

Sun City Computer Club

Windows SIG

August 10, 2021

**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
- Cyber OK?
- In person meetings

Windows Update



Updates available

Last checked: Today, 12:01 PM

Windows Malicious Software Removal Tool x64 - v5.92 (KB890830)

Status: Installing - 0%

2021-08 Cumulative Update for Windows 10 Version 21H1 for x64-based Systems (KB5005033)

Status: Downloading - 0%

✓ Quality Updates (24)

[2021-08 Cumulative Update for Windows 10 Version 21H1 for x64-based Systems \(KB5005033\)](#)

Successfully installed on 8/10/2021

Microsoft Patch Tuesday



[August 10, 2021—KB5005033 \(OS Builds 19041.1165, 19042.1165, and 19043.1165\) \(microsoft.com\)](#)

Microsoft Patch Tuesday

- TCP/IP Remote Code Execution Vulnerability
CVE-2021-26424
Hyper-V triggered by IPv6 ping
- Windows Update Medic Service
CVE-2021-36984
No user interaction, low attack complexity
Actively being exploited
- Print Spooler
CVE-2021-36936
Patch to all versions, even Windows 7
- Windows LSA
CVE-2021-36942
Remote exploit, no user interaction, NTLM authenticate

Microsoft Patch Tuesday

Control if audio and video play automatically on sites

All media will play automatically. Refresh the page to see changes to this setting.

Allow ▼

Control if audio and video play automatically on sites

Media will play depending on how you've visited the page and whether you interacted with media in the past. Refresh the page to see changes to this setting.

Limit ▼

Edge AutoPlay

```
C:\Windows\system32>icacls c:\Windows\system32\config\SAM
c:\Windows\system32\config\SAM BUILTIN\Administrators:(I)(F)
                                NT AUTHORITY\SYSTEM:(I)(F)
                                BUILTIN\Users:(I)(RX)
                                APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(I)(RX)
                                APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES:(I)(RX)
```

Successfully processed 1 files; Failed processing 0 files

```
C:\Windows\system32>icacls c:\Windows\system32\config\SYSTEM
c:\Windows\system32\config\SYSTEM BUILTIN\Administrators:(I)(F)
                                   NT AUTHORITY\SYSTEM:(I)(F)
                                   BUILTIN\Users:(I)(RX)
                                   APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(I)(RX)
                                   APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES:(I)(RX)
```

Successfully processed 1 files; Failed processing 0 files

Administrator: Windows PowerShell

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

Try the new cross-platform PowerShell https://aka.ms/pscore6

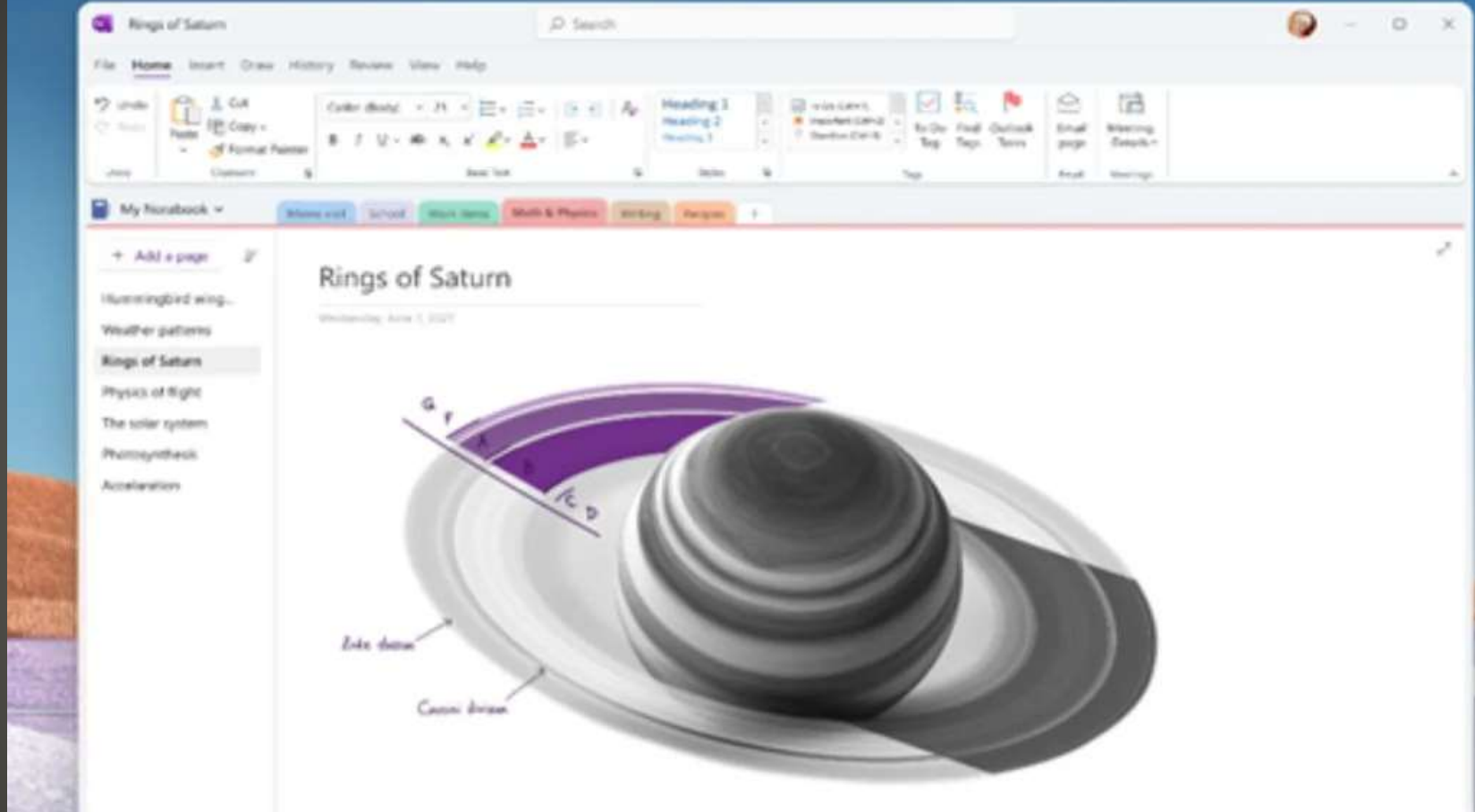
PS C:\WINDOWS\system32> icacls c:\Windows\system32\config\SAM
c:\Windows\system32\config\SAM NT AUTHORITY\SYSTEM:(I)(F)
                                BUILTIN\Administrators:(I)(F)

Successfully processed 1 files; Failed processing 0 files
PS C:\WINDOWS\system32> icacls c:\Windows\system32\config\SYSTEM
c:\Windows\system32\config\SYSTEM NT AUTHORITY\SYSTEM:(I)(F)
                                   BUILTIN\Administrators:(I)(F)

