Sun City Computer Club

Windows SIG

August 9, 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

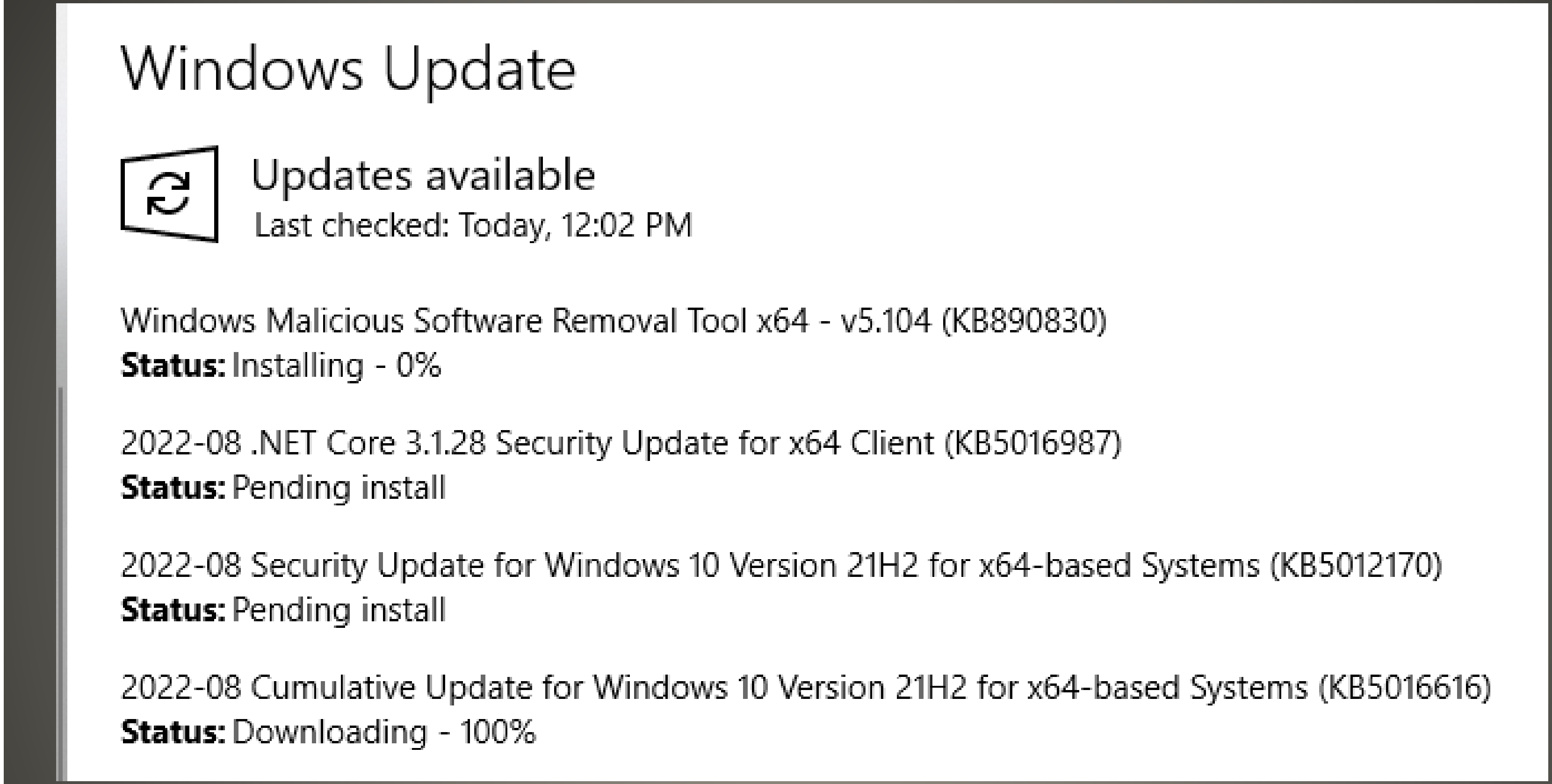
- Sig leader – anyone?
- Topic Suggestions – plea(se)
- Your suggestions future presentations
- In person meetings

- Ever want to be a presenter??

Presenter???

- 141 vulnerabilities
- 17 Critical
- 2 Previously disclosed
- 1 Active exploitation

Microsoft Patch Tuesday



Windows Update

Updates available

Last checked: Today, 12:02 PM

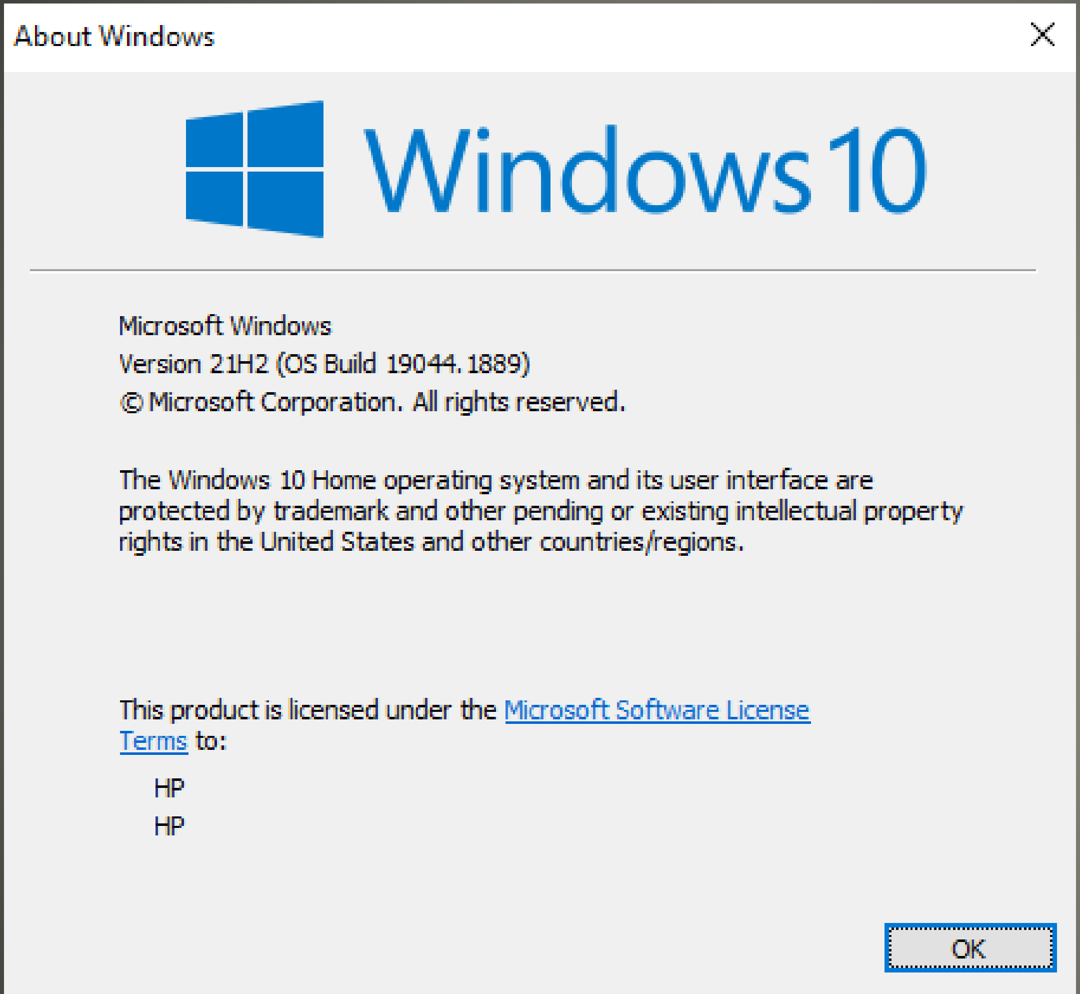
Windows Malicious Software Removal Tool x64 - v5.104 (KB890830)
Status: Installing - 0%

2022-08 .NET Core 3.1.28 Security Update for x64 Client (KB5016987)
Status: Pending install

2022-08 Security Update for Windows 10 Version 21H2 for x64-based Systems (KB5012170)
Status: Pending install

2022-08 Cumulative Update for Windows 10 Version 21H2 for x64-based Systems (KB5016616)
Status: Downloading - 100%

