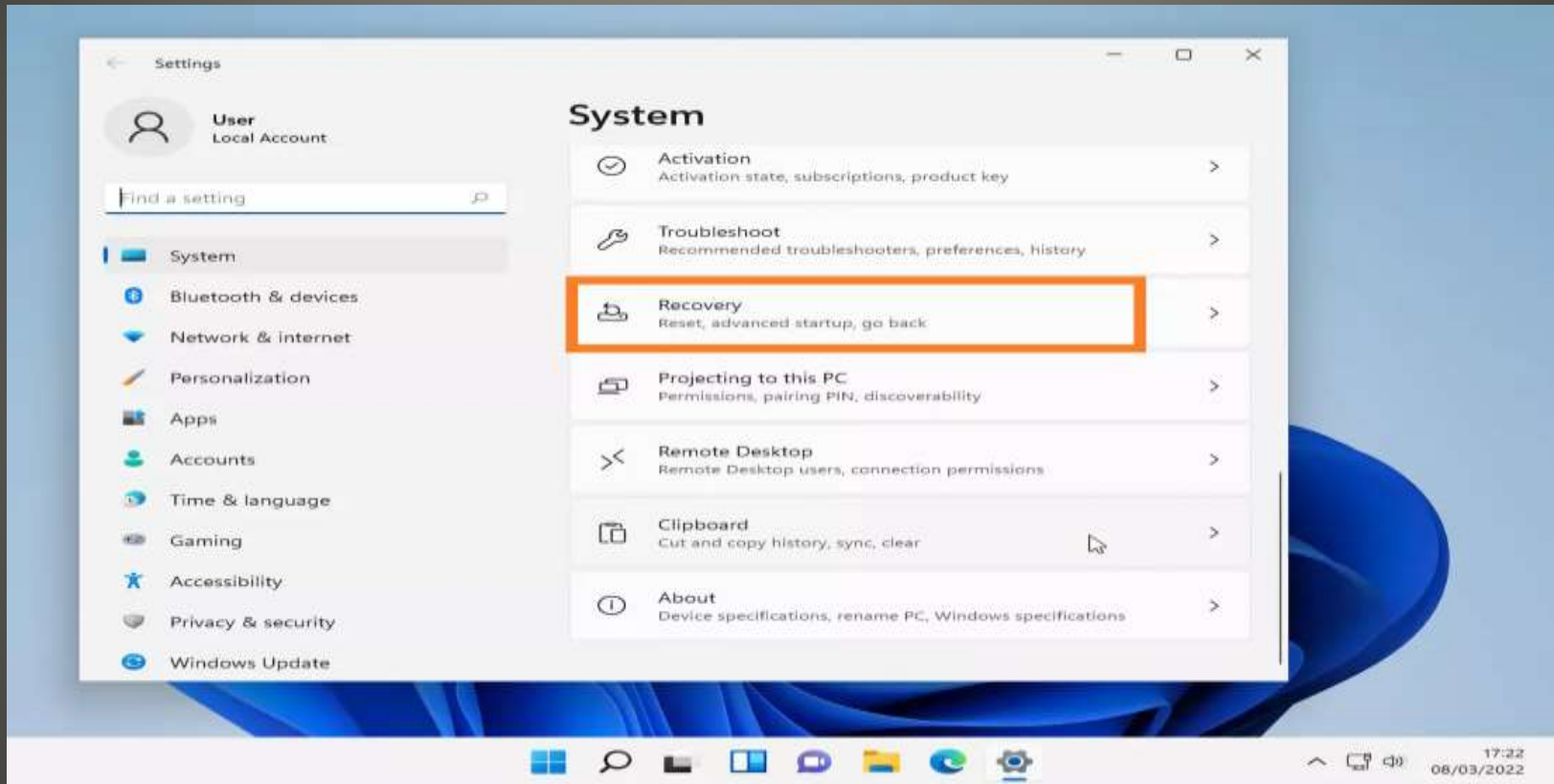
2



3














- Option 2 Windows Settings



Accessing BIOS

 **User**
Local Account

Find a setting 

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

System > Recovery

If you're having problems with your PC or want to reset it, these recovery options might help.



Fix problems without resetting your PC
Resetting can take a while — first, try resolving issues by running a troubleshooter



Recovery options



Reset this PC
Choose to keep or remove your personal files, then reinstall Windows

Reset PC



Advanced startup
Restart your device to change startup settings, including starting from a disc or USB drive

Restart now

 [Get help](#)

 [Give feedback](#)



- After either Option 1 or 2

Choose an option



Continue
Exit and continue to Windows 11



Turn off your PC



Use a device
Use a USB drive, network connection,
or Windows recovery DVD



Troubleshoot
Reset your PC or see advanced options

Accessing BIOS

Choose an option



Continue
Exit and continue to Windows 11



Turn off your PC



Use a device
Use a USB drive, network connection,
or Windows recovery DVD



Troubleshoot
Reset your PC or see advanced options

Accessing BIOS

← Advanced options



Startup Repair

Fix problems that keep Windows from loading



Uninstall Updates

Remove recently installed quality or feature updates from Windows



Startup Settings

Change Windows startup behavior



UEFI Firmware Settings

Change settings in your PC's UEFI firmware



Command Prompt

Use the Command Prompt for advanced troubleshooting



System Restore

Use a restore point recorded on your PC to restore Windows

See more recovery options

UEFI Firmware Settings

← UEFI Firmware Settings

Restart to change UEFI firmware settings

Restart

UEFI Restart

Boot Manager

Boot normally

EFI VMware Virtual SATA Hard Drive (0.0)

EFI VMware Virtual SATA CDROM Drive (1.0)

EFI Network

Enter setup

Reset the system

Shut down the system

Configure the firmware
boot environment and
options.