Successfully processed 1 files; Failed processing 0 files
PS C:\WINDOWS\system32>
```

Yeah, BUT Windows 11

- Layered Group Policy feature
 - Types of devices allowed
- Parallels Desktop 17
 - Windows 11 on Intel and M1 based MACs
- Oeclassic
 - Outlook Express Windows live Mail replacement
 - Recent certificate registration based in Croatia
 - Free version, then credit card
- Outlook client Outlook WEB Outlook extension
 - Active development by Microsoft



OneNote Desktop – Kill OneNote on Windows 10

- NO Please NO

Windows 11 get yours here

Manage Patches

AvailableHidden

| | NAME | PRODUCT | IMPORTANCE |
|-------------------------------------|--|----------------------------|------------|
| <input checked="" type="checkbox"/> | Oracle VirtualBox 6.1.20 for Windows (See Notes) | VirtualBox | Critical |
| <input checked="" type="checkbox"/> | PuTTY 0.75 for Windows (See Notes) | PuTTY | Critical |
| <input checked="" type="checkbox"/> | Wireshark 3.4.6 for Windows (See Notes) | Wireshark | Critical |

Install

Vipre

✓ Other Updates (35)

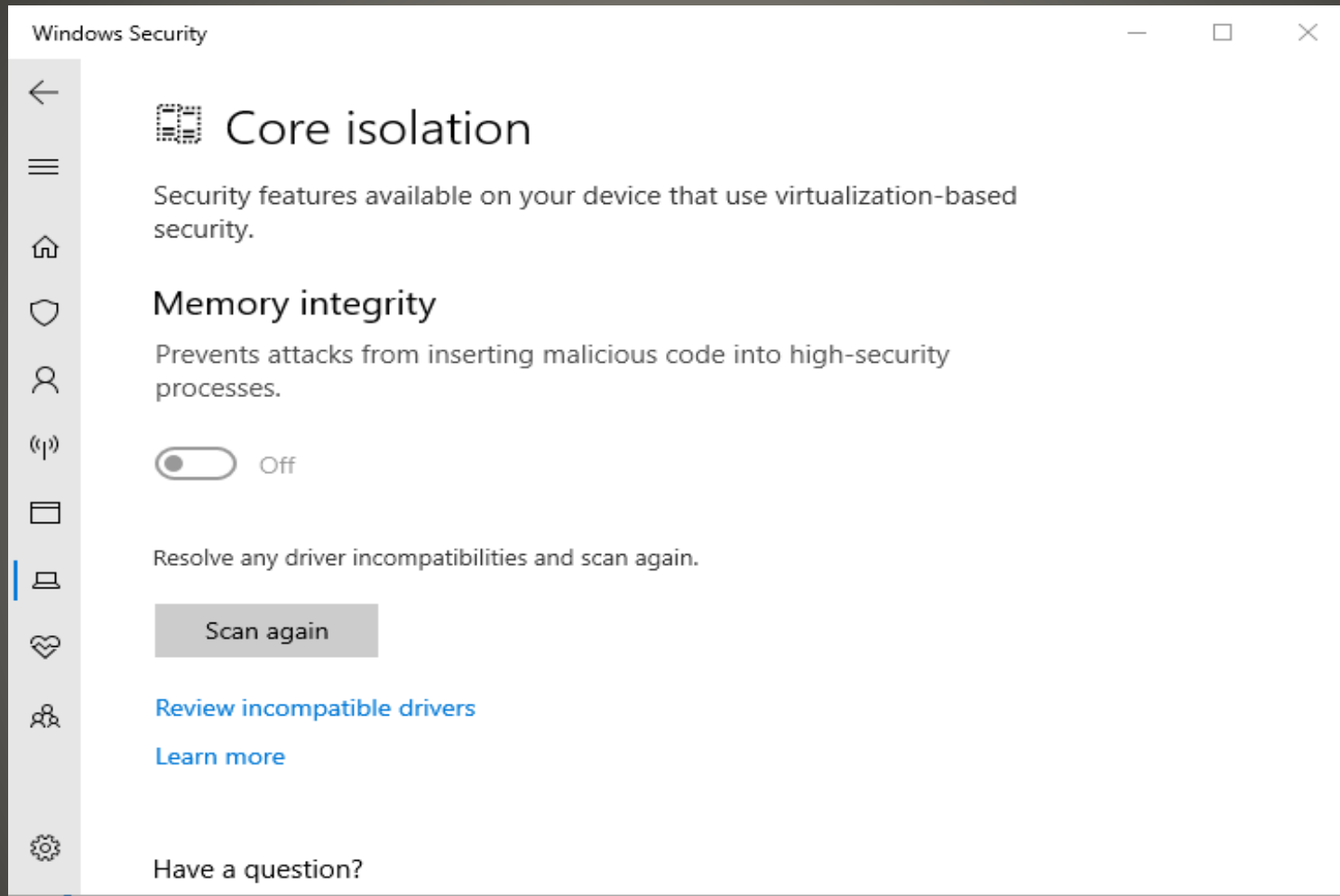
2021-07 Cumulative Update Preview for Windows 10 Version 21H1 for x64-based Systems (KB5004296)

Successfully installed on 7/29/2021

2021-07 Cumulative Update Preview for .NET Framework 3.5 and 4.8 for Windows 10 Version 21H1 for x64 (KB5004331)

Successfully installed on 7/29/2021

Windows Update



Core Isolation – Memory Integrity



Incompatible drivers

Resolving incompatibilities with these drivers will enable you to turn on Memory integrity.

[Learn how to resolve problems with incompatible drivers](#)

usb2ser.sys
MediaTek Inc.

Have a question?

[Get help](#)

Help improve Windows Security

[Give us feedback](#)

Why do incompatible drivers prevent using Memory integrity?

Security, Windows 10

Turning on the Memory integrity setting would block these incompatible drivers from loading. Because blocking these drivers might cause unwanted or unexpected behaviors, the Memory integrity setting is turned off to allow these drivers to load.

If you want to restore the Memory integrity setting, you can try to resolve a driver incompatibility by seeing if an updated and compatible driver is available through Windows Update or from the driver manufacturer. Microsoft does not recommend that you delete drivers to attempt to restore this setting.

- Recent research has revealed that Microsoft Windows 10 and 11 versions may have left or changed permissions on the SYSTEM and SAM hives in the Windows registry such that any local user can access the information stored in these registry hives. The SAM hive contains hashes of users on that windows system! Including the Administrator account(s).