Windows 10



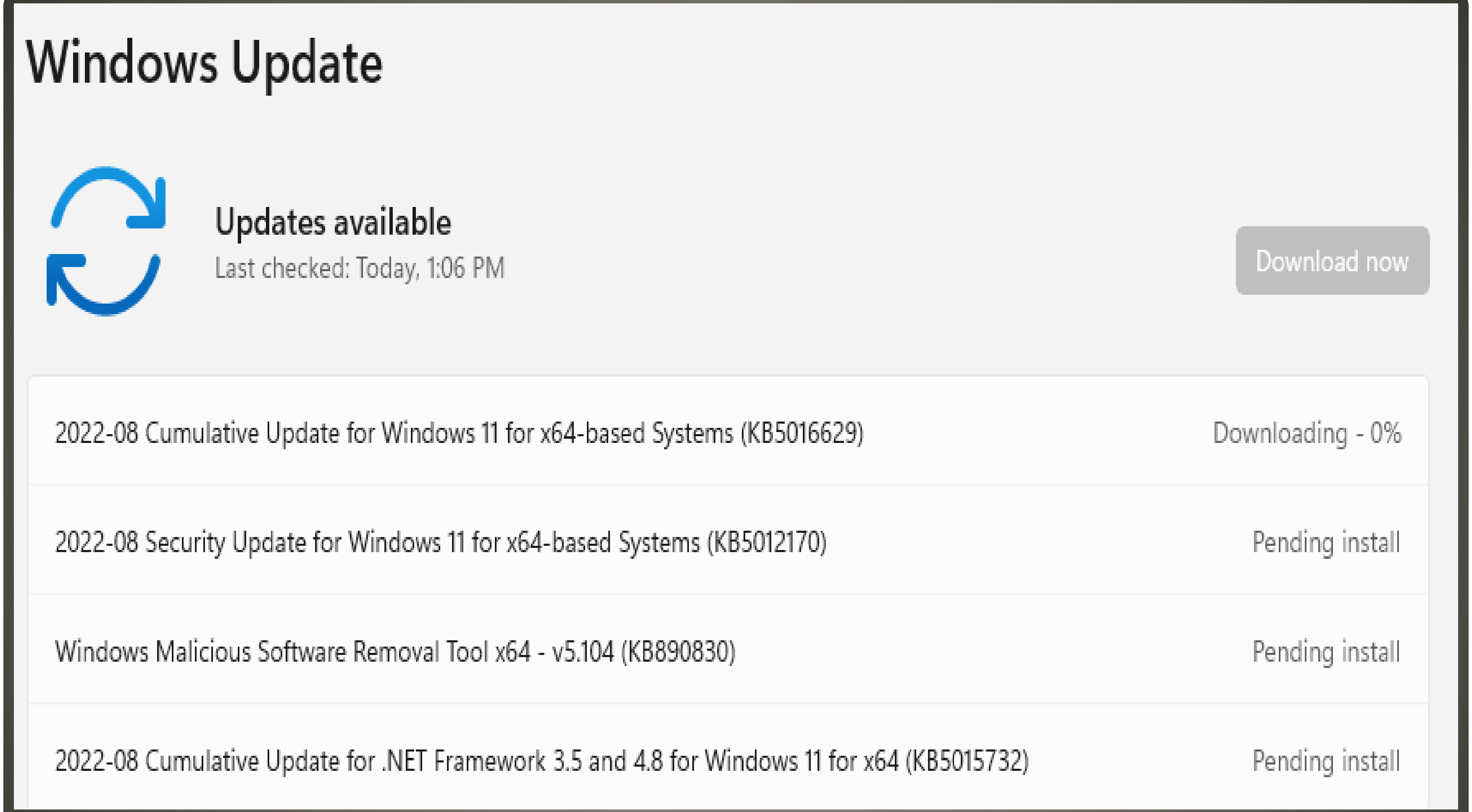
Microsoft Windows
Version 21H2 (OS Build 19044.1889)
© Microsoft Corporation. All rights reserved.

The Windows 10 Home operating system and its user interface are protected by trademark and other pending or existing intellectual property rights in the United States and other countries/regions.

This product is licensed under the Microsoft Software License Terms to:

HP
HP

Windows 10



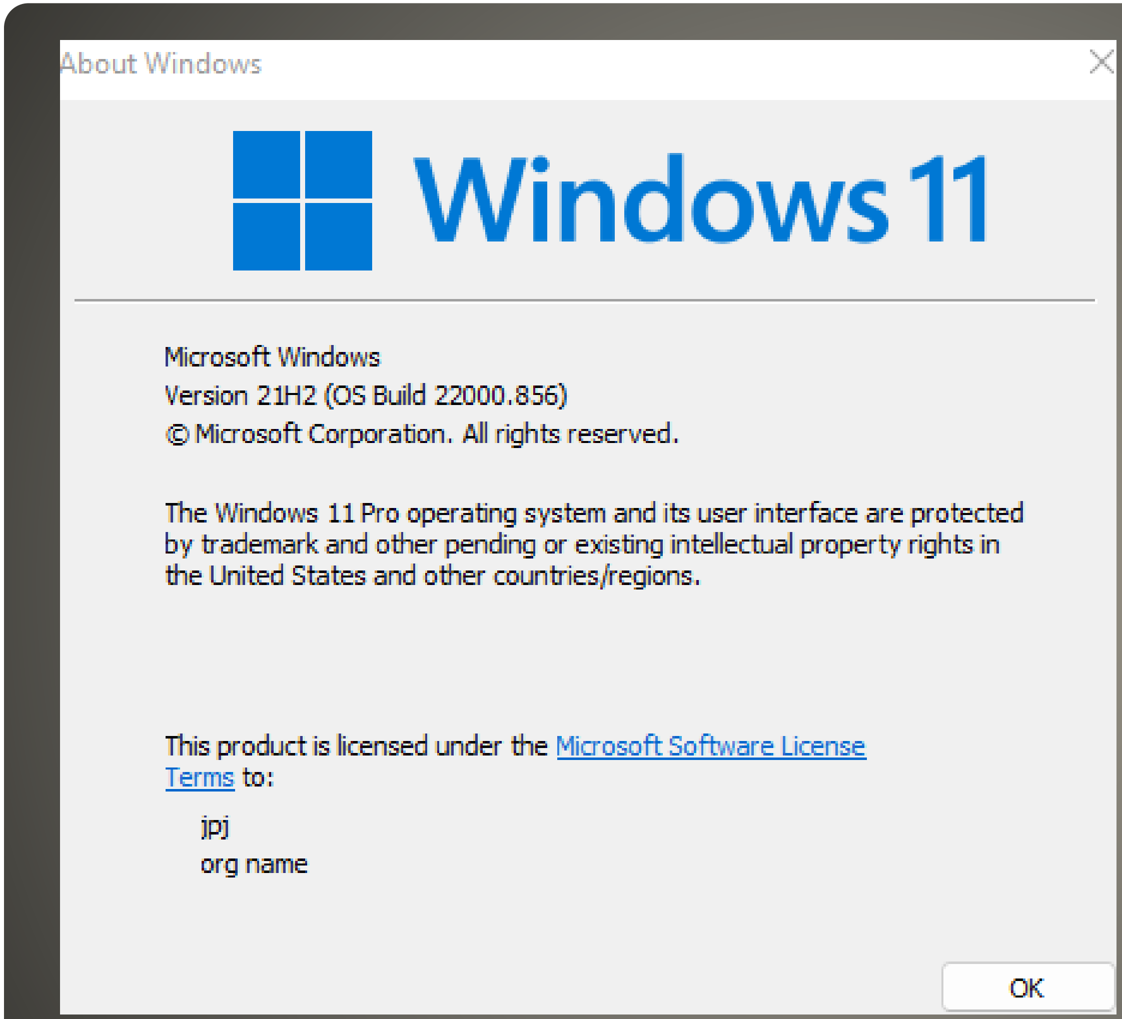
Windows Update

Updates available

Last checked: Today, 1:06 PM

2022-08 Cumulative Update for Windows 11 for x64-based Systems (KB5016629)	Downloading - 0%
2022-08 Security Update for Windows 11 for x64-based Systems (KB5012170)	Pending install
Windows Malicious Software Removal Tool x64 - v5.104 (KB890830)	Pending install
2022-08 Cumulative Update for .NET Framework 3.5 and 4.8 for Windows 11 for x64 (KB5015732)	Pending install

Windows 11



Microsoft Windows
Version 21H2 (OS Build 22000.856)
© Microsoft Corporation. All rights reserved.

The Windows 11 Pro operating system and its user interface are protected by trademark and other pending or existing intellectual property rights in the United States and other countries/regions.