↑↓=Move Highlight

<Enter>=Select Entry

UEFI Restart YMMV

16:39 Wed 4 Mar, 2020

GAME BOOST



A-XMP



CPU Speed 3.90 GHz
DDR Speed 2666 MHz

CPU Temperature: 34°C
MotherBoard Temperature: 32°C

MB: MEG X570 ACE (MS-7C35)
CPU: AMD Ryzen 7 3800X 8-Core Processor
Memory Size: 16384MB
VCore: 1.444V
DDR Voltage: 1.220V
BIOS Ver: E7C35AMS.180
BIOS Build Date: 01/16/2020

Boot Priority



SETTINGS

Settings \ Advanced

HOT KEY | ↵

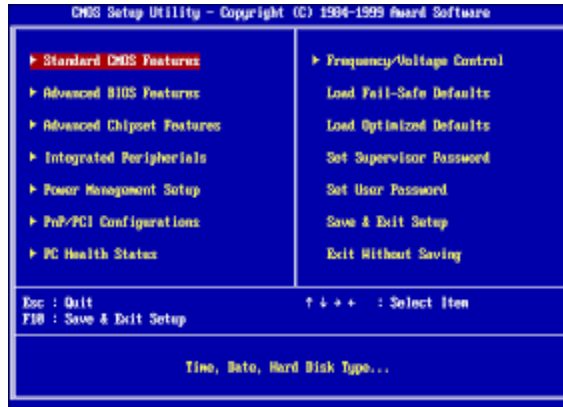
- > PCI Subsystem Settings
- > ACPI Settings
- > Integrated Peripherals
- > USB Configuration
- > Power Management Setup
- > Windows OS Configuration
- > Wake Up Event Setup
- > Secure Erase+
- > AMD Overclocking

Overclocking settings
OC

HELP

INFO

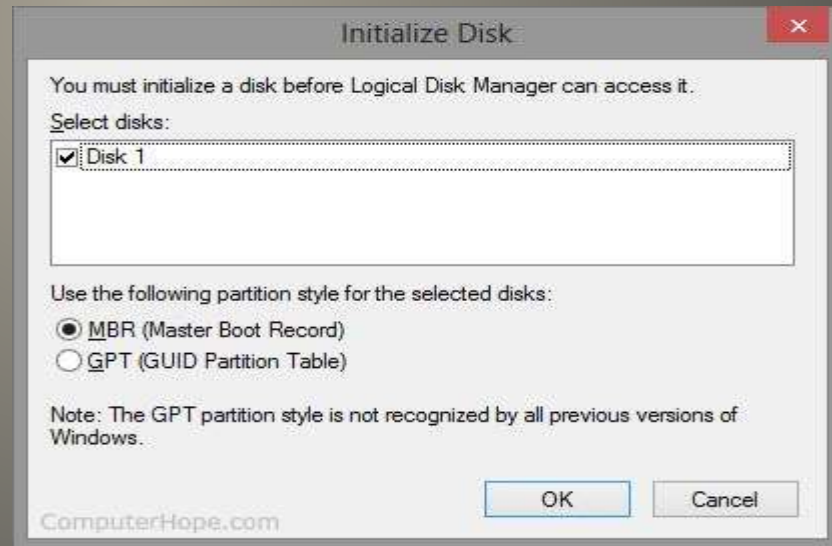
SSD performance may getting lower over time as with any storage medium due to data processing. Activate Secure Erase+ to recover SSD default performance through complete written. Be aware of that data on SSD will be lost after Secure Erase+ execution.



- One Beep – good
- No or multiple beeps – vendor documentation
- BIOS – nonvolatile
- CMOS Volatile user custom settings
CMOS battery

BIOS Beep Codes

- Colors, Animations, Mouse, Larger drives
- Secure Boot
- LARGE disk drives
- MBR Master Boot Record < 2TB
- GUID Partition Table (GPT)
UEFI standard



UEFI

- Pre-Release
- Developer workstation in the Azure cloud
- Windows Subsystem for Linux
- Windows Subsystem for Android
- Sizing 4 vCPUs & 16 GB
16 vCPUs & 128GB
- Windows 365 Cloud PC \$20 -> \$163 per month