- The discovery is hitting security news sites today (July 20, 2021) so attackers are or will soon be aware.
- The above commands will indicate if your versions of Windows has the misconfiguration. Most users are reporting the problem has existed since Windows 10 version 1809.
- While Windows is running these hives are locked.
- BUT Volume Shadow Copy has read these hives and abusers CAN read those volume copies.
- Methods to read the contents of these hives and obtain hashed passwords and other security configuration settings involve some knowledge that attackers have.
- The hive permissions, the still unpatched (third time) Print Spooler vulnerability kinda makes a bad period for Microsoft.

Summer of SAM

- Disable Shadow Volume copies?

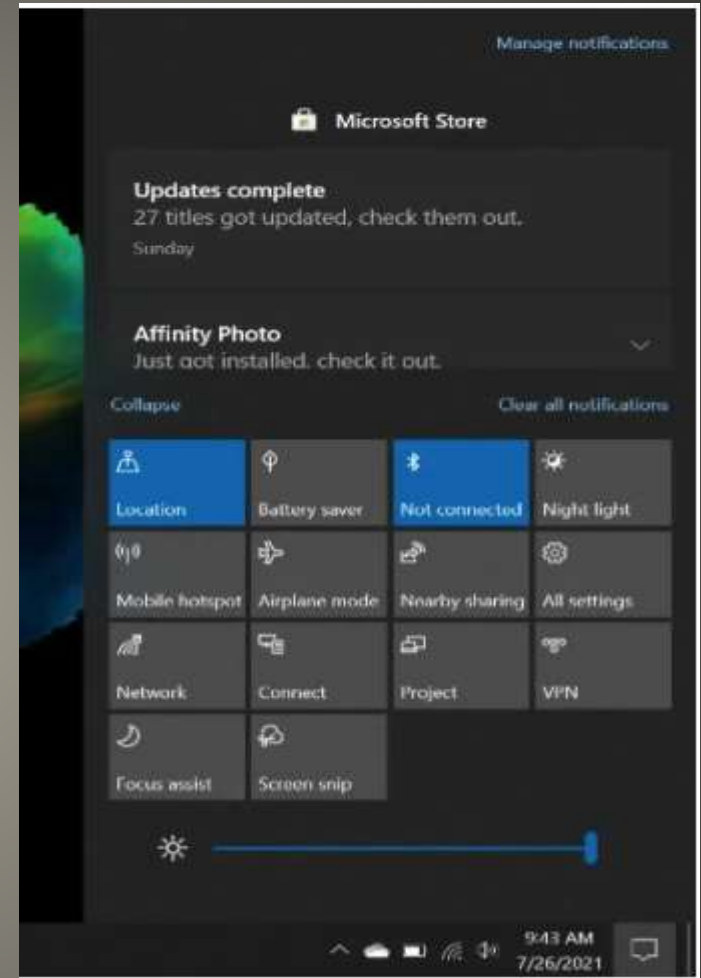
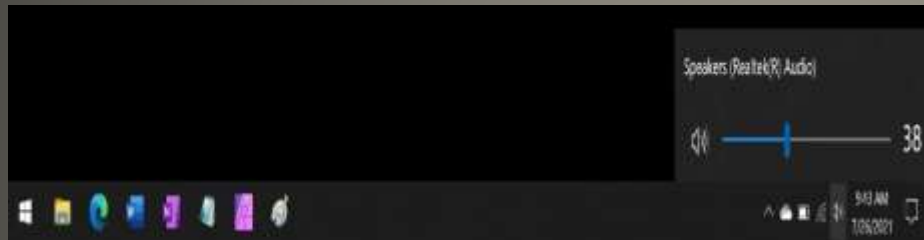
Summer of SAM workaround ??

- Internet Explorer – finally
- Timeline
- Live Tiles -> Widgets
- Start Menu Groups
- Quick Status Lock screen feature
- Taskbar locked to bottom of screen
- Tablet Mode
- Cortana
- Windows S Mode
- Skype -> Teams
- Task Manager via right click on Task Bar
 - CTRL + Shift + Esc
 - CTRL + ALT + Delete
 - Search

Missing from Windows 11

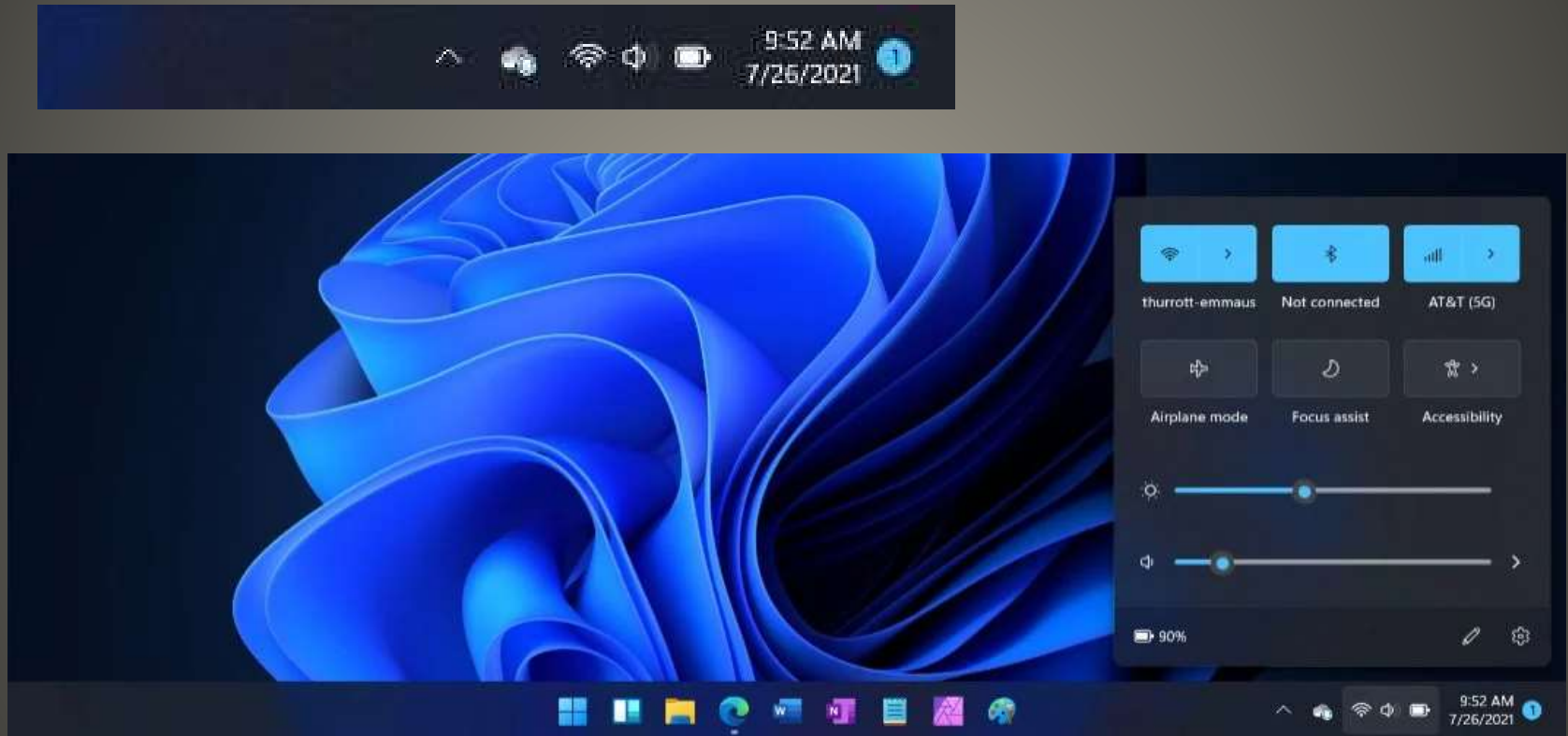
| Feature | Windows 11 Home | Windows 11 Pro |
|-------------------------------------|-----------------|----------------|
| Set up with a local account | No | Yes |
| Join Active Directory/Azure AD | No | Yes |
| Hyper-V | No | Yes |
| Windows Sandbox | No | Yes |
| Microsoft Remote Desktop | Client only | Yes |
| Windows Hello | Yes | Yes |
| Device encryption | Yes | Yes |
| Firewall and network protection | Yes | Yes |
| Internet protection | Yes | Yes |
| Parental controls/protection | Yes | Yes |
| Secure Boot | Yes | Yes |
| Windows Defender Antivirus | Yes | Yes |
| BitLocker device encryption | No | Yes |
| Windows Information Protection | No | Yes |
| Mobile device management (MDM) | No | Yes |
| Group Policy | No | Yes |
| Enterprise State Roaming with Azure | No | Yes |
| Assigned Access | No | Yes |
| Dynamic Provisioning | No | Yes |
| Windows Update for Business | No | Yes |
| Kiosk mode | No | Yes |
| Maximum RAM | 128GB | 2TB |
| Maximum no. of CPUs | 1 | 2 |
| Maximum no. of CPU cores | 64 | 128 |

- Windows 10

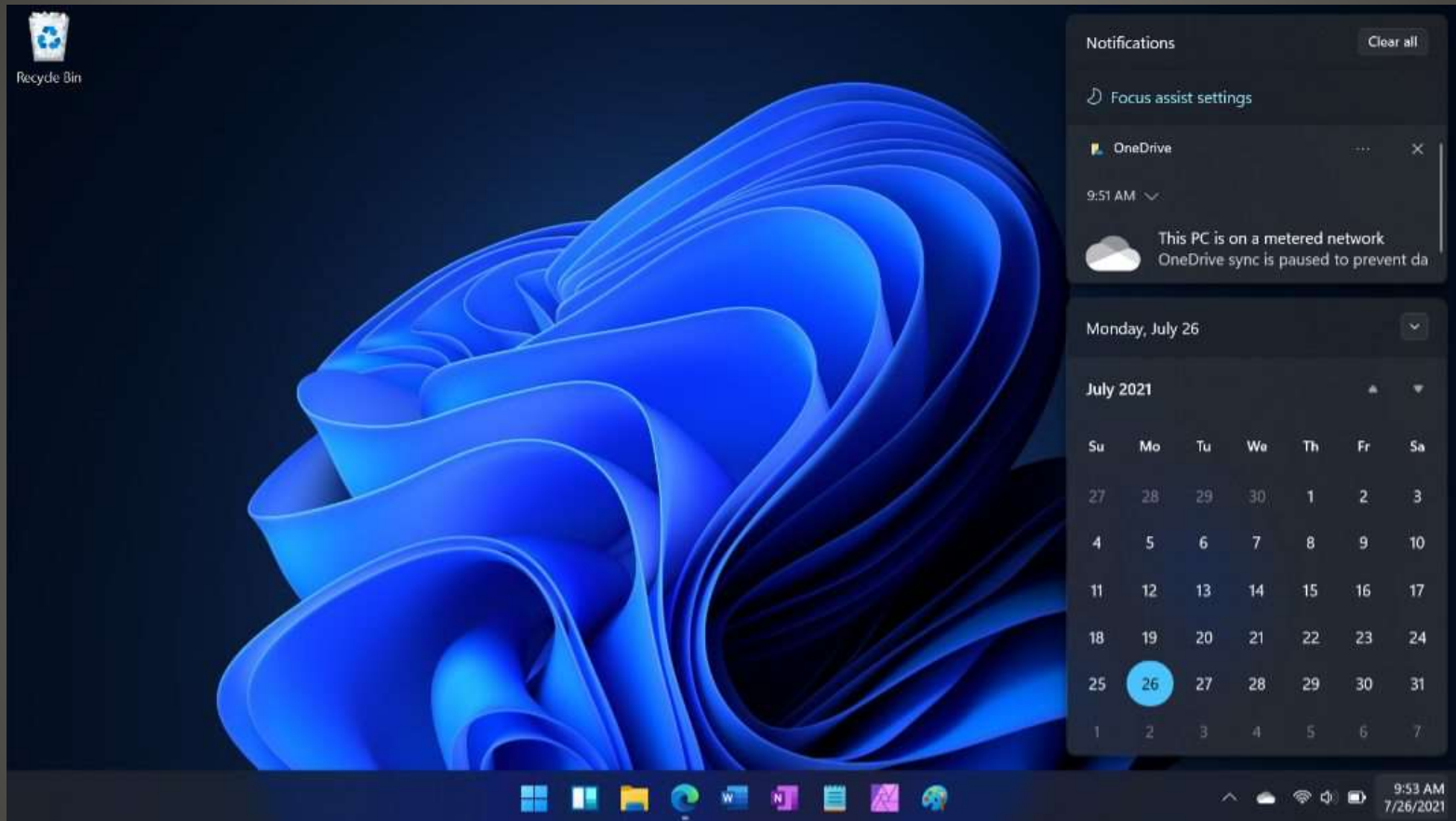


Quick Settings & Notifications

- Windows 11



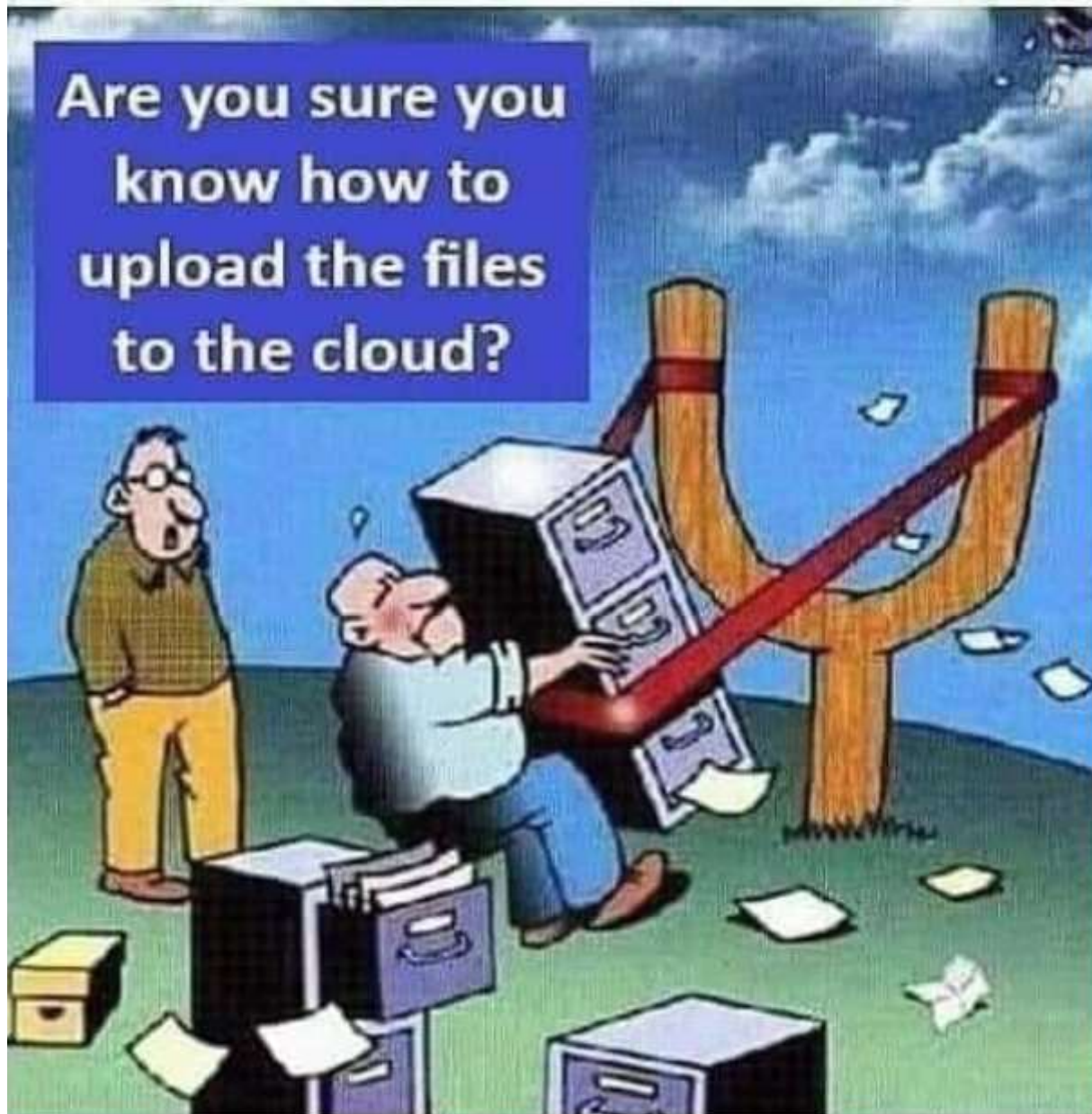
Quick Settings & Notifications



Quick Settings & Notifications

- Office 365 virtual refresh - toned down?
- Windows 365 \$31/mo.
- Windows 10 21H2