This product is licensed under the Microsoft Software License Terms to:

jpj
org name

Windows 11

While you are at it

- Microsoft Store
- Browser Updates
- Browser extension updates
- App updates

- Bug fixes
- Focus Assist

  New option *Important Notifications*

Feature updates

Purchase & download Windows 11

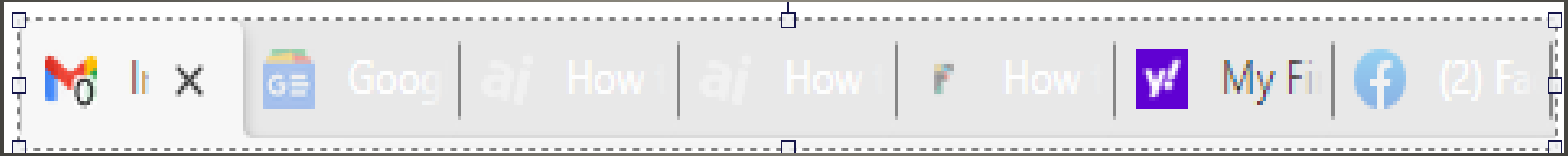
- Windows 11 Home $139
- Windows 11 Pro $199

Faster Edge?

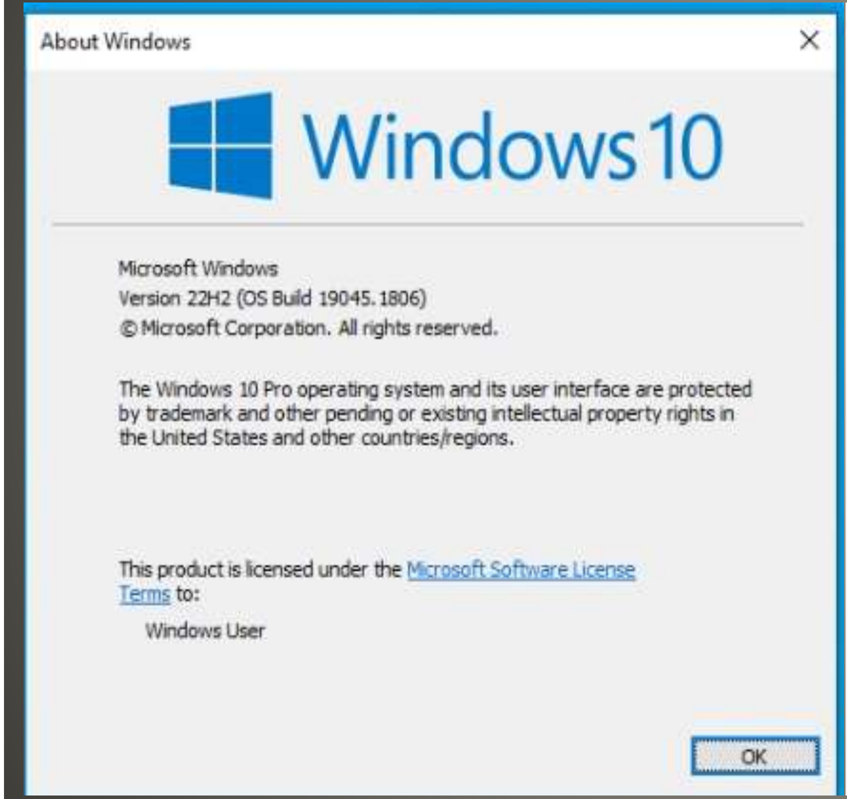
- Compressing disk caches

- Sleeping Tabs 32% less memory
- Sleeping Tabs 37% less cup
- Edge versions 103.1264.77 (Official)
- Edge versions 105.0.1329.1 Dev channel

- https://www.microsoftedgeinsider.com/en-us/whats-new



- Insider
- 10 & 11

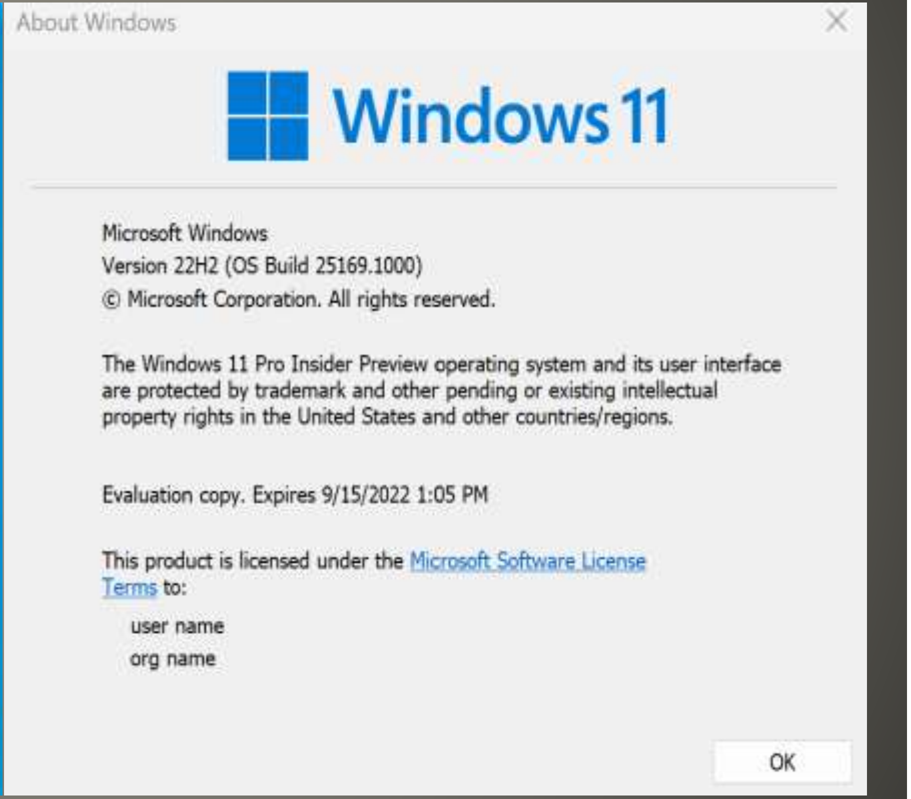


Microsoft Windows
Version 22H2 (OS Build 19045.1806)
© Microsoft Corporation. All rights reserved.

The Windows 10 Pro operating system and its user interface are protected by trademark and other pending or existing intellectual property rights in the United States and other countries/regions.

This product is licensed under the Microsoft Software License Terms to:

Windows User



Microsoft Windows
Version 22H2 (OS Build 25169.1000)
© Microsoft Corporation. All rights reserved.

The Windows 11 Pro Insider Preview operating system and its user interface are protected by trademark and other pending or existing intellectual property rights in the United States and other countries/regions.

Evaluation copy. Expires 9/15/2022 1:05 PM

This product is licensed under the Microsoft Software License Terms to:

user name
org name

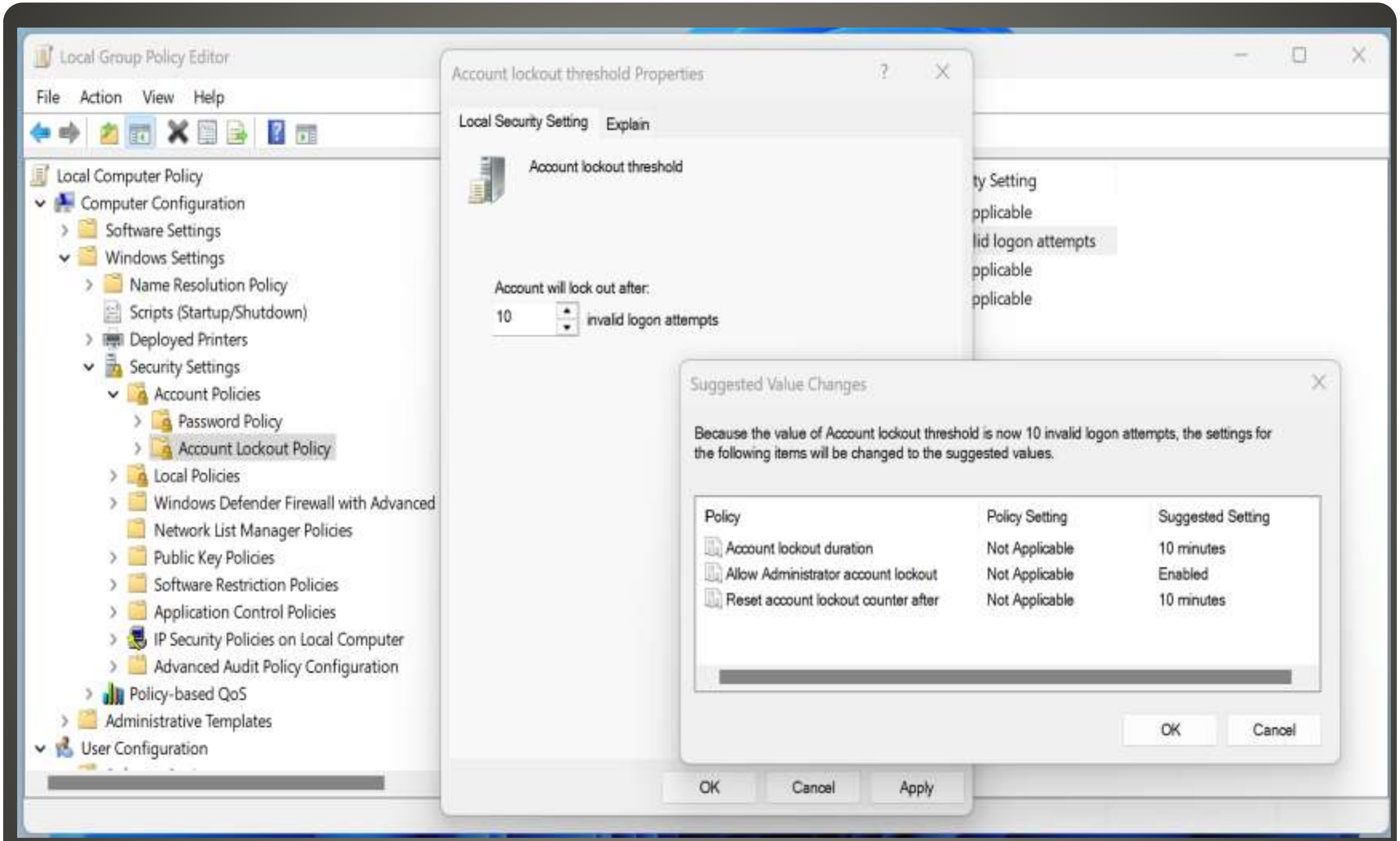
Windows 22H2

- Virtualization-Based Security
- Small performance gain
- Large security risk

Disable VBS ?

CCleaner update

- Microsoft Store awareness
- V6.02.9938 (July 20, 2022)
- NOT A RECOMMENDATION
- INFORMATION
- Past history



Account will lock out after: 10 invalid logon attempts

Because the value of Account lockout threshold is now 10 invalid logon attempts, the settings for the following items will be changed to the suggested values.

Policy	Policy Setting	Suggested Setting
Account lockout duration	Not Applicable	10 minutes
Allow Administrator account lockout	Not Applicable	Enabled
Reset account lockout counter after	Not Applicable	10 minutes

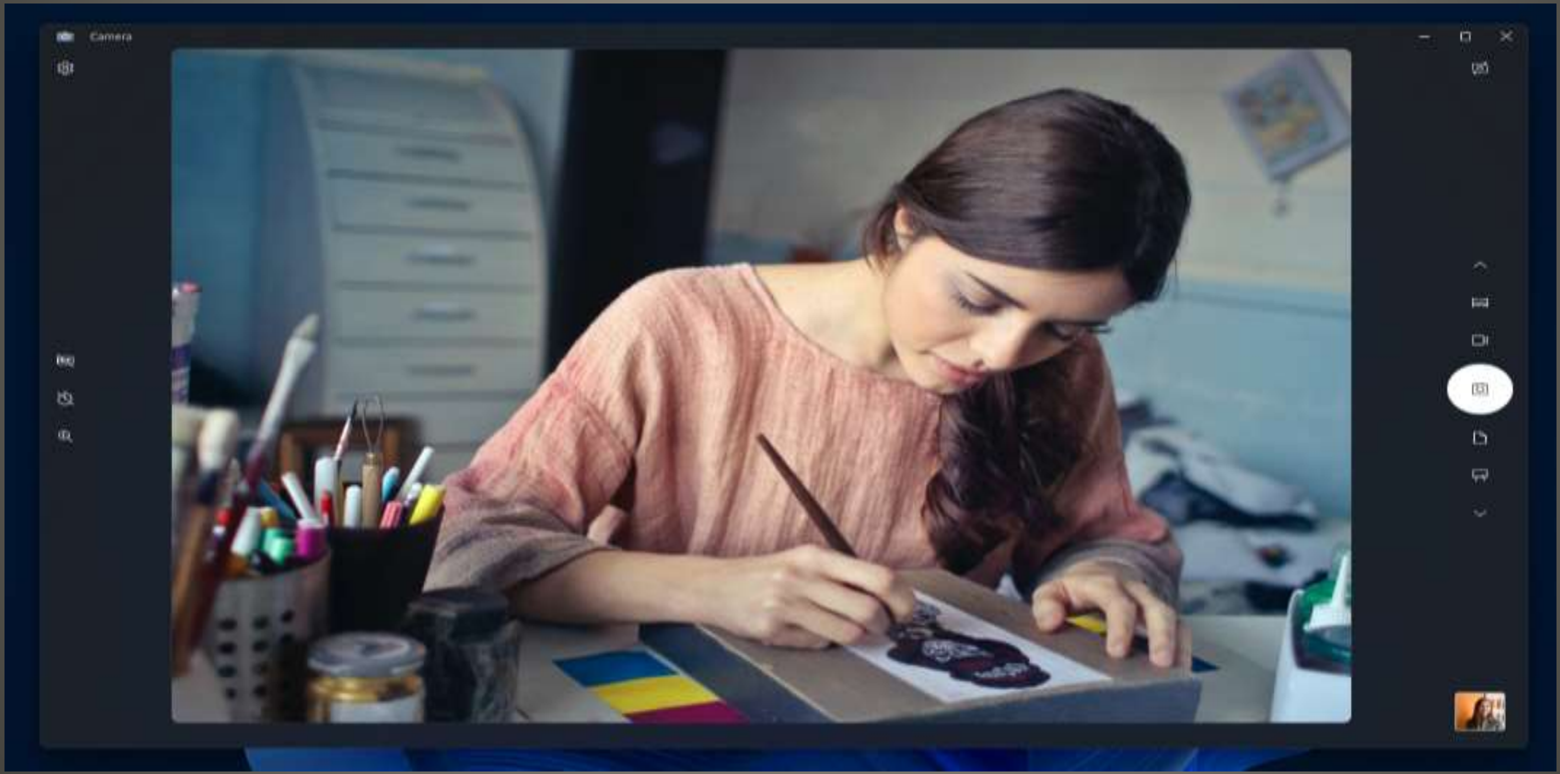
RDP Account Lockout

RDP lockout

- Duration 10 Minute default
- Reset after 10 Minutes
- Brute force
- Low & Slow attackers
- Group Policy to enable

  Even on Windows 10

- Camera Windows 11 visual style QR code barcode scanning

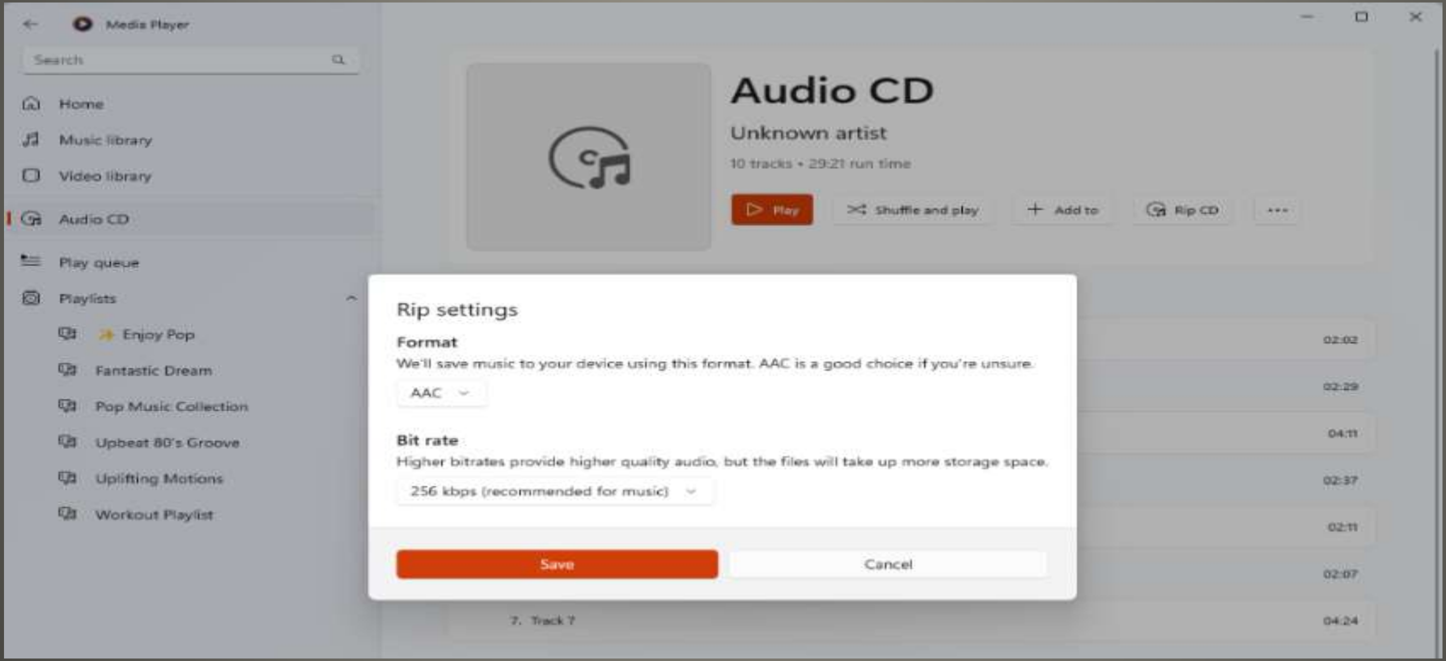


Refresh Apps

- Media Player

  CD ripping capabilities

  Formats supported: AAC, WMA, FLAC, ALAC



Audio CD

Unknown artist

10 tracks • 29:21 run time

Rip settings

Format

We'll save music to your device using this format. AAC is a good choice if you're unsure.