Microsoft Dev Box

- XPS viewer

File format for digital documents

Disabled by default

Start > optional features > View features

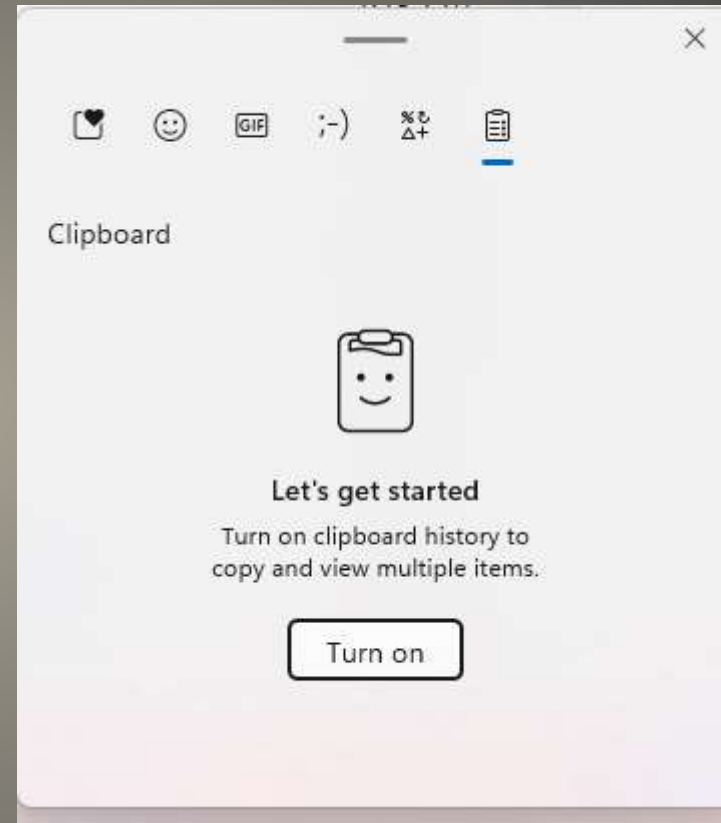
Select XPS viewer > Install

-or-

Search XPS Viewer

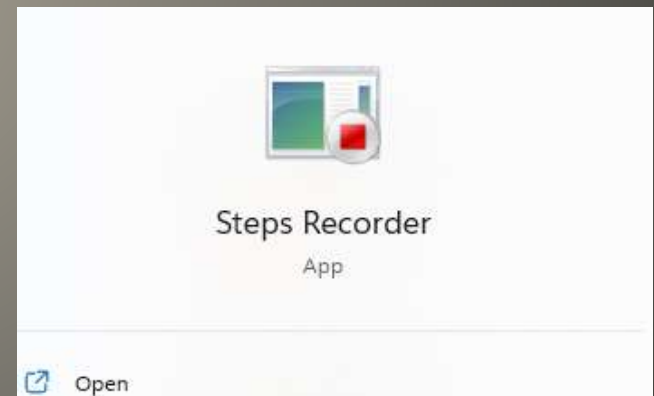
Windows Features

- Clipboard Manager
Not on by default
Windows + V



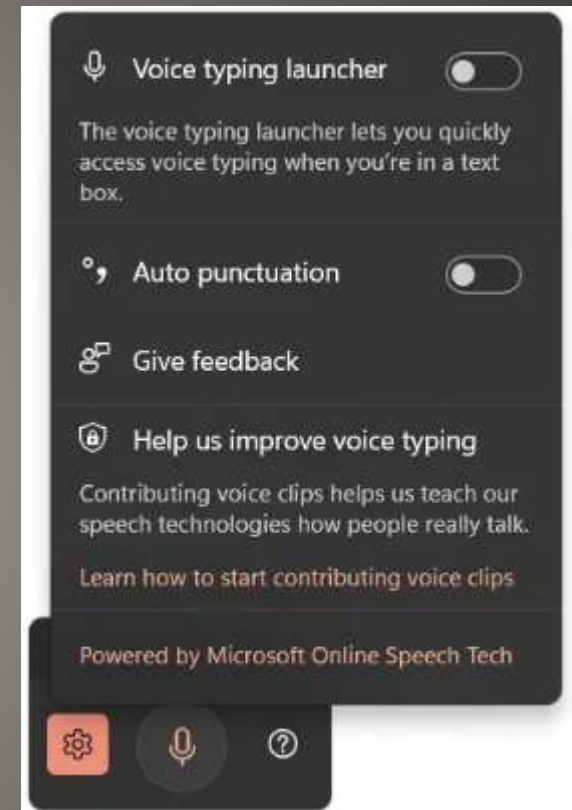
Windows Features

- File History
Auto backup Files External drive
Settings -> Control Panel
Search > Control Panel > File History
- Steps Recorder
Records actions to slide show
Search > Step Recorder



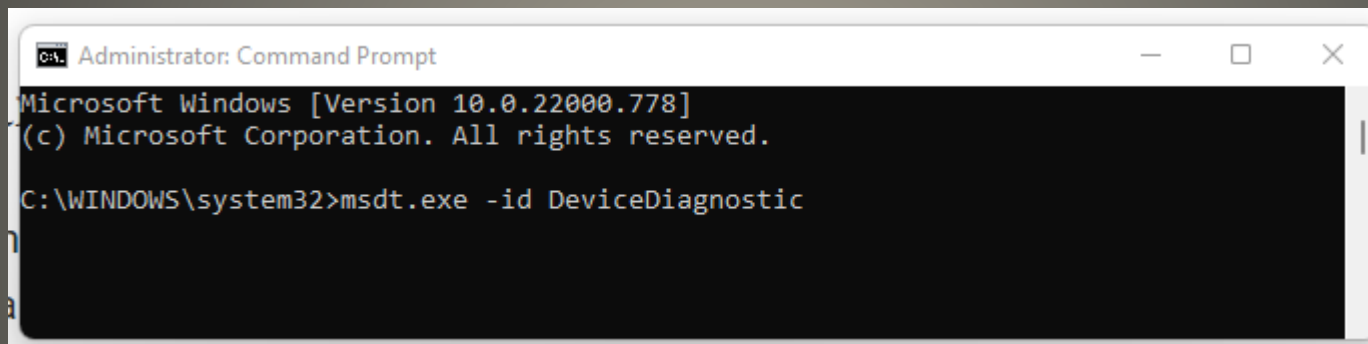
Windows Features

- Voice Typing
Windows 11 Microphone
Win + H



Windows Features

- Troubleshooter
Removed from settings Windows 11
CMD `msdt.exe -id DeviceDiagnostic`




```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.22000.778]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>msdt.exe -id DeviceDiagnostic
```

Windows Features



 Hardware and Devices

Troubleshoot and help prevent computer problems



Hardware and Devices

Find and fix problems with devices and hardware.

[Advanced](#)

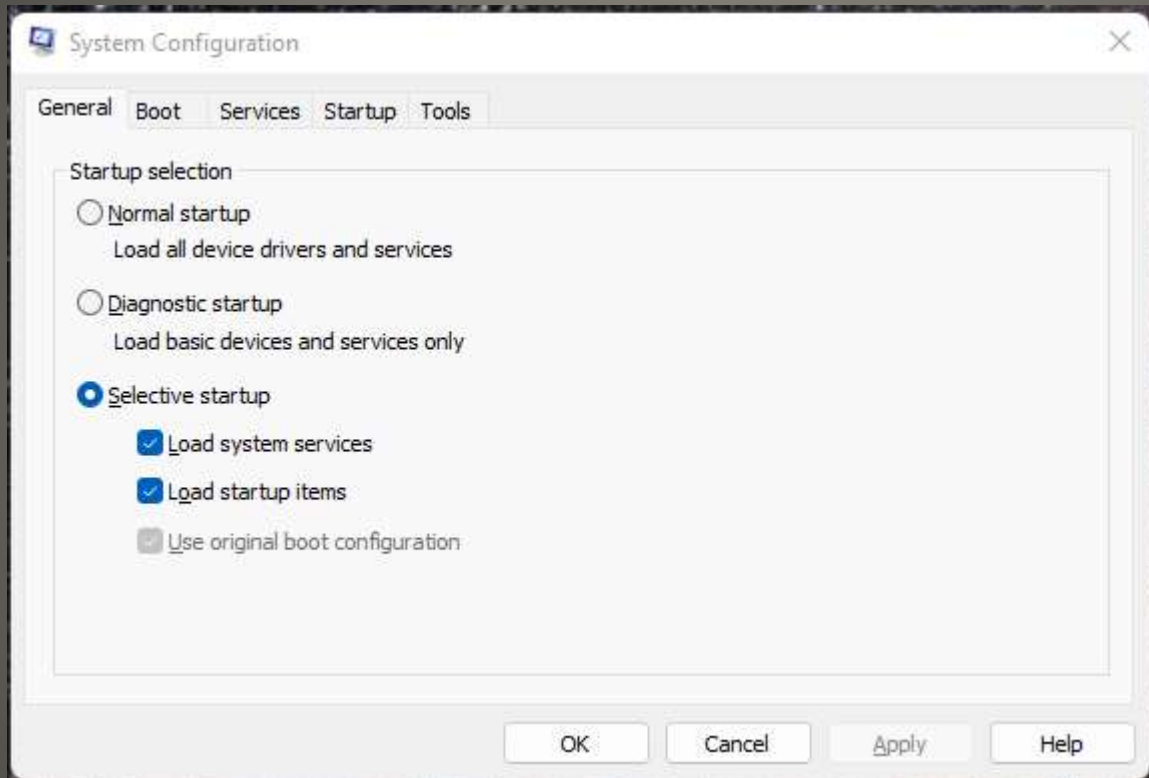
Publisher: Microsoft Corporation

[Privacy statement](#)