- Microsoft Store Business and Education

**Are you sure you
know how to
upload the files
to the cloud?**



- macOS

Version 16.51 (21071101)

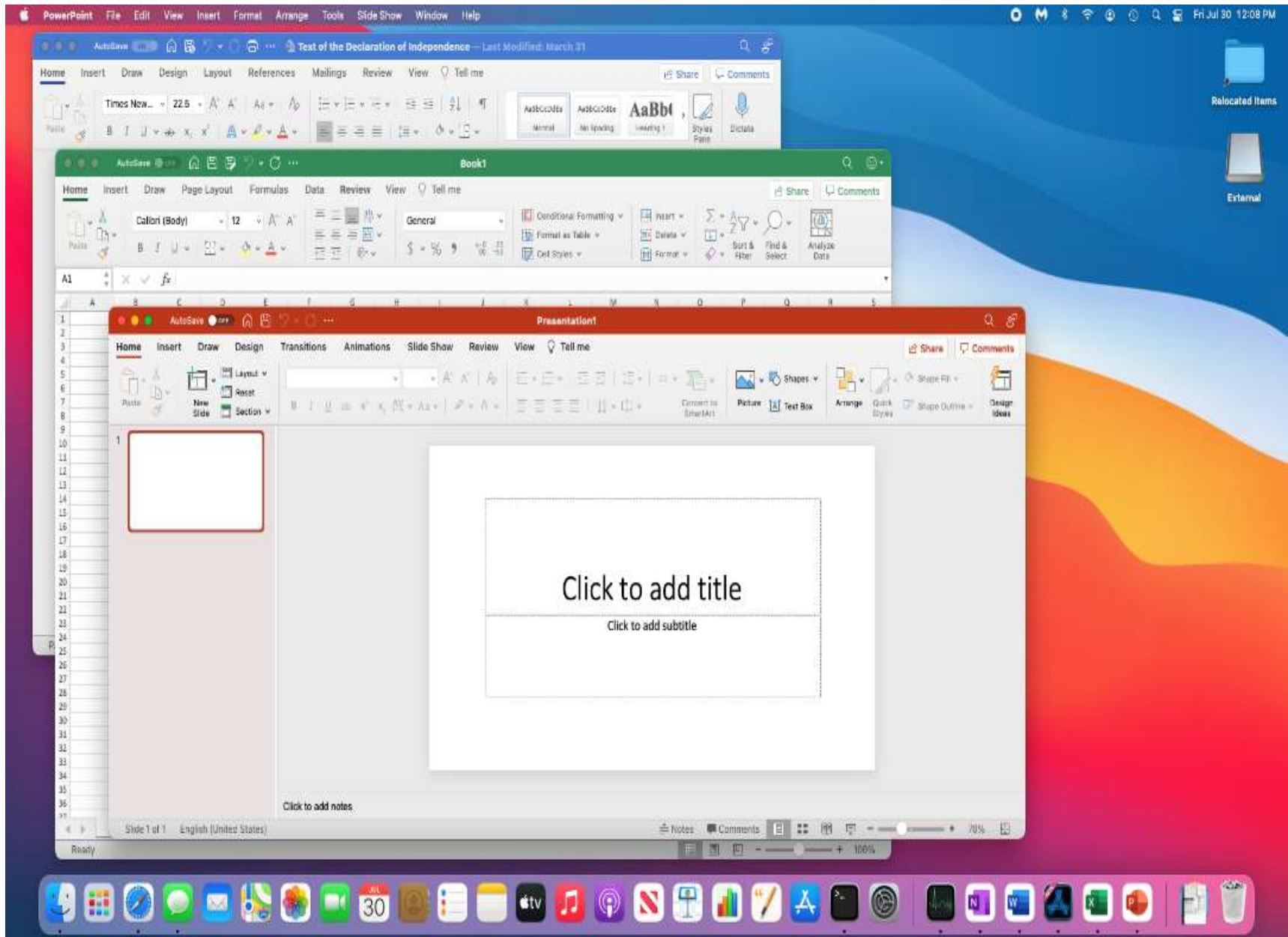
- Windows 11 Office Preview

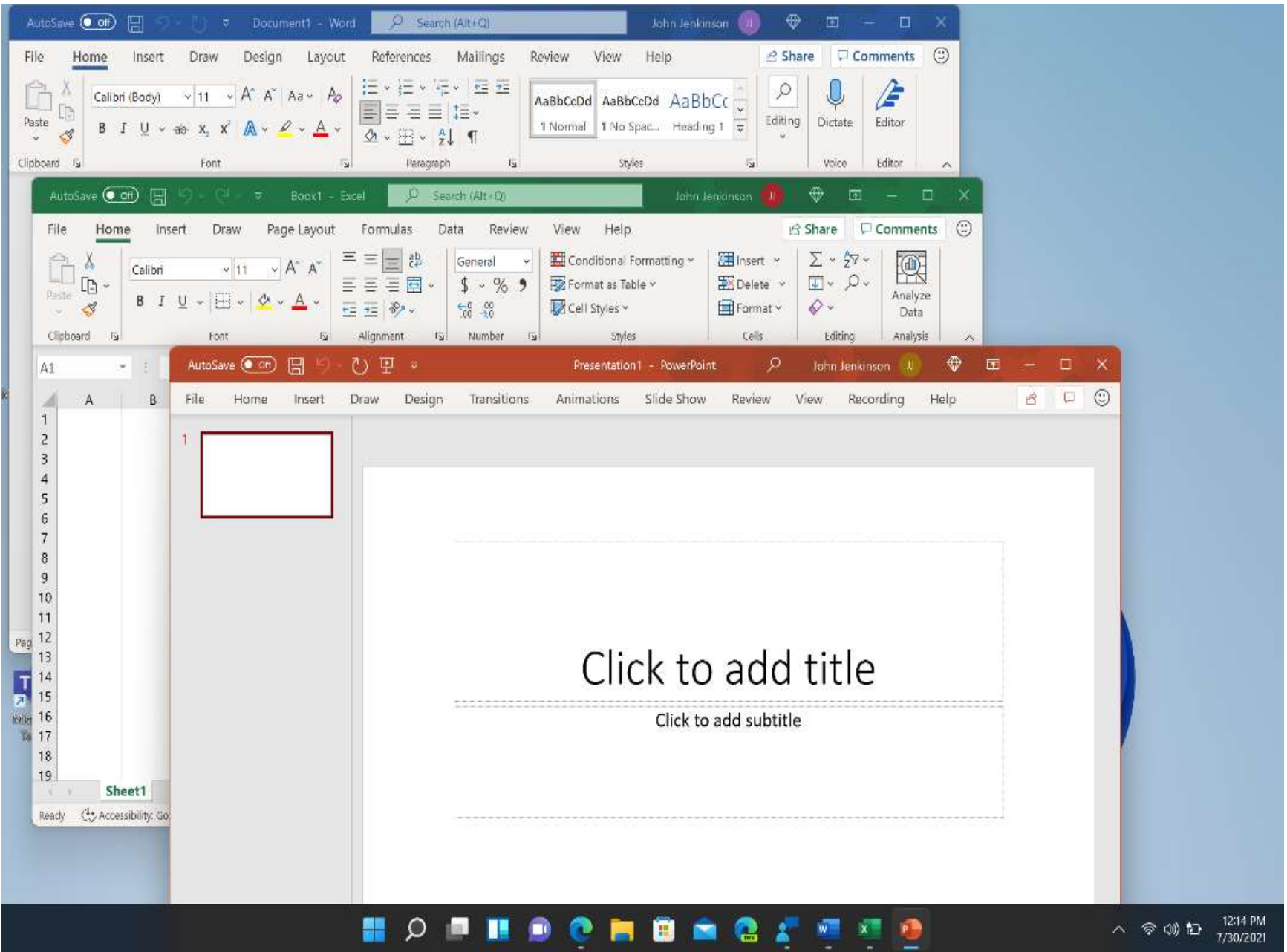
Microsoft® PowerPoint® for Microsoft 365 MSO (16.0.14228.20158) 64-bit

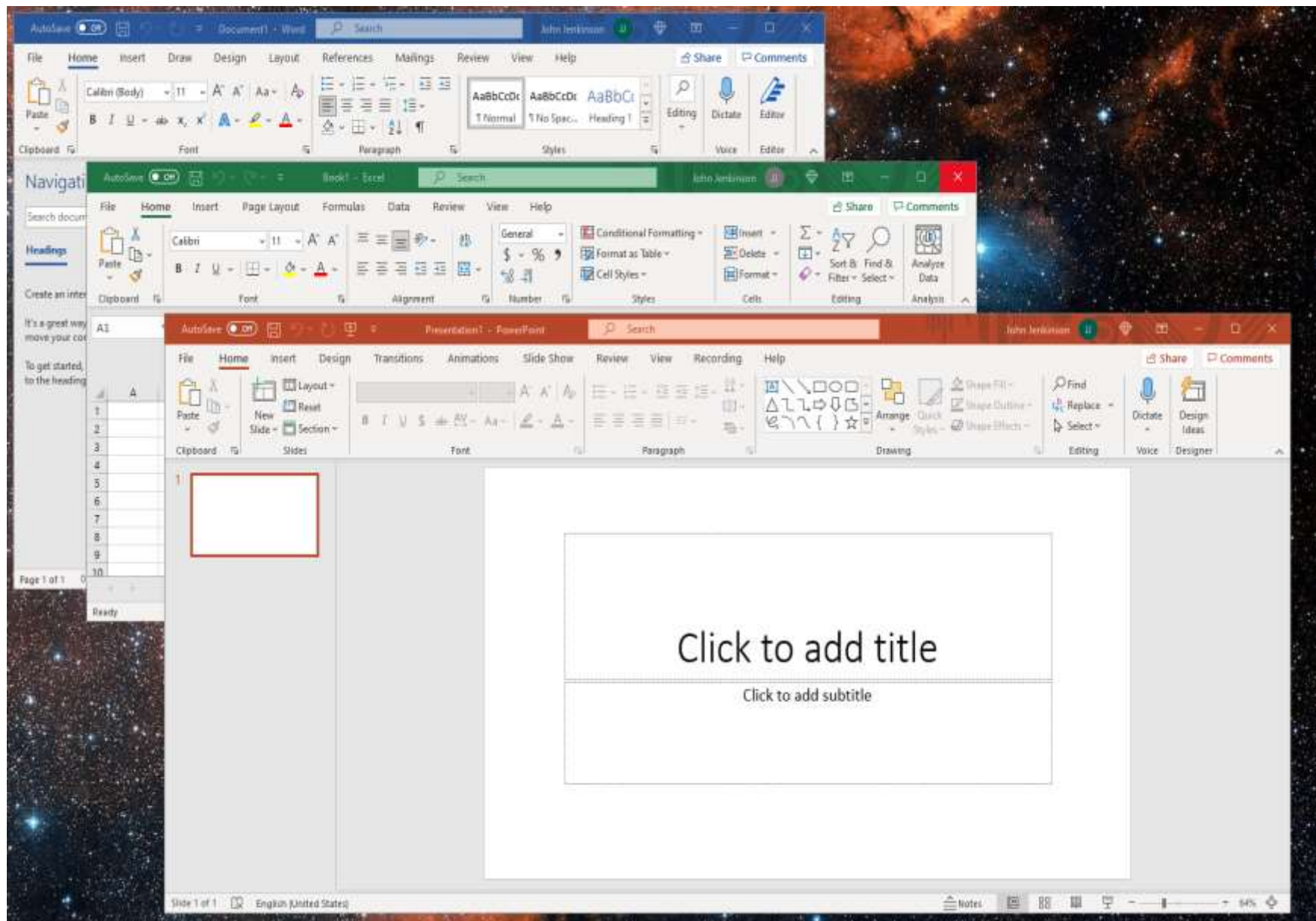
- Windows 10

Microsoft® PowerPoint® for Microsoft 365 MSO (16.0.14228.20200) 32-bit

Microsoft Office 365 style







- Windows 11 feature
- Gaming technology
- Xbox series X Xbox series S
- DirectX 12
- NVMe SSD
- Non-Volatile Memory Express Solid-State Drive
- Direct access to GPU
- Large world loads/saves
- Smaller “chunks”

Direct Storage

KB4023057: Update for Windows 10 Update Service components

- **Summary**
- This update includes reliability improvements to Windows Update Service components in all editions of Windows 10, version 1507, 1511, 1607, 1703, 1709, 1803, 1809, 1903, 1909, 2004, 20H2, and 21H1. It may take steps to free up disk space on your device if you do not have enough disk space to install Windows updates.

Windows Update Update

Notes about this update

- This update may request your device to stay awake longer to enable installation of updates.
Note The installation will respect any user-configured sleep configurations and also your "active hours" when you use your device the most.
- This update may try to reset network settings if problems are detected, and it will clean up registry keys that may be preventing updates from being installed successfully.
- This update may repair disabled or corrupted Windows operating system components that determine the applicability of updates to your version of Windows 10.
- This update may compress files in your user profile directory to help free up enough disk space to install important updates.
- This update may reset the Windows Update database to repair the problems that could prevent updates from installing successfully. Therefore, you may see that your Windows Update history was cleared.

- Settings -> Update & Security -> Windows Security

Windows Security

Windows Security is your home to view and manage the security and health of your device.

Open Windows Security

Protection areas



Virus & threat protection
No actions needed.



Account protection
No actions needed.



Firewall & network protection
No actions needed.



App & browser control
No actions needed.



Device security
No actions needed.

PUP PUA defense settings



Reputation-based protection

These settings protect your device from malicious or potentially unwanted apps, files, and websites.

Check apps and files