AAC

Bit rate

Higher bitrates provide higher quality audio, but the files will take up more storage space.

256 kbps (recommended for music)

Refresh Apps

Refresh Apps

- Movies & TV App
  Available on ARM PCs
  Migration plans to Media Player App

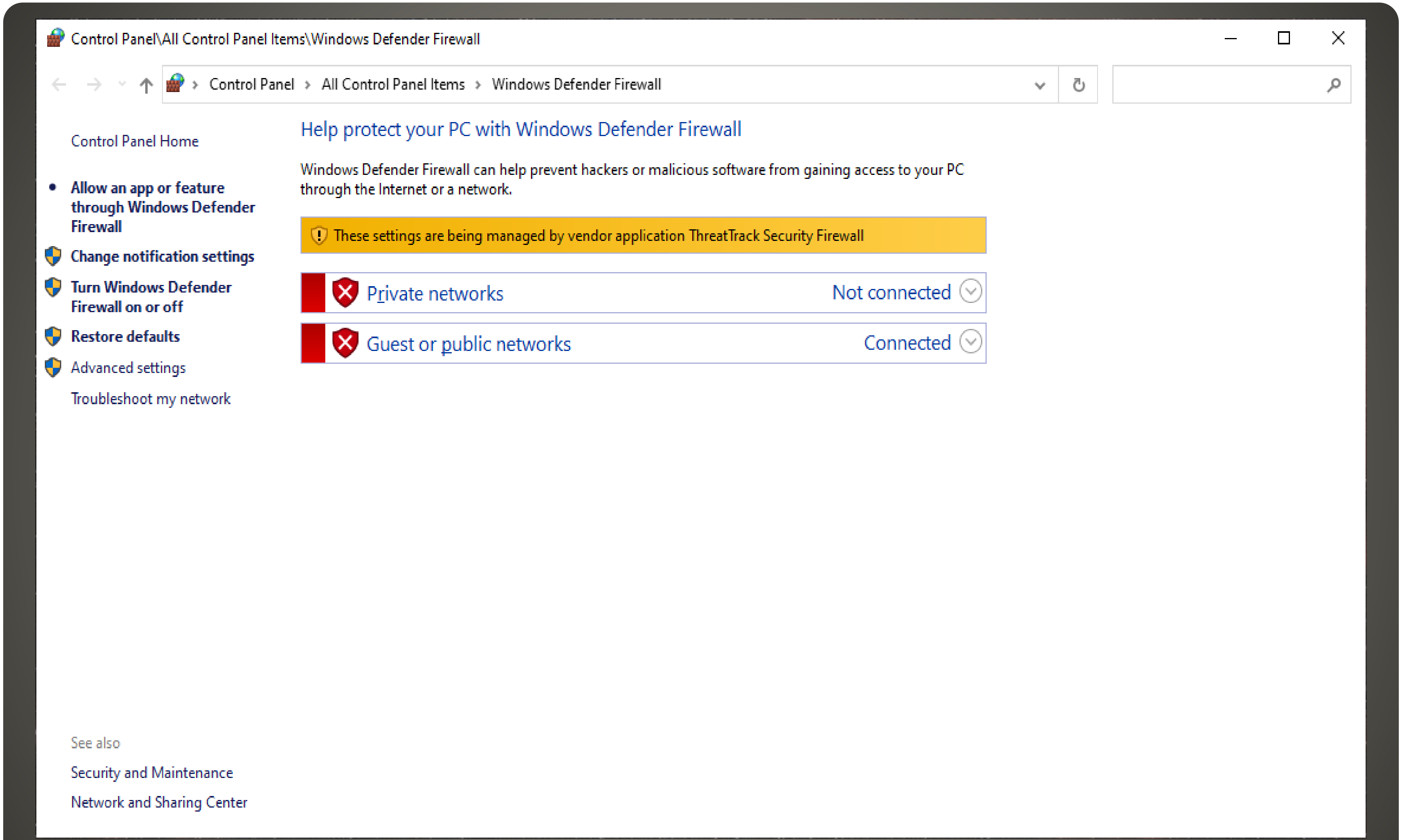
Windows Firewall

- What is a Firewall?
  Network security system
  Monitors and controls network traffic
  Based on rules
  Barrier between trusted and untrusted
- Firewalls can be
  In and on the Internet
  At your ISP
  In your cable modem
  In your router(s)
  In your Wireless Access Point
  In your devices
  In your applications
- Microsoft Windows Firewall

Windows Defender Firewall

- Can be turned off
- Search Box   Windows Firewall
  Control Panel

Inbound rules/filters
Block
Allow
Outbound rules/filters
Block
Allow


Control Panel\All Control Panel Items\Windows Defender Firewall
Control Panel › All Control Panel Items › Windows Defender Firewall
Control Panel Home
Allow an app or feature through Windows Defender Firewall
Change notification settings
Turn Windows Defender Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Security and Maintenance
Network and Sharing Center

Help protect your PC with Windows Defender Firewall

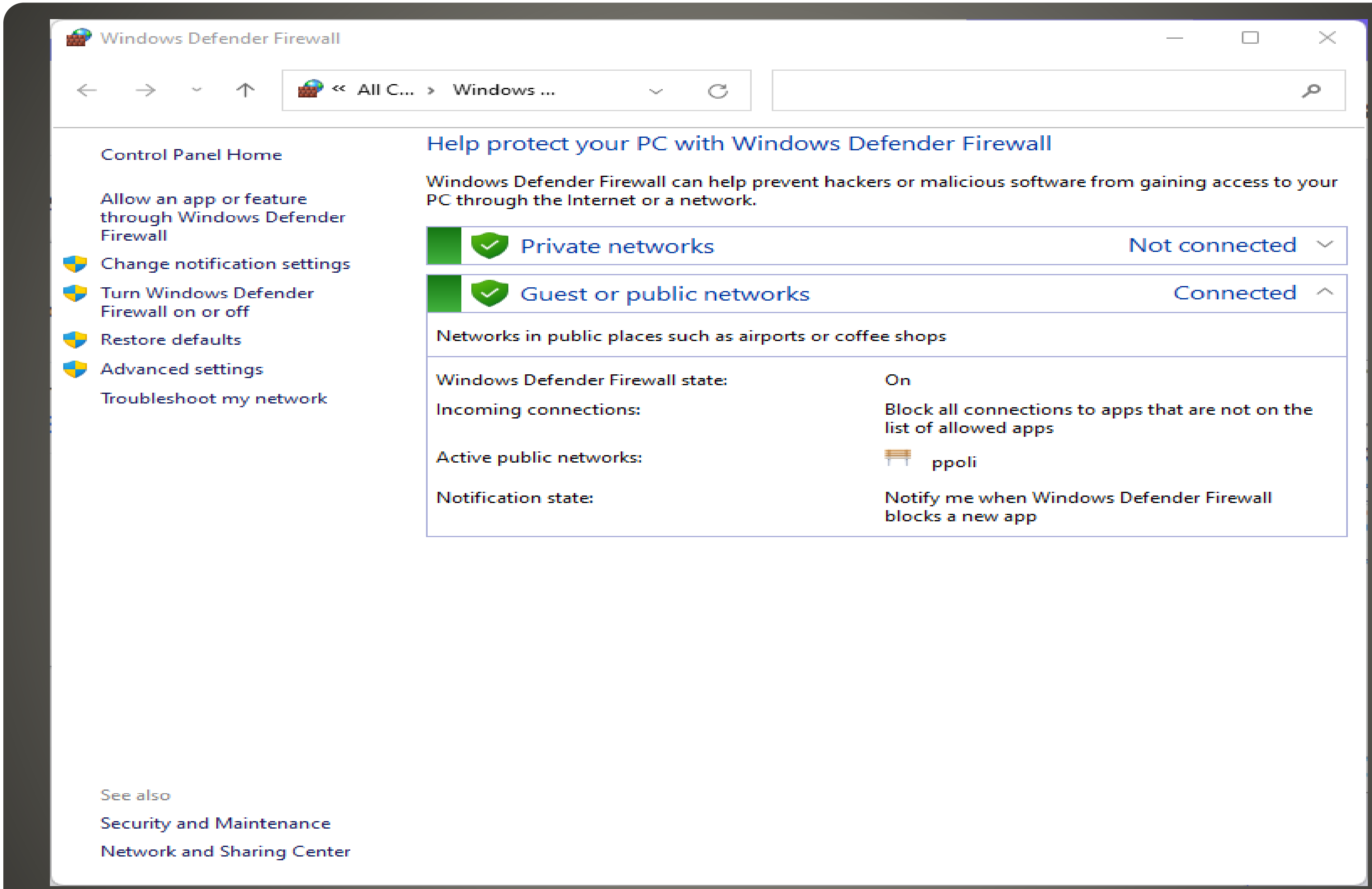
Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