[Next](#)

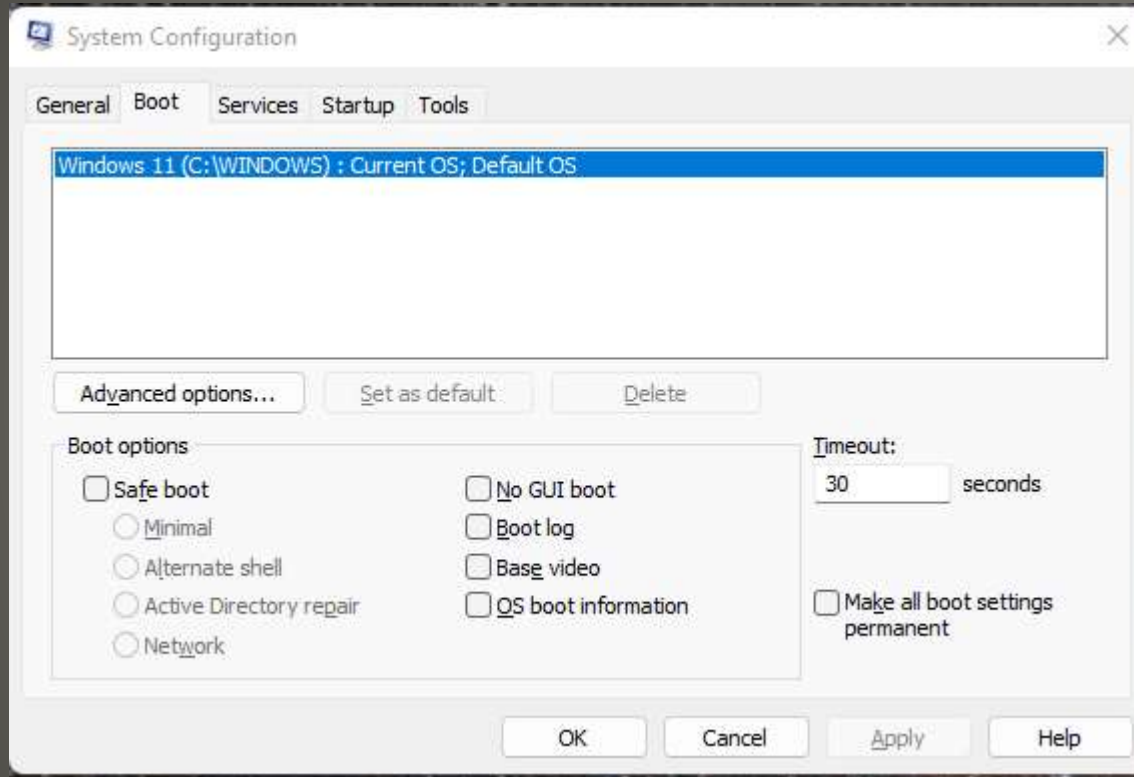
Cancel

- MSConfig



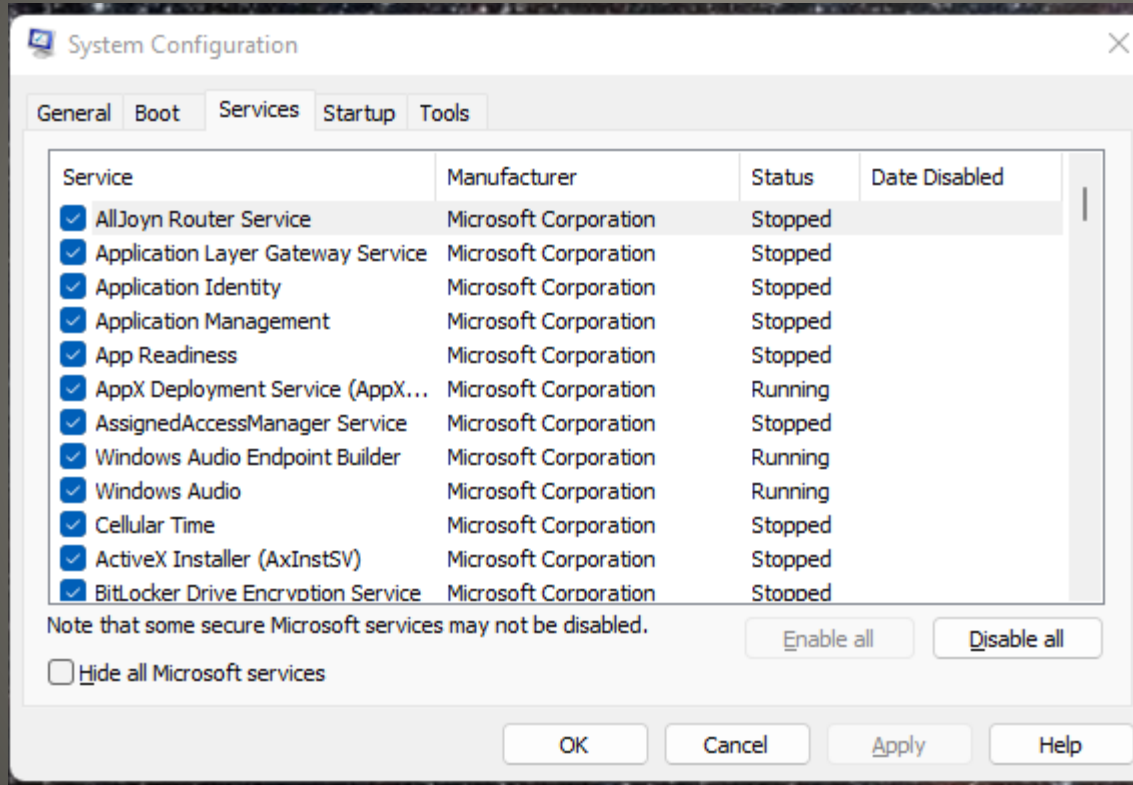
Windows Features

- MSConfig



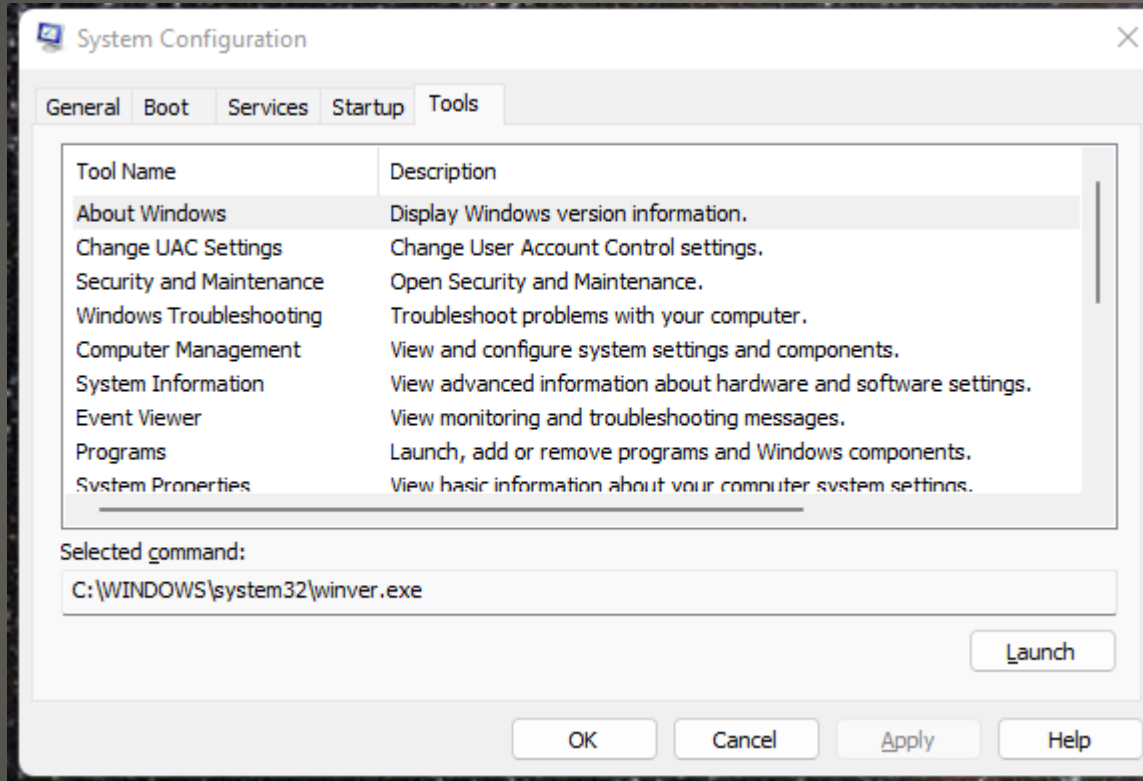
Windows Features

- MSConfig



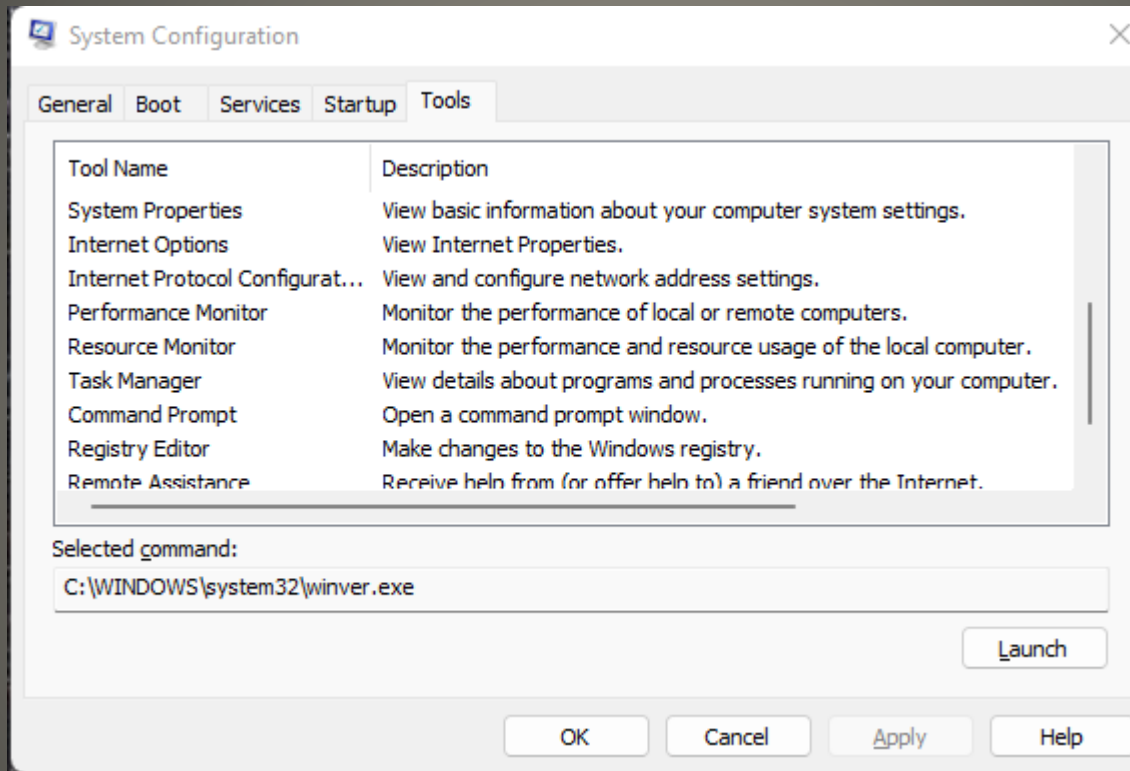
Windows Features

- MSConfig



Windows Features

- MSConfig



Windows Features

• winget Windows Package Manager

```
Administrator: Command Prompt
Copyright (c) Microsoft Corporation. All rights reserved.

The winget command line utility enables installing applications and other packages from the command line.

Usage: winget [<command>] [<options>]

The following commands are available:
install    Installs the given package
show       Shows information about a package
source     Manage sources of packages
search     Find and show basic info of packages
list       Display installed packages
upgrade    Shows and performs available upgrades
uninstall  Uninstalls the given package
hash       Helper to hash installer files
validate   Validates a manifest file
settings   Open settings or set administrator settings