Microsoft Defender SmartScreen helps protect your device by checking for unrecognized apps and files from the web.

 On

SmartScreen for Microsoft Edge

Microsoft Defender SmartScreen helps protect your device from malicious sites and downloads.

 On

Potentially unwanted app blocking

Protect your device from low-reputation apps that might cause unexpected behaviors.

 On

☒ Block apps

☒ Block downloads

• edge://flags

Edge | edge://flags

Search flags

Reset all

Experiments

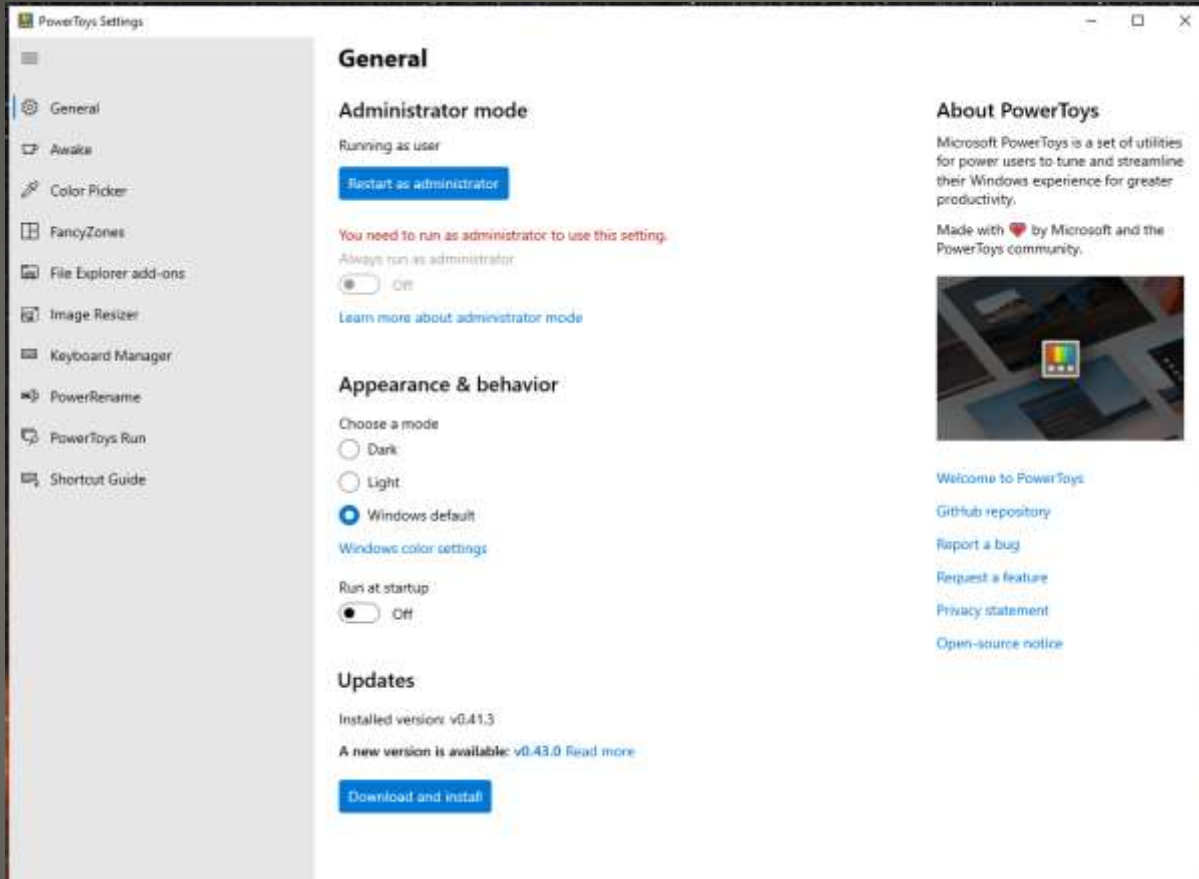
94.0.972.0

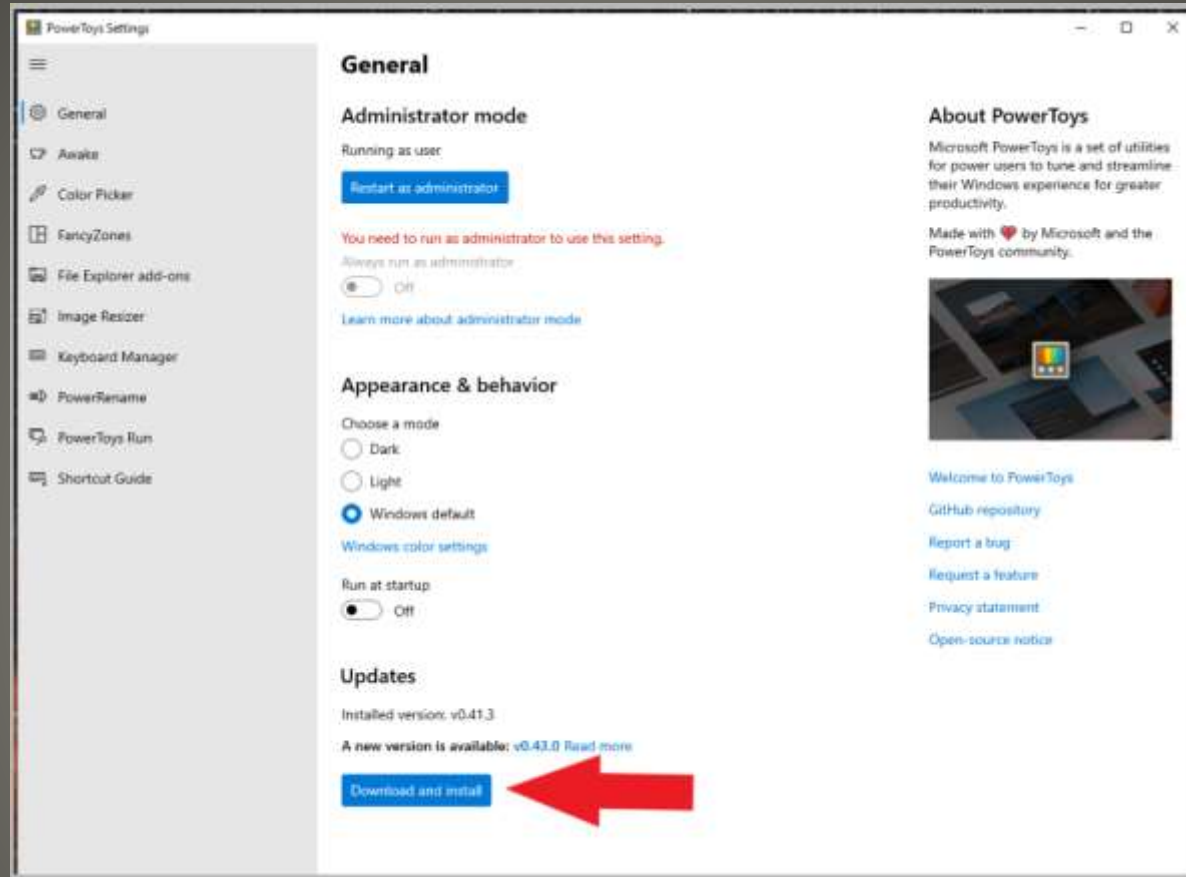
WARNING: EXPERIMENTAL FEATURES AHEAD! By enabling these features, you could lose browser data or compromise your security or privacy. Enabled features apply to all users of this browser. If you are an enterprise admin you should not be using these flags in production.

Available Unavailable

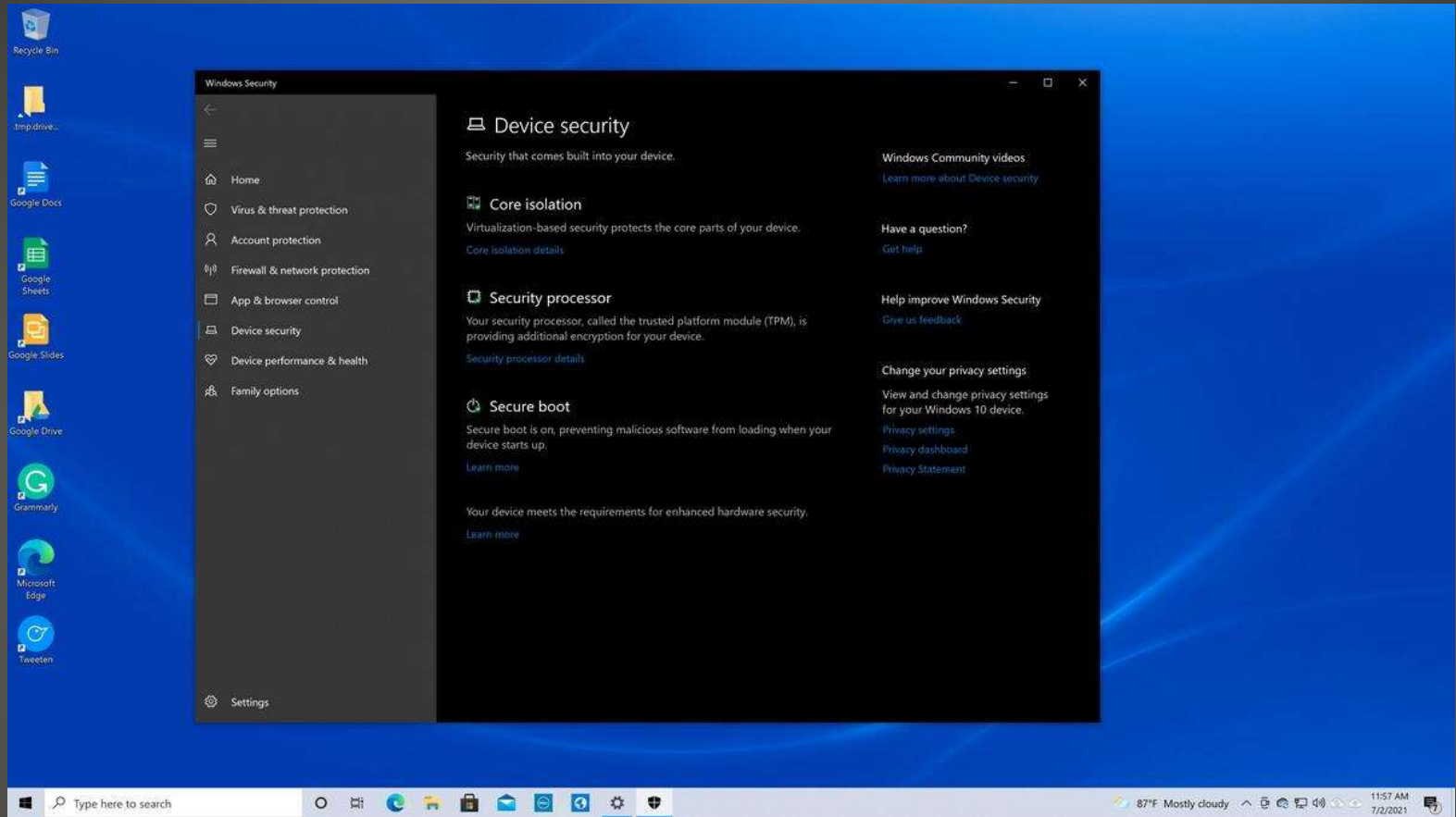
- Automatic HTTPS**
Enables support for Automatic HTTPS, which switches connections to websites from HTTP to HTTPS. The feature can then be turned on/off or further configured at <edge://settings/privacy>. – Mac, Windows, Linux, Android
[#edge-automatic-https](#) **Enabled**
- Super Duper Secure Mode**
Disables the JIT and enables new security mitigations to provide a more secure browsing experience. – Windows
[#edge-enable-super-duper-secure-mode](#) **Enabled**

Edge Super Duper Secure Mode

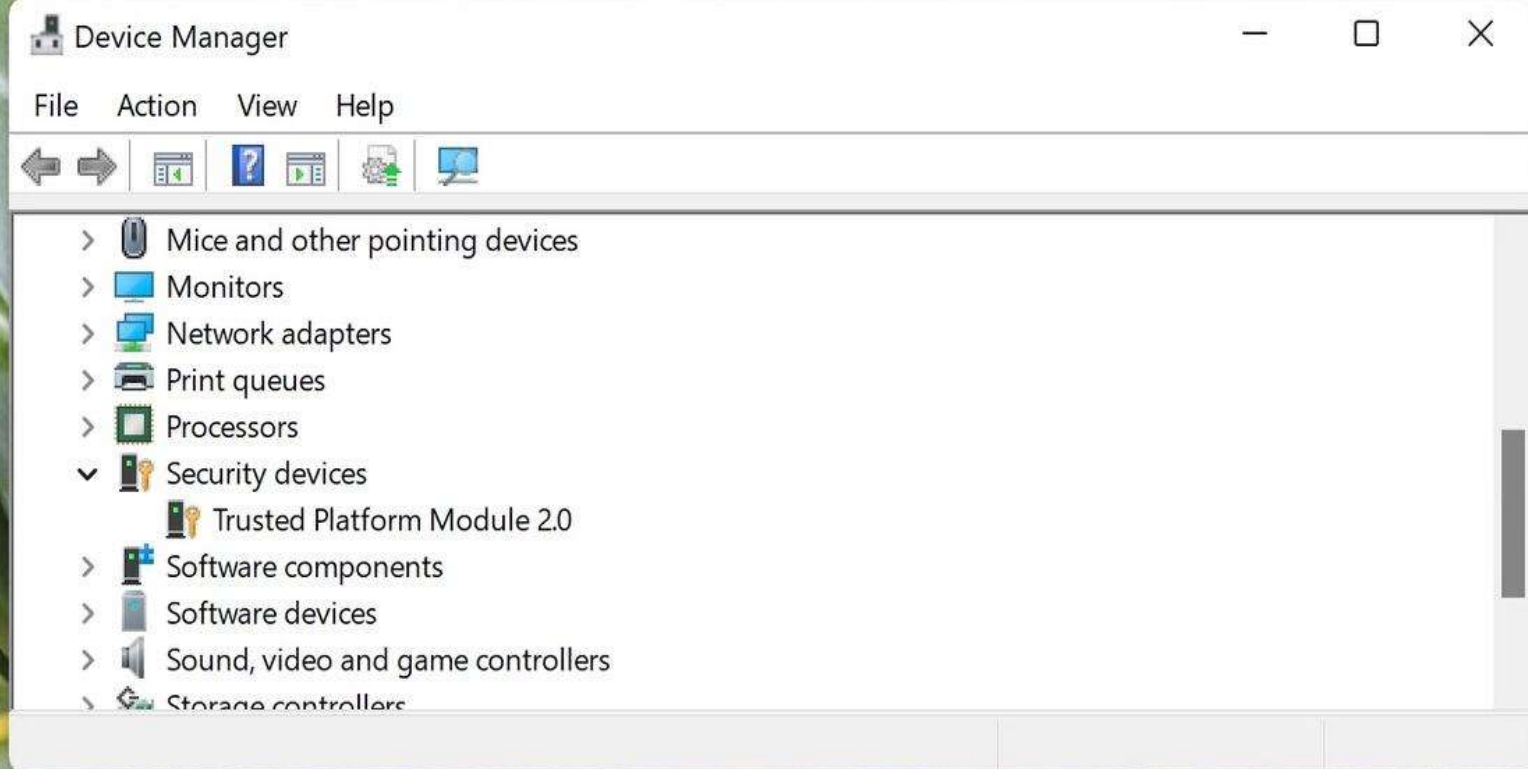




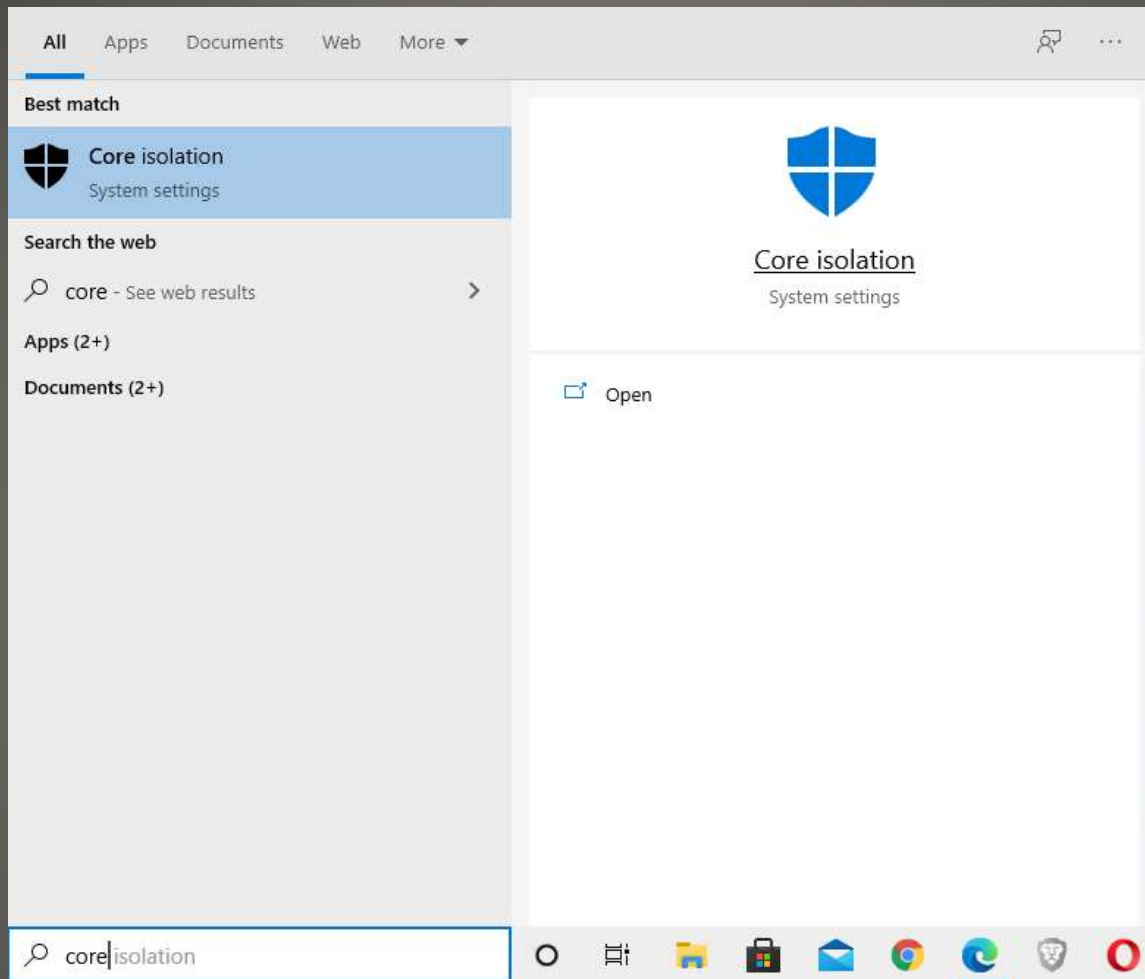
PowerTools



Device Security



Trusted Platform Module 2.0



Hypervisor Protected Code Integrity (HVCI) Virtualization-Based Security



Windows Security

←

☰

Home

Virus & threat protection

Account protection

Firewall & network protection

App & browser control

Device security

Device performance & health

Family options

Settings

Core isolation

Security features available on your device that use virtualization-based security.

Memory integrity

Prevents attacks from inserting malicious code into high-security processes.

On

[Learn more](#)

Have a question?

[Get help](#)

Help improve Windows Security

[Give us feedback](#)

Change your privacy settings

View and change privacy settings for your Windows 10 device.

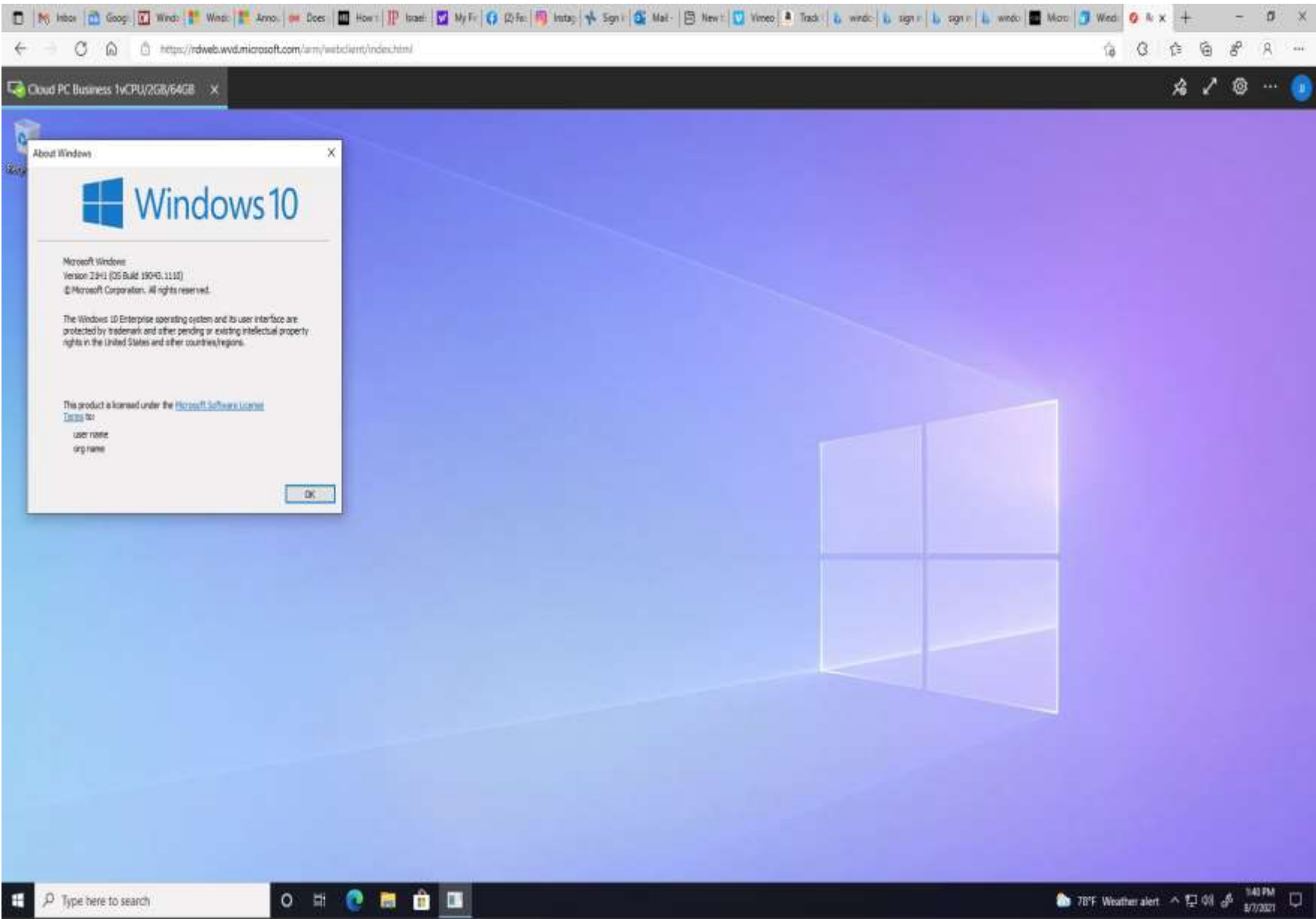
[Privacy settings](#)

[Privacy dashboard](#)

[Privacy Statement](#)

Core Isolation

Windows 365



Oops, we couldn't connect to "Cloud PC Business
1vCPU/2GB/64GB"

You have been disconnected because another connection was made to the remote PC.

Reconnect

Cancel

- Azure Virtual Desktop (AVD)

W

Réunion - Wikipedia

✕

Mail - John Jenkinson - Outlook

✕