These settings are being managed by vendor application ThreatTrack Security Firewall

Private networks — Not connected

Guest or public networks — Connected

Windows 10



Windows Defender Firewall

Control Panel Home

Allow an app or feature through Windows Defender Firewall

Change notification settings

Turn Windows Defender Firewall on or off

Restore defaults

Advanced settings

Troubleshoot my network

See also

Security and Maintenance

Network and Sharing Center

Help protect your PC with Windows Defender Firewall

Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Private networks — Not connected

Guest or public networks — Connected

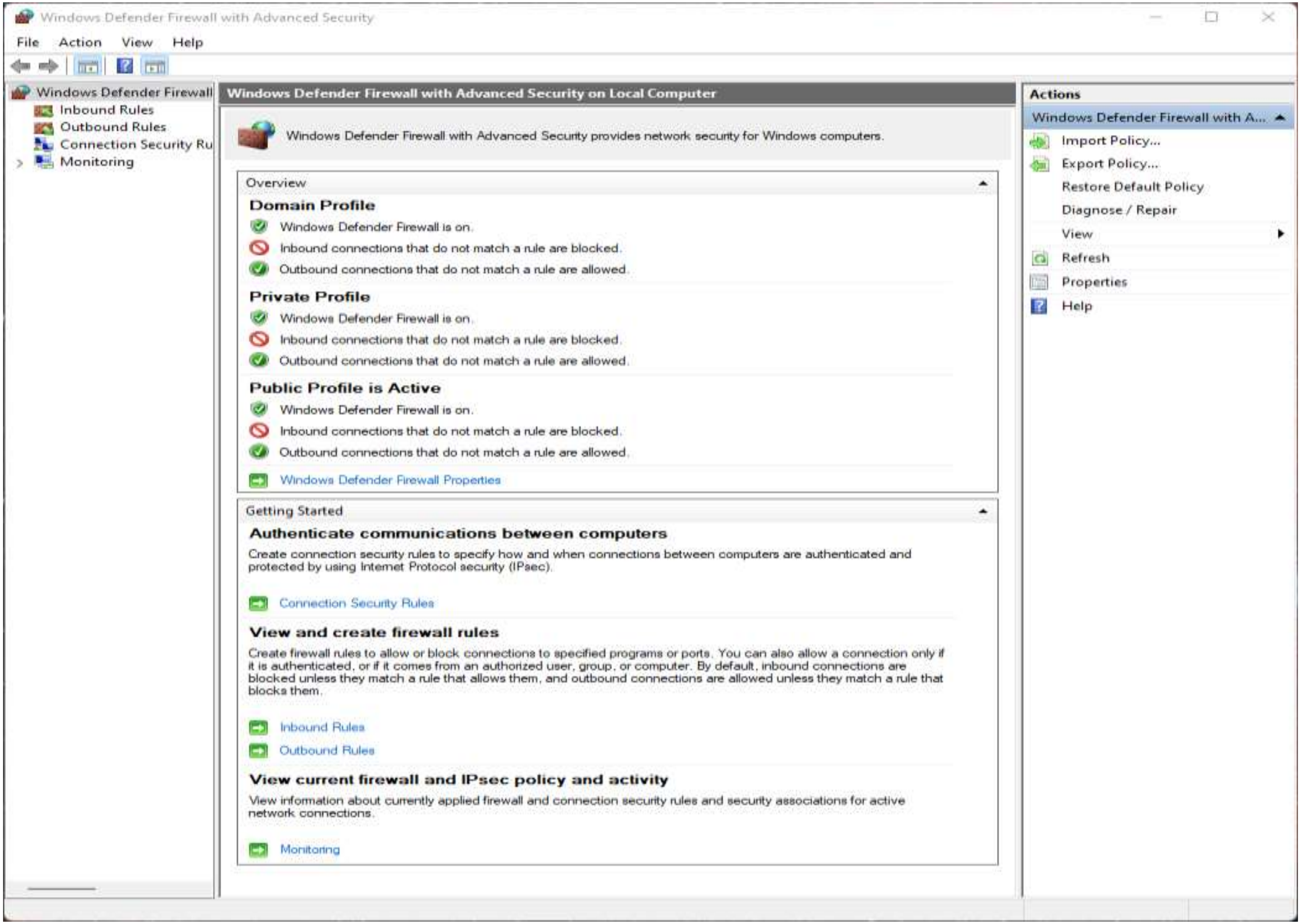
Networks in public places such as airports or coffee shops

Windows Defender Firewall state:	On
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active public networks:	ppoli
Notification state:	Notify me when Windows Defender Firewall blocks a new app

Windows 11

- Domain - Domain controller
- Private - home networks
- Public - Wi-Fi

Network Profiles



Windows Defender Firewall with Advanced Security on Local Computer

Windows Defender Firewall with Advanced Security provides network security for Windows computers.

Overview

Domain Profile

- ✓ Windows Defender Firewall is on.
- ⊘ Inbound connections that do not match a rule are blocked.
- ✓ Outbound connections that do not match a rule are allowed.

Private Profile

- ✓ Windows Defender Firewall is on.
- ⊘ Inbound connections that do not match a rule are blocked.
- ✓ Outbound connections that do not match a rule are allowed.

Public Profile is Active

- ✓ Windows Defender Firewall is on.
- ⊘ Inbound connections that do not match a rule are blocked.
- ✓ Outbound connections that do not match a rule are allowed.

Windows Defender Firewall Properties

Getting Started

Authenticate communications between computers

Create connection security rules to specify how and when connections between computers are authenticated and protected by using Internet Protocol security (IPsec).

Connection Security Rules

View and create firewall rules

Create firewall rules to allow or block connections to specified programs or ports. You can also allow a connection only if it is authenticated, or if it comes from an authorized user, group, or computer. By default, inbound connections are blocked unless they match a rule that allows them, and outbound connections are allowed unless they match a rule that blocks them.