features   Shows the status of experimental features
export     Exports a list of the installed packages
import     Installs all the packages in a file

For more details on a specific command, pass it the help argument. [-?]

The following options are available:
-v,--version  Display the version of the tool
--info        Display general info of the tool

More help can be found at: https://aka.ms/winget-command-help

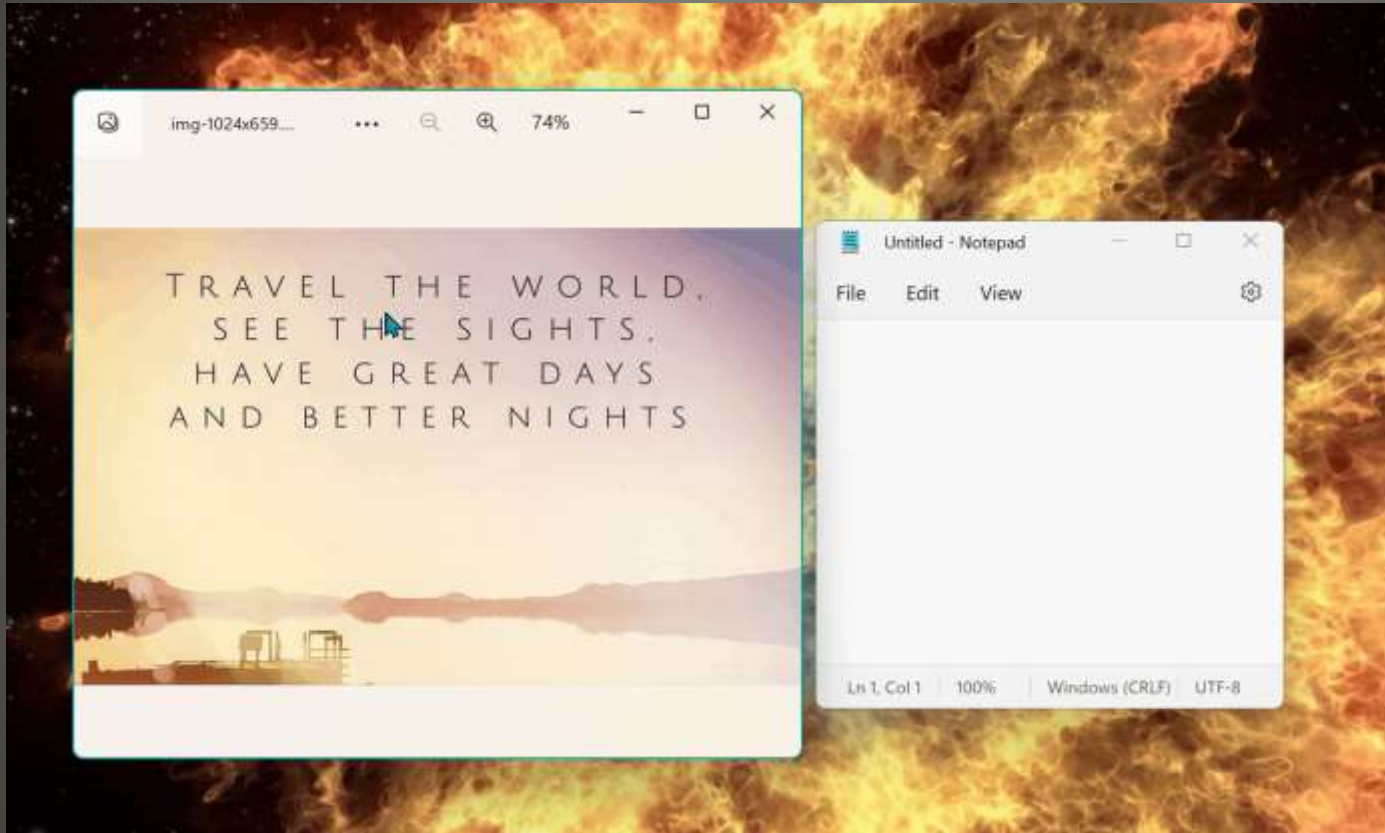
C:\WINDOWS\system32>
```

Windows Features

- Windows Media Player
- Taskbar Hotkeys
Win + <number along taskbar>
- Old Volume Mixer
Win + X Run sndvol.exe

Windows Features

- PowerOCR



Potential future PowerToys

- Transferrable? OEM Discount Maby
- Windows versions prior to 10
- Upgrade “trick”
- ONLY Authorized vendors Microsoft & Amazon
Use their sites to view license key

[How to Transfer a Windows 10 or 11 License to Another PC | Tom's Hardware \(tomshardware.com\)](https://www.tomshardware.com/how-to/transfer-windows-license)

Transfer Microsoft Windows

- Moments
“feature” updates

Windows Update future

- XP, Vista unusable post trial period
- Users got cracked license keys
- Usable not *Activated*
 - No Security Updates
 - Delay for new features
 - Screen watermark
 - Reminders
 - Less customization settings
 - Upgrades may not be free
 - Legal recourse

Un Activated use

- Screen Reader
- Many other options
- If you need screen reader otherwise
Control + Windows + Enter

Welcome to Narrator

This is Narrator Home, where you can get help, access your settings, and learn about new features. Narrator is a screen reader that describes aloud what's on your screen, so you can use that information to navigate your device. To start or stop Narrator, press the Windows logo key + Ctrl + Enter. Explore the sections below to get started.



QuickStart

Learn the basics of Narrator.



Narrator guide

View the complete Narrator guide online.



What's new

Get an overview of new and updated features.



Settings

Customize Narrator. Press Windows logo key + Ctrl + N to access settings anytime.



Feedback

Help improve Narrator. Press Narrator key + Alt + F to give feedback anytime.