Microsoft 365 admin center

✕

+

admin.microsoft.com/AdminPortal/Home?#/subscriptions/webdirect/48dd69ac-9043-44c9-84bd-c4467b7b1120

Microsoft 365 admin center

Search

Dark mode

Home

Users

Groups

Billing

Purchase services

Your products

Licenses

Bills & payments

Billing accounts

Payment methods

Billing notifications

Show all

Home > Your products - Products > Windows 365 Business 1 vCPU, 2 GB, 64 GB

Windows 365 Business 1 vCPU, 2 GB, 64 GB

License

1/1 assigned

Assigned

Available

Buy licenses

Remove licenses

Assign licenses

Purchase information

| | |
|-----------------------|--------------------|
| Initial purchase date | Unit price |
| 8/6/2021 | \$24.00 user/month |

Purchase channel

Commercial direct

Download and install software

Subscription and payment settings

Recurring billing

On, renews on 9/6/2021

Edit recurring billing

Billing frequency

Monthly, \$24.00

Edit billing frequency

Payment method

Visa ****0173

Edit payment method

Replace payment method

Subscription status

Active

Cancel subscription

Service usage address

105 Liatris Ln
Georgetown, TX
US

Edit service usage address

Product details and upgrades

Add-ons

- My account
- Personal info
- Subscriptions
- Security & privacy
- App permissions
- Apps & devices
- Tools & add-ins

Office apps & devices

View apps & devices

Subscriptions

Verify what products and licenses you have.

View subscriptions

Security & privacy

Protect your account and adjust important privacy settings to your preference.

Manage security & privacy

App permissions

Apps with access to your data: 3

Manage which apps have access to your data. You can revoke permission whenever you want.

Change app permissions



Welcome to Windows 365, John Jenkinson

With the world's first cloud PC, Windows 365 is the next step in personal computing. It's Windows in the cloud for you.

Back

Next



Setting up your cloud PC
[VSB_Policy_with_OS_Optimizations - John Jenkinson](#)



What's a cloud PC?

A cloud PC is your desktop, apps, settings, and content streamed from Windows 365 to any supported device.

Back

Next



Setting up your cloud PC
[VSB_Policy_with_OS_Optimizations - John Jenkinson](#)



What can I do with a cloud PC?

With a cloud PC, you'll have a secured place to store and access your apps, files, and documents. Get to it anytime on any supported, internet-connected device.

[Back](#)[Next](#)

Setting up your cloud PC
[VSB_Policy_with_OS_Optimizations](#) - John
Jenkinson



W Réunion - Wikipedia



Mail - John Jenkinson - Outlook



Microsoft 365 admin center



Windows 365



windows365.microsoft.com



Your cloud PC is getting ready