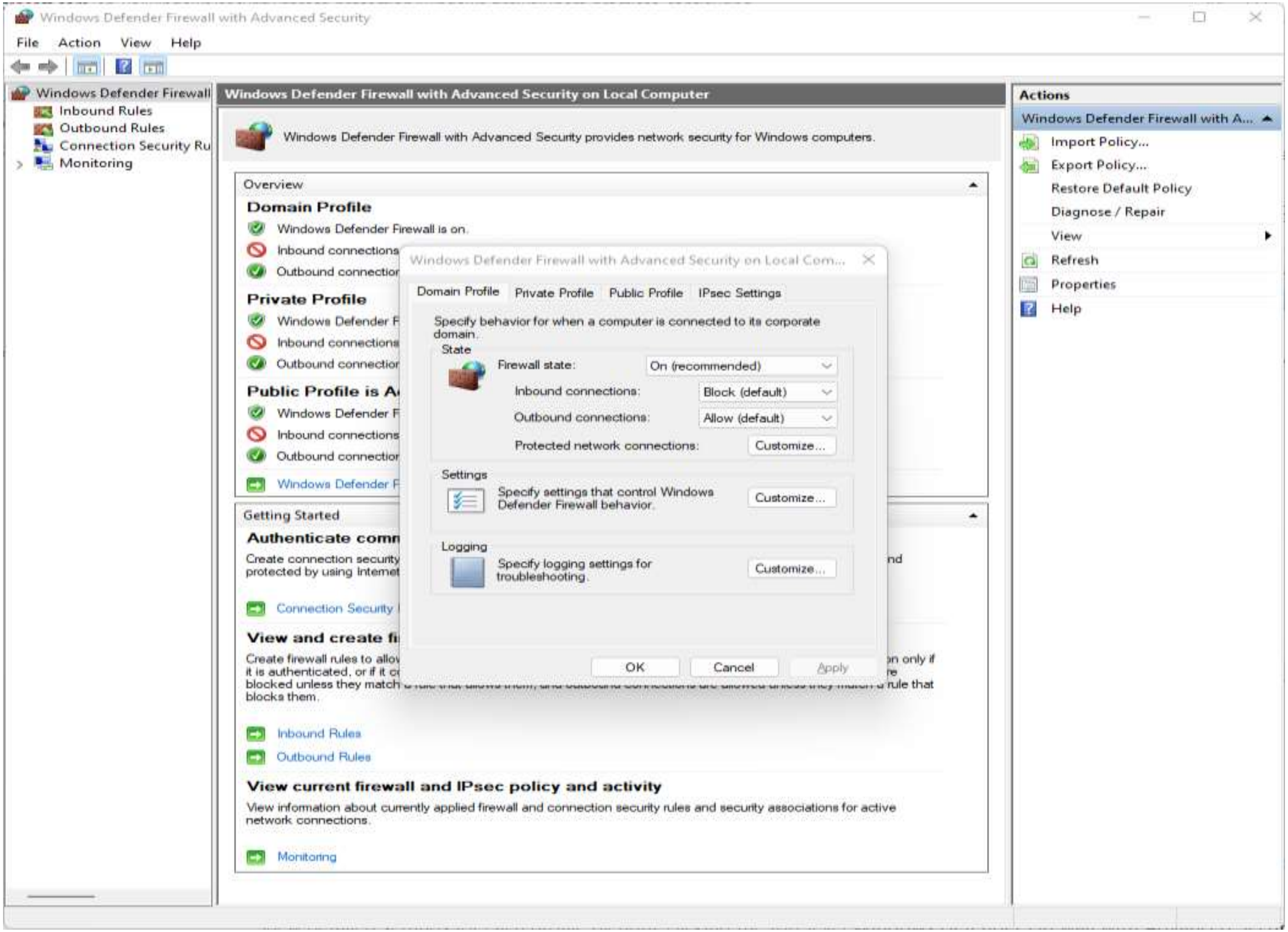
Inbound Rules

Outbound Rules

View current firewall and IPsec policy and activity

View information about currently applied firewall and connection security rules and security associations for active network connections.

Monitoring



Windows Defender Firewall with Advanced Security on Local Computer

Windows Defender Firewall with Advanced Security provides network security for Windows computers.

Overview

Domain Profile

Windows Defender Firewall is on.

Inbound connections

Outbound connectio

Private Profile

Windows Defender F

Inbound connections

Outbound connectio

Public Profile is A

Windows Defender F

Inbound connections

Outbound connectio

Windows Defender F

Getting Started

Authenticate comm

Create connection security … nd protected by using Internet

Connection Security

View and create fi

Create firewall rules to allow … on only if it is authenticated, or if it c… re blocked unless they match a rule that allows them, and outbound connections are allowed unless they match a rule that blocks them.

Inbound Rules

Outbound Rules

View current firewall and IPsec policy and activity

View information about currently applied firewall and connection security rules and security associations for active network connections.

Monitoring

Windows Defender Firewall with Advanced Security on Local Com...

Specify behavior for when a computer is connected to its corporate domain.

State

Firewall state: On (recommended)

Inbound connections: Block (default)

Outbound connections: Allow (default)

Protected network connections: Customize...

Settings

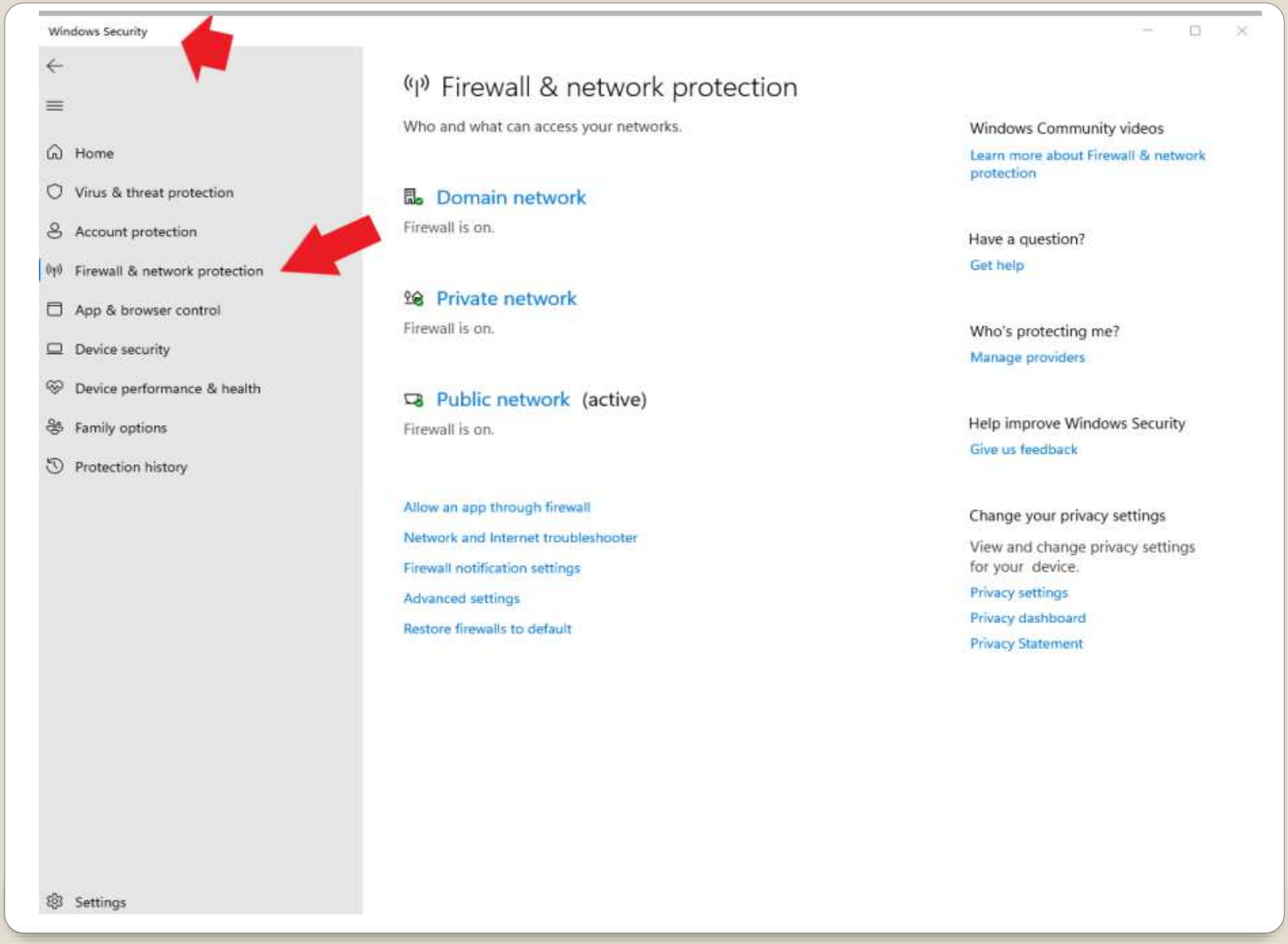
Specify settings that control Windows Defender Firewall behavior. Customize...

Logging

Specify logging settings for troubleshooting. Customize...

- Add rule or filter
- Need an app or feature currently blocked
- Think thrice
- Consider order rule precedence
- Document
- Test
- Temporarily enable logs
- AUDIT those logs
- Use logging with care

Windows Defender Firewall



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

Restore firewalls to default

Windows Community videos

Learn more about Firewall & network protection

Have a question?

Get help

Who's protecting me?

Manage providers

Help improve Windows Security

Give us feedback

Change your privacy settings

View and change privacy settings for your device.