Narrator

- Settings > Accessibility > Narrator

Accessibility > Narrator

Use Narrator



Narrator

Off



Keyboard shortcut for Narrator

Press the Windows logo key + Ctrl + Enter to turn Narrator on and off

On



Narrator Home

Get help, access settings, and learn about new Narrator features



Complete guide to Narrator



Narrator's voice



Voice

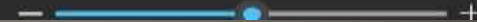
Microsoft David - English (United States)



Add voices



Speed



Narrator

- Malware deployment method
- .EXE .DLL .SYS
- File path
- Hash match
- Dropped from specific executables
i.e.. Office modules via macros

**Sysmon ability to block malicious
.exe from creation**

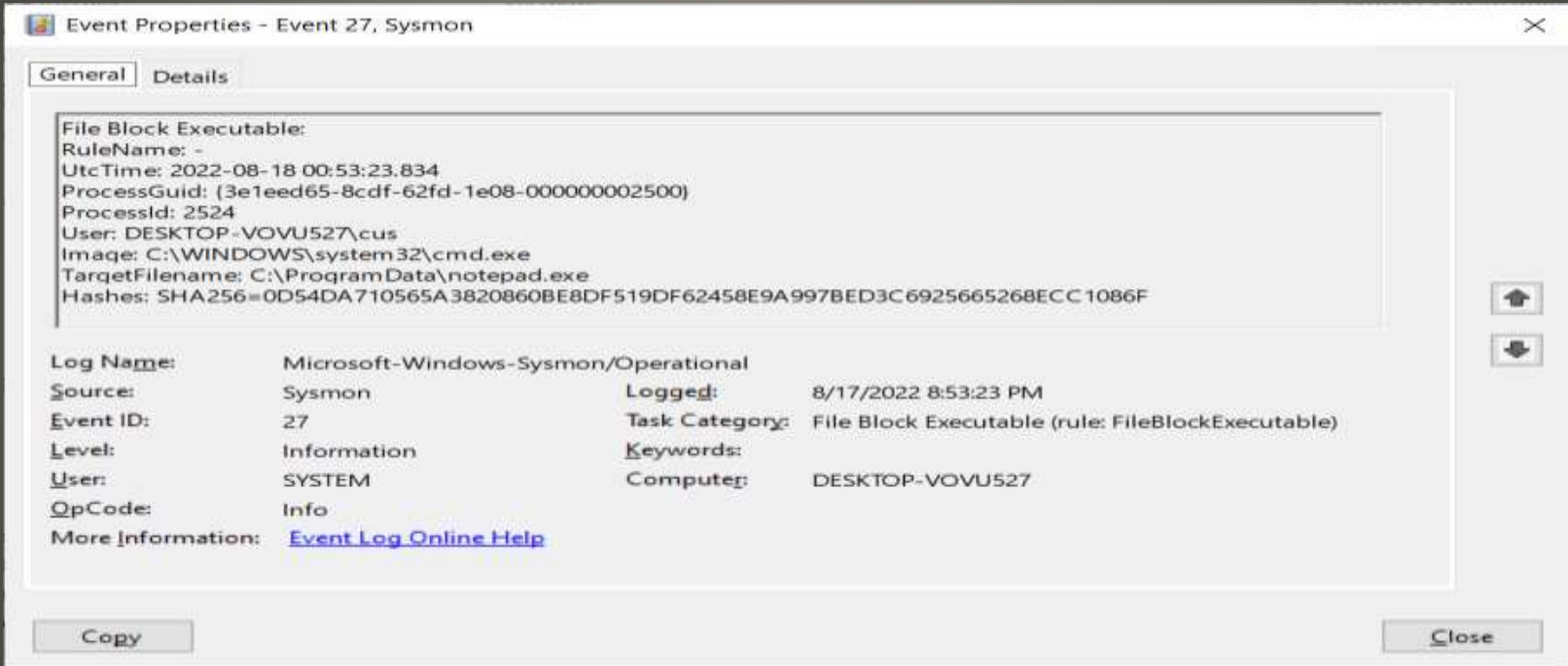
- Microsoft Store
- Microsoft Sysinternals
sysmon -s
- Sysmon schema

Sysmon?

```
<Sysmon schemaversion="4.82">
  <EventFiltering>
    <RuleGroup name="" groupRelation="or">
      <FileBlockExecutable onmatch="include">
        <Image name="technique_id=T1105,technique_name=Ingress Tool
Transfer" condition="image">excel.exe</Image>
        <Image name="technique_id=T1105,technique_name=Ingress Tool
Transfer" condition="image">winword.exe</Image>
        <Image name="technique_id=T1105,technique_name=Ingress Tool
Transfer" condition="image">powerpnt.exe</Image>
        <Image name="technique_id=T1105,technique_name=Ingress Tool
Transfer" condition="image">outlook.exe</Image>
        <Image name="technique_id=T1105,technique_name=Ingress Tool
Transfer" condition="image">msaccess.exe</Image>
        <Image name="technique_id=T1105,technique_name=Ingress Tool
Transfer" condition="image">mspub.exe</Image>
      </FileBlockExecutable>
    </RuleGroup>
  </EventFiltering>
</Sysmon>
```

**Example
block Office created executables**

- `sysmon -i msoffice-fileblock.xml`



The screenshot shows the 'Event Properties' window for 'Event 27, Sysmon'. The 'General' tab is selected, displaying the following details:

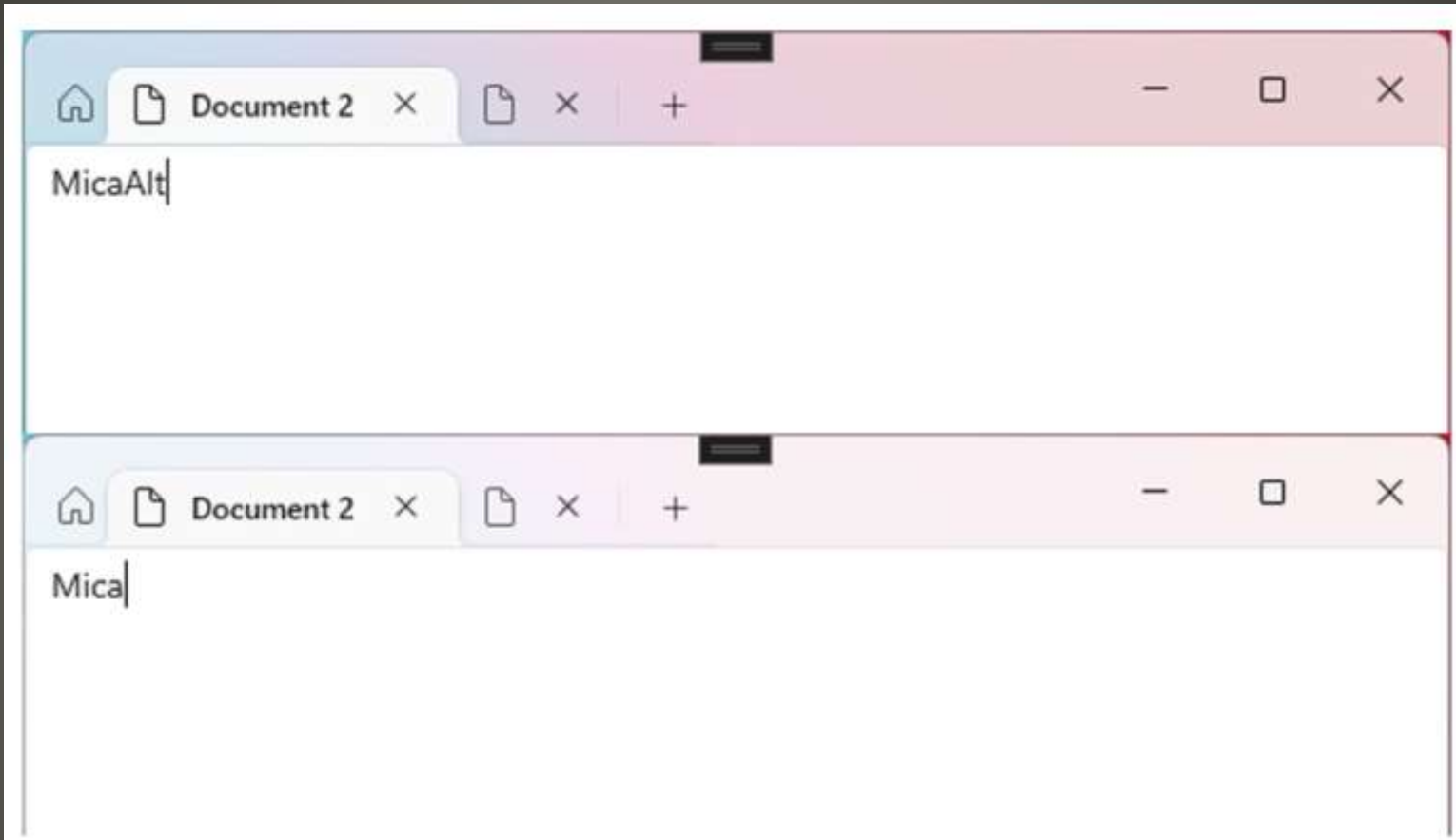
File Block Executable:
RuleName: -
UtcTime: 2022-08-18 00:53:23.834
ProcessGuid: {3e1eed65-8cdf-62fd-1e08-000000002500}
ProcessId: 2524
User: DESKTOP-VOVU527\cus
Image: C:\WINDOWS\system32\cmd.exe
TargetFilename: C:\ProgramData\notepad.exe
Hashes: SHA256=0D54DA710565A3820860BE8DF519DF62458E9A997BED3C6925665268ECC1086F

Log Name: Microsoft-Windows-Sysmon/Operational
Source: Sysmon
Event ID: 27
Level: Information
User: SYSTEM
OpCode: Info
More Information: [Event Log Online Help](#)

Logged: 8/17/2022 8:53:23 PM
Task Category: File Block Executable (rule: FileBlockExecutable)
Keywords:
Computer: DESKTOP-VOVU527

Buttons: Copy, Close

sysmon



New Windows 11 Visual Effect

- Screen Ruler measure pixels on your screen
- Quick Accent write letters with accents
- Text Extractor copy text from region with OCR

Three more tools to PowerToys

- General
- Always On Top
- Awake
- Color Picker
- FancyZones
- File Explorer add-ons
- Image Resizer
- Keyboard Manager
- Mouse utilities
- PowerRename
- PowerToys Run
- Quick Accent
- Screen Ruler
- Shortcut Guide
- Text Extractor

What's new

[See more detailed release notes on GitHub](#)

Release v0.62.0

In the [v0.62 release cycle](#), we focused on releasing three new PowerToys.

Highlights

- New utility: Screen Ruler is a quick and easy way to measure pixels on your screen.
- New utility: Quick Accent is an easy way to write letters with accents. Thanks [@damienleroy!](#)
- New utility: Text Extractor works like Snipping Tool, but copies the text out of the selected region using OCR and puts it on the clipboard. Thanks [@TheJoeFin!](#)
- PowerToy Run ships with a new Plugin letting you search in past query results. Thanks [@jefflord!](#)

Known issues

- The Text Extractor utility [fails to recognize text in some cases on ARM64 devices running Windows 10](#).
- After installing PowerToys, [the new Windows 11 context menu entries for PowerRename and Image Resizer might not appear before a system restart](#).
- There are reports of users who are [unable to open the Settings window](#). This is being caused by incompatibilities with some applications (RTSS RivaTuner Statistics Server and MSI AfterBurner are known examples of this). If you're affected by this, please check the linked issue to verify if any of the presented solutions works for you.

General

- Added a new utility: Screen Ruler.
- Added a new utility: Quick Accent. Thanks [@damienleroy!](#)
- Added a new utility: Text Extractor. Thanks [@TheJoeFin!](#)
- Upgraded the Windows App SDK runtimes to 1.1.4.

Administrator: Command Prompt

```
C:\WINDOWS\system32>powercfg /a
```

```
The following sleep states are available on this system:
```

```
Standby (S0 Low Power Idle) Network Connected  
Hibernate  
Fast Startup
```

```
The following sleep states are not available on this system:
```

```
Standby (S1)  
The system firmware does not support this standby state.  
This standby state is disabled when S0 low power idle is supported.
```

```
Standby (S2)  
The system firmware does not support this standby state.  
This standby state is disabled when S0 low power idle is supported.
```

```
Standby (S3)  
The system firmware does not support this standby state.  
This standby state is disabled when S0 low power idle is supported.
```

```
Hybrid Sleep  
Standby (S3) is not available.
```

```
C:\WINDOWS\system32>
```

Modern Standby

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