While you're waiting, learn how to get around Windows 365.

Get started




Setting up your cloud PC
[VSB_Policy_with_OS_Optimizations](#) - John
Jenkinson






Welcome John Jenkinson


Quick actions




Manage your organization
Manage users and assign licenses for Microsoft 365 products.



Download Remote Desktop
Access your cloud PC directly from your device with the Remote Desktop...




Get more cloud PCs
Add more cloud PCs to your subscription for you and your team.







Your cloud PCs

○ Setting up cloud PC



VSB_Policy_with_OS_... ⚙️

 1 vCPU
 2GB RAM
 64GB Storage

 Open in browser

Your cloud PC is ready for you
It has all the apps you need, with no additional setup.

1 of 3

Next



Welcome John Jenkinson

Quick actions



Manage your organization
Manage users and assign licenses for Microsoft 365 products.



Download Remote Desktop
Access your cloud PC directly from your device with the Remote Desktop...




Get more cloud PCs
Add more cloud PCs to your subscription for you and your team.





Your cloud PCs


⌚ Setting up cloud PC




VS_B_Policy_with_OS_... ⚙️

 1 vCPU

 2GB RAM

 64GB Storage

 Open in browser

Manage your cloud PC ✕

To see more options, select Settings.

3 of 3

Previous

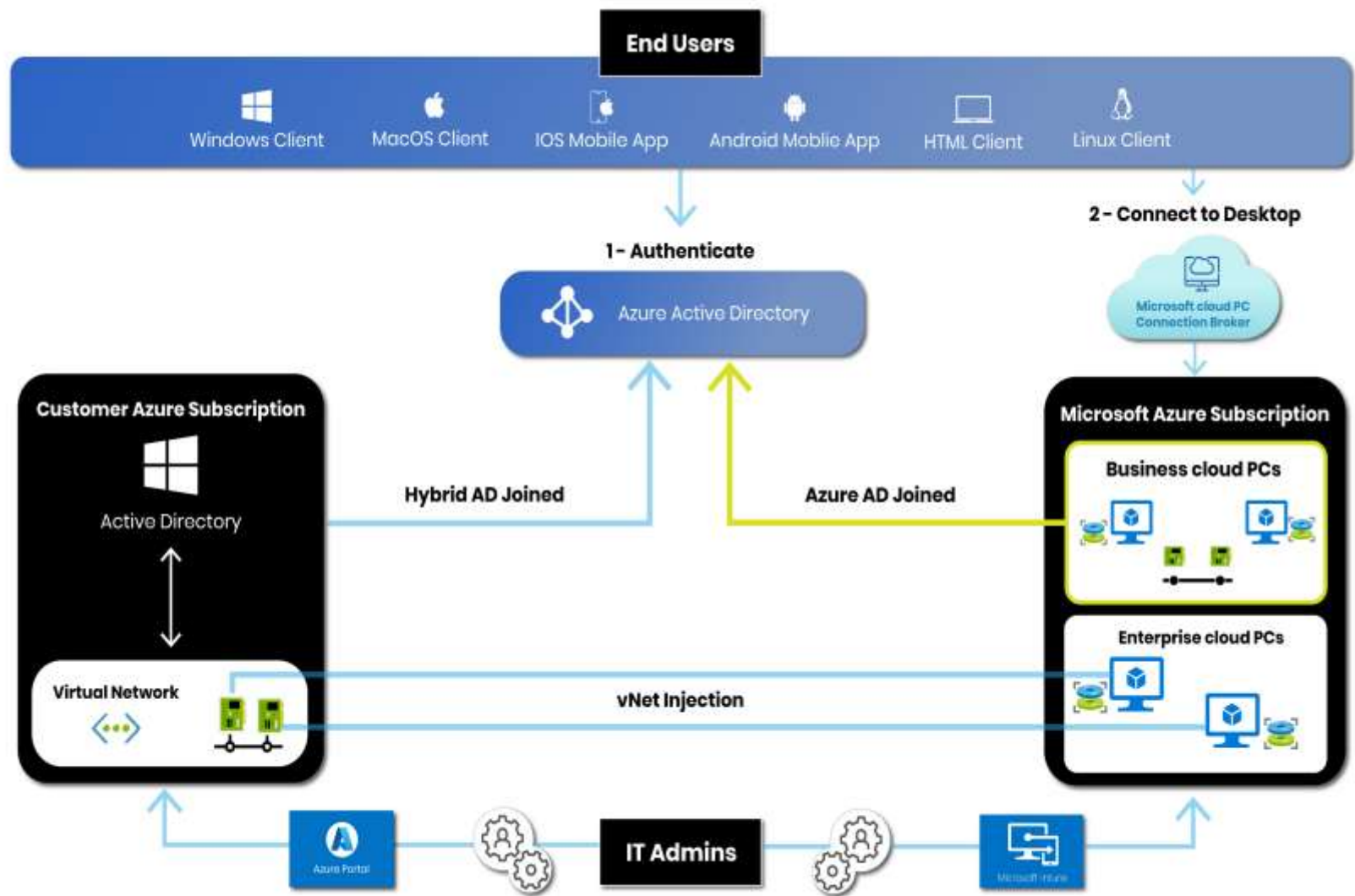
Got it

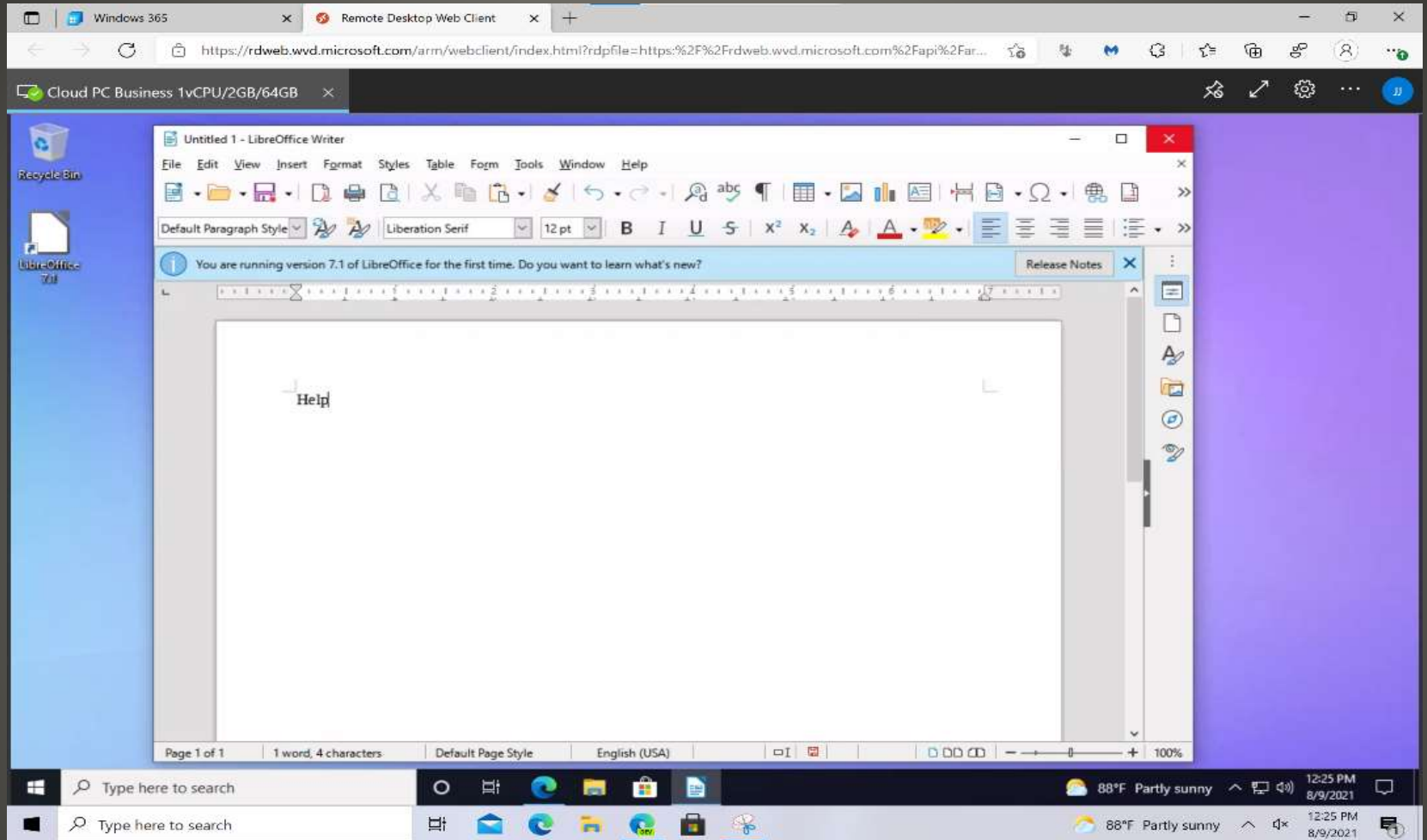
- Virtual desktop service
- Part of Microsoft 365
- Cloud PC Dedicated to a user
- Fixed price – No consumption pricing
- Not Azure

Windows 365

| Compute | Storage | Example scenarios | Recommended apps |
|--------------------|---------|--|--|
| 1 vCPU / 2 GB RAM | 64 | Firstline workers, call centers, education/training/CRM access | Office light (web-based), Microsoft Edge, OneDrive, lightweight line-of-business apps, Defender support |
| 2 vCPU / 4 GB RAM | 64 | Mergers and acquisitions, short-term and seasonal, customer service, bring-your-own-PC, work from home | Microsoft 365 Apps, Microsoft Teams (audio only), Outlook, Excel, PowerPoint, OneDrive, Adobe Reader, Microsoft Edge, line-of-business apps, Defender support |
| | 128 | | |
| | 256 | | |
| 2 vCPU / 8 GB RAM | 128 | Bring-your-own-PC, work from home, market researchers, government, consultants | Microsoft 365 Apps, Microsoft Teams, Outlook, Excel, Access, PowerPoint, OneDrive, Adobe Reader, Microsoft Edge, line-of-business apps, Defender support |
| | 256 | | |
| 4 vCPU / 16 GB RAM | 128 | Finance, government, consultants, healthcare services, bring-your-own-PC, work from home | Microsoft 365 Apps, Microsoft Teams, Outlook, Excel, Access, PowerPoint, Power BI, Dynamics 365, OneDrive, Adobe Reader, Microsoft Edge, line-of-business apps, Defender support |
| | 256 | | |
| | 512 | | |
| 8 vCPU / 32 GB RAM | 128 | Software developers, engineers, content creators, design and engineering workstations | Microsoft 365 Apps, Microsoft Teams, Outlook, Excel, Access, PowerPoint, Power BI, Visual Studio Code, OneDrive, Adobe Reader, Microsoft Edge, line-of-business apps, Defender support |
| | 256 | | |
| | 512 | | |

Windows 365 sizes





Windows 365 LibreOffice

Windows 365 x Remote Desktop Web Client x (2,076 unread) - jenkinsonjp@y... x +

https://rdweb.wvd.microsoft.com/arm/webclient/index.html?rdpfile=https:%2F%2Frdweb.wvd.microsoft.com%2Fapi%2Far...

Cloud PC Business 1vCPU/2GB/64GB x

Settings

View configured update policies

Wondering why you're seeing 'Some settings are managed by your organization'?

This text is typically displayed on Windows Update after installation and delivery policies are configured.

Examples include:

- Your organization has set some policies to manage updates
- You have opted in for the Windows Insider Program

Policies set on your device

Automatically download updates and install them on the specified schedule
Source: Administrator
Type: Group Policy

Quality update deferral period
Source: Administrator
Type: Mobile Device Management

Feature update deferral period
Source: Administrator
Type: Mobile Device Management

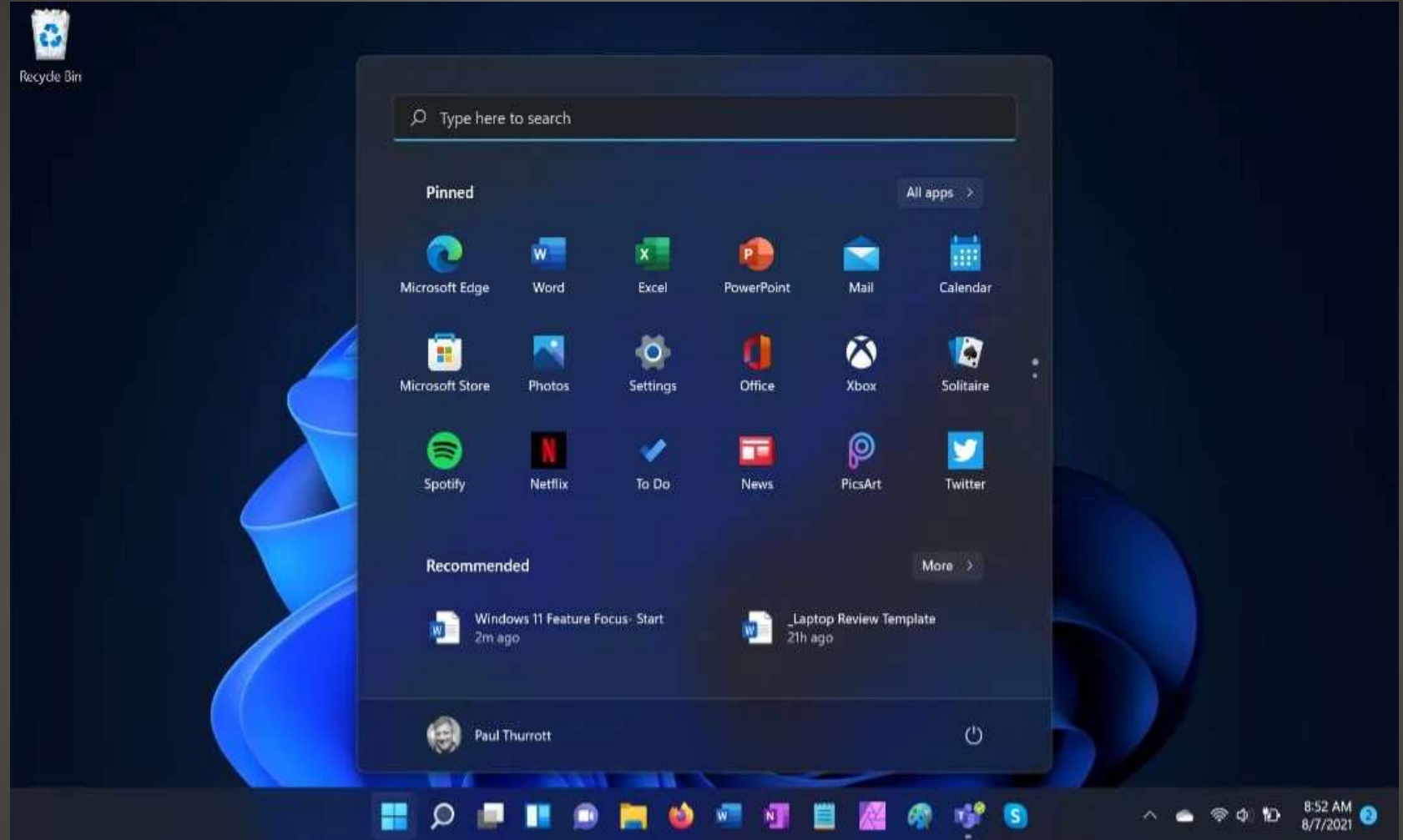
Enable deadline for automatic updates and restarts for Quality Updates
Source: Administrator
Type: Mobile Device Management

Type here to search

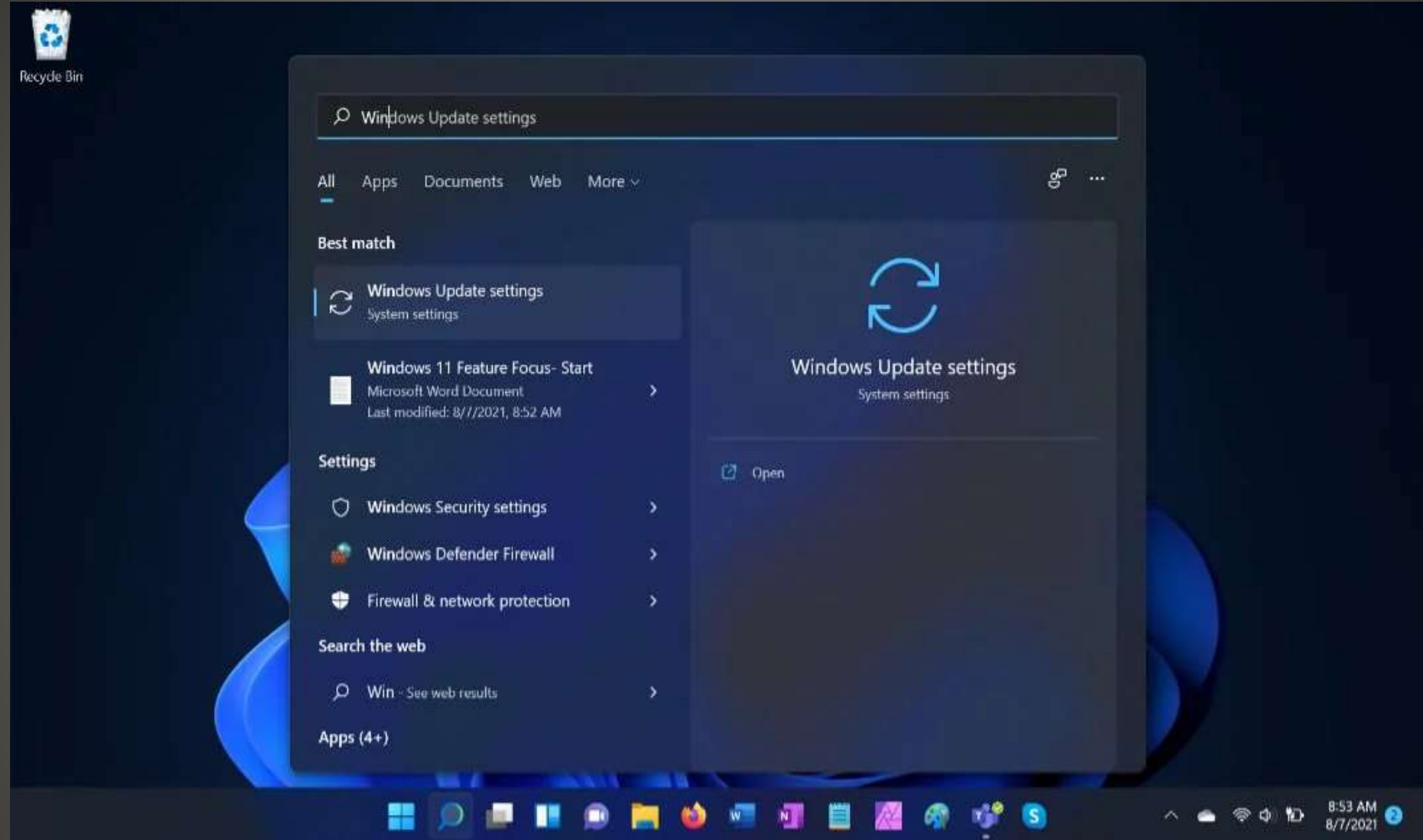
90°F Partly sunny 12:51 PM 8/9/2021

- Fast Internet download (1.3Gb/s – 230 Mb/s)
- Work on large content
- MINIMAL PROTECTIONS
- Account & Passphrase
- Easy to take over
- It's just out there

Windows 365



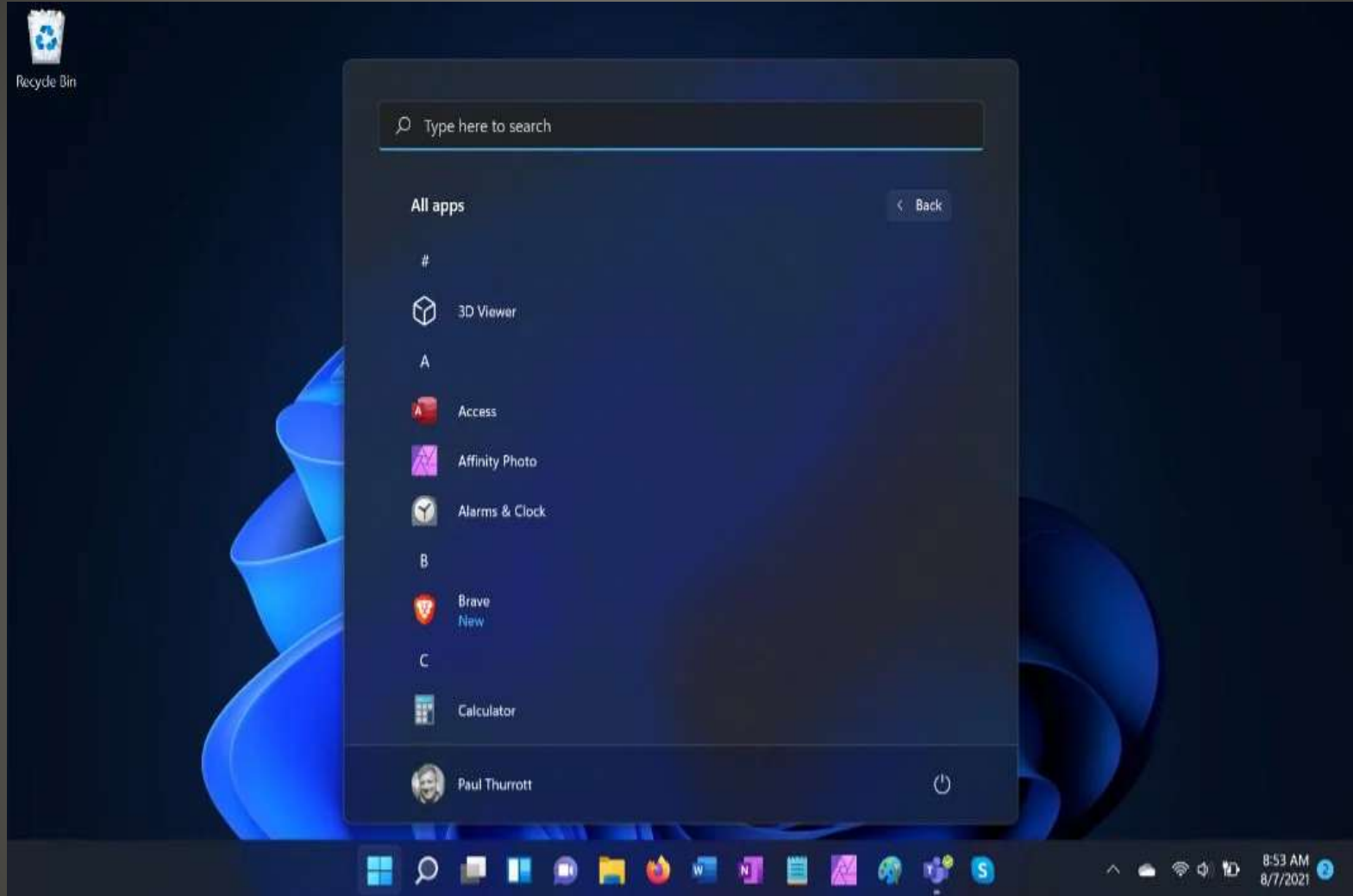
Windows 11 Start Menu



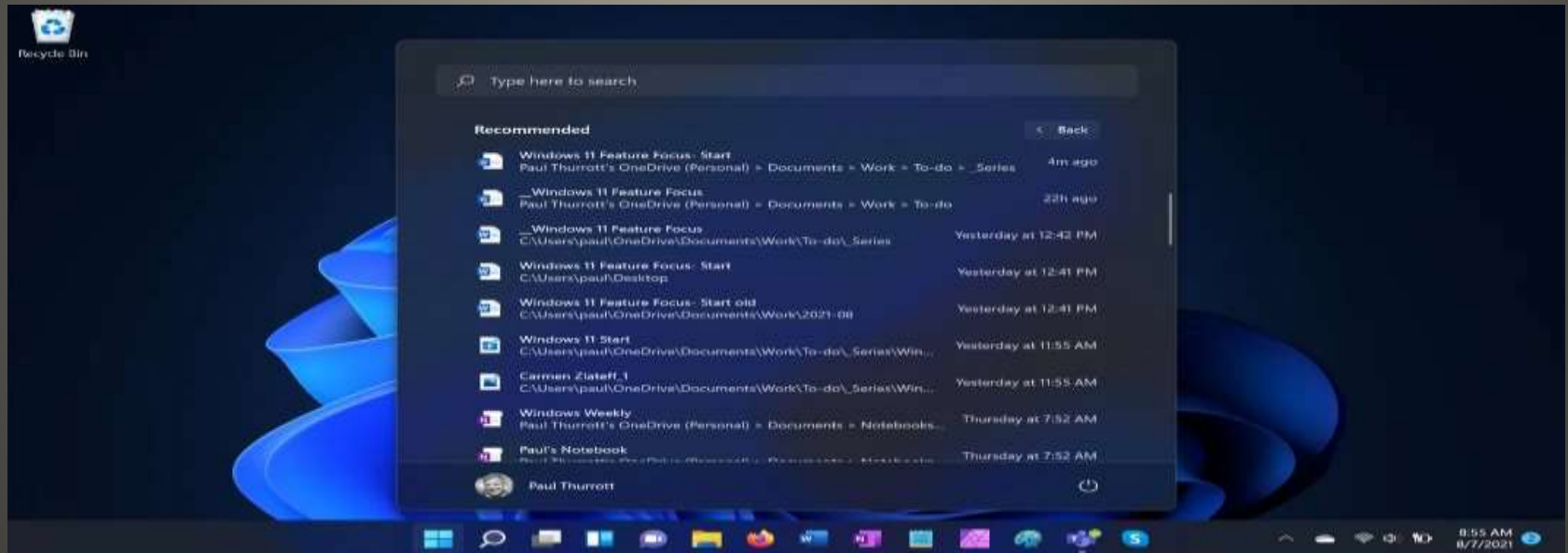
Windows 11 Start Menu - Search



Windows 11 Start Menu - Pinned



Windows 11 Start Menu – All Apps

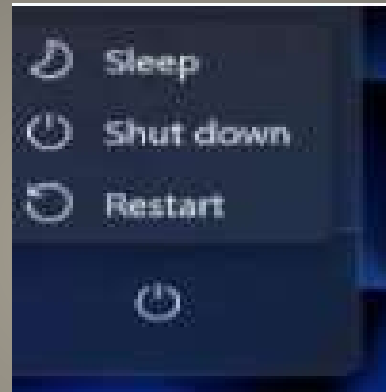


Windows 11 Start Menu - Recommended

- Change account settings
- Lock PC
- Sign out
- Switch user



Windows 11 Start Menu - Account

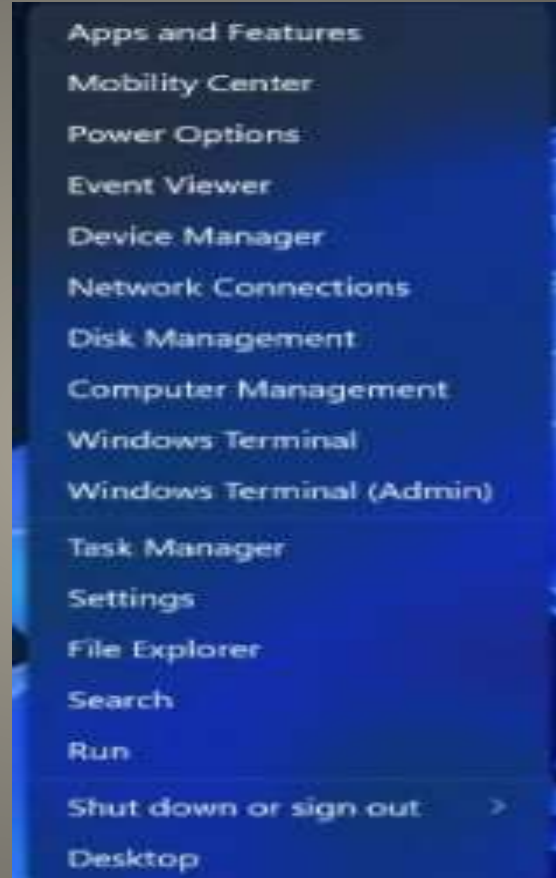


Windows 11 Start Menu - Power

Windows 10



Windows 11



Start Menu right click

Personalization > Start



Show recently added apps

On



Show most used apps

Off



Show recently opened items in Start, Jump Lists, and File Explorer

On



Folders

These folders appear on Start next to the Power button



Get help



Give feedback

Windows 11 Start Menu Personalization

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