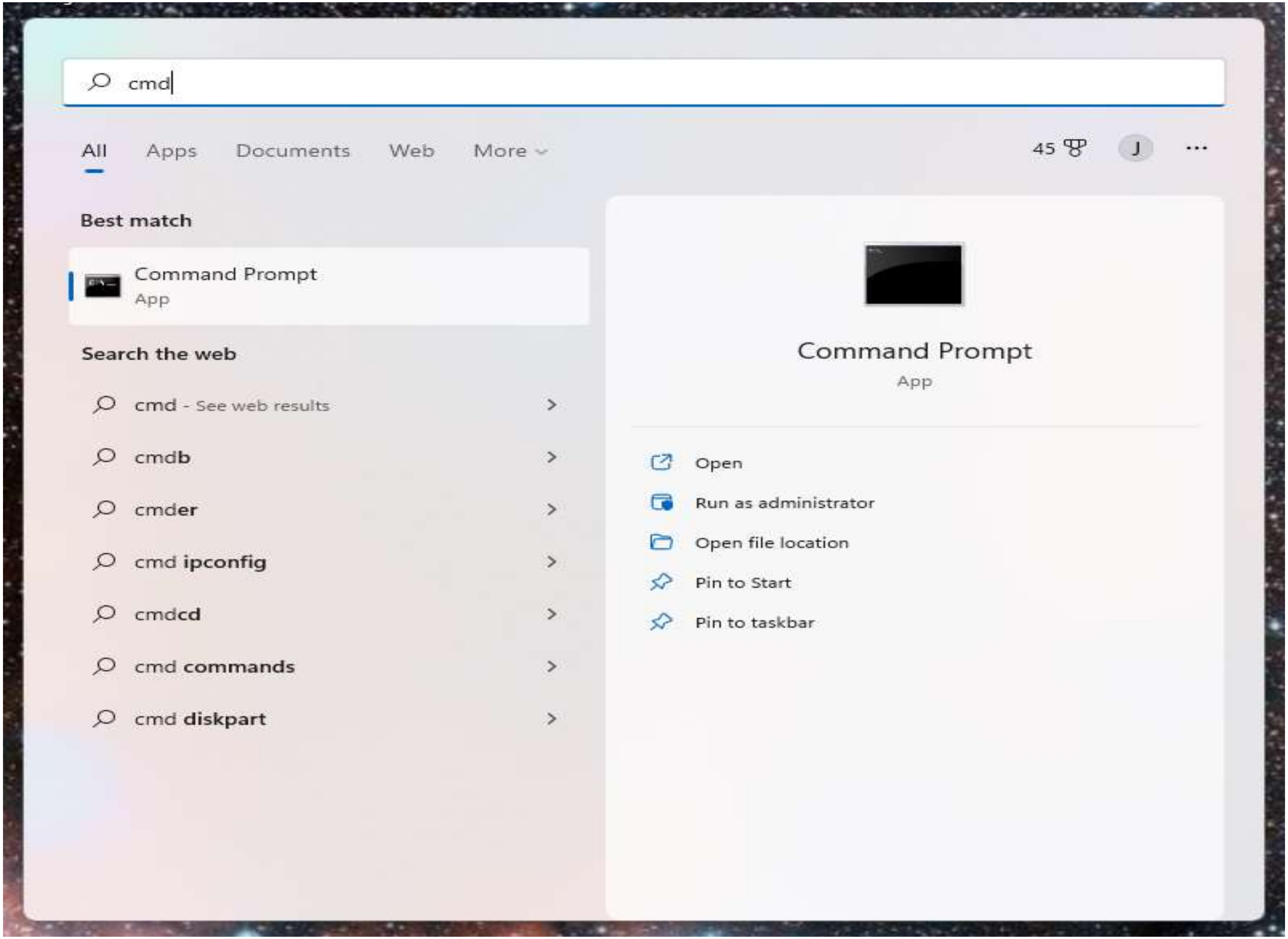
Privacy settings

Privacy dashboard

Privacy Statement

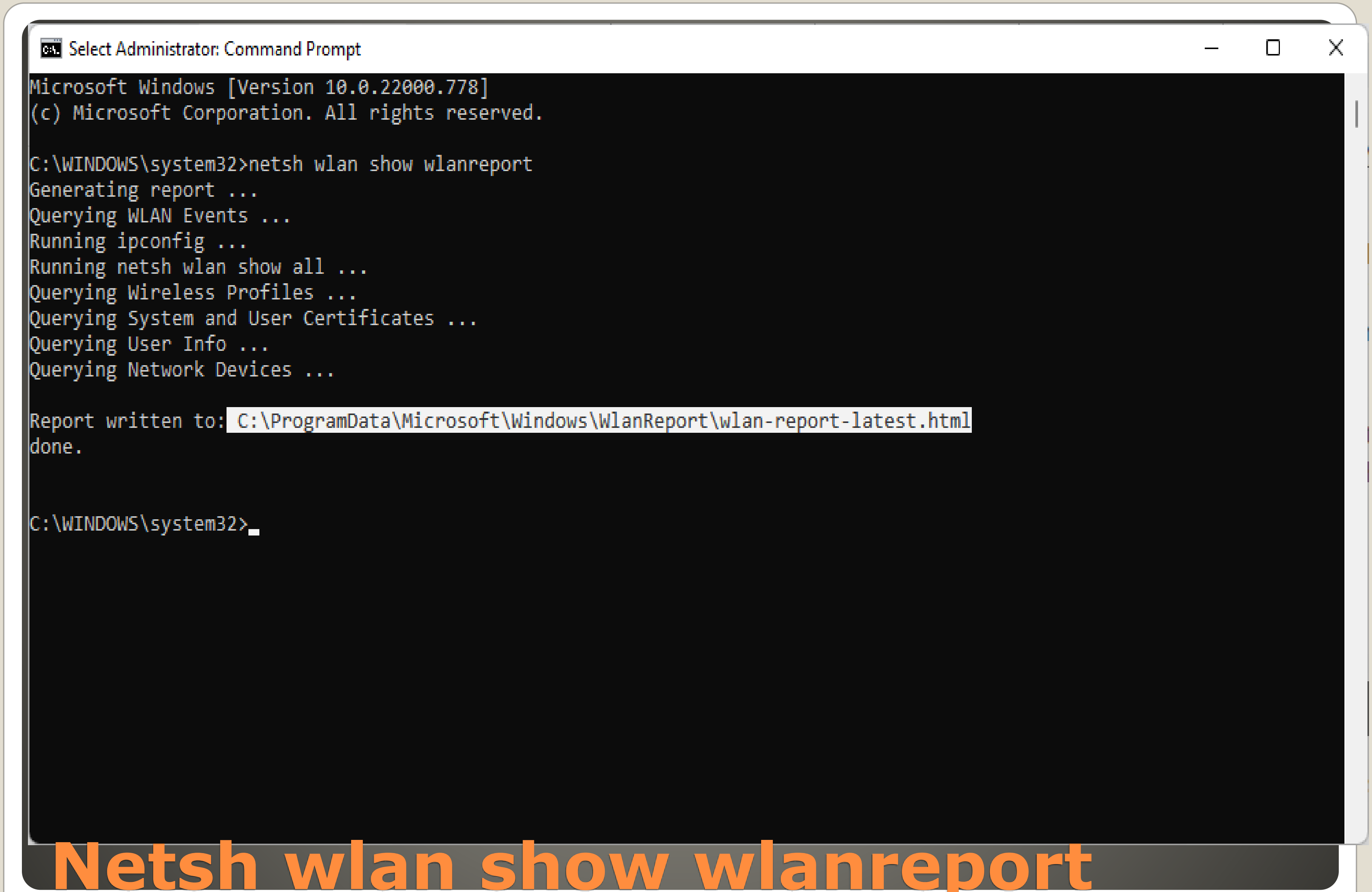
- A LOT of variables
- Radio
- CMD as Administrator

Wireless Woes?



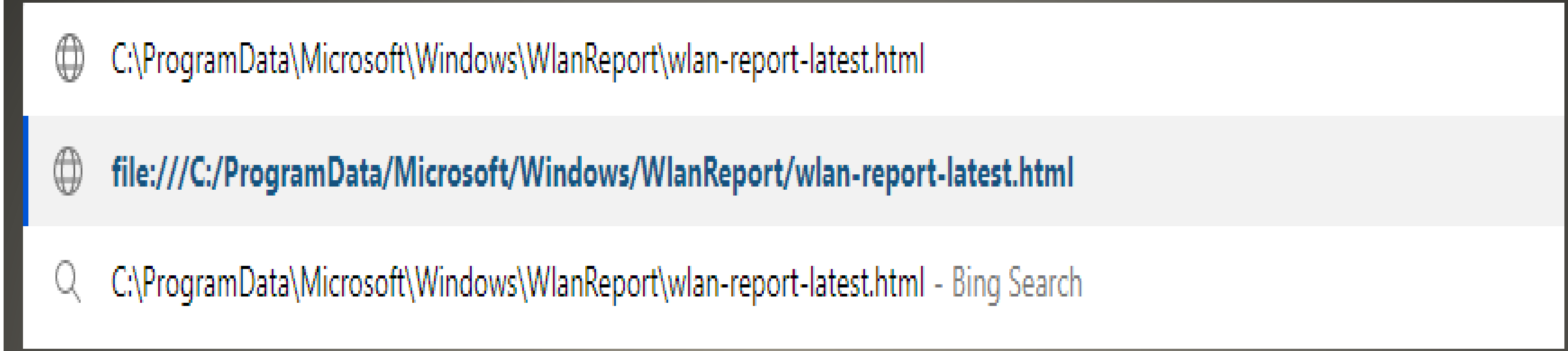
cmd

All
Apps
Documents
Web
More
45
J
Best match
Command Prompt
App
Search the web
cmd - See web results
cmdb
cmder
cmd ipconfig
cmdcd
cmd commands
cmd diskpart
Command Prompt
App
Open
Run as administrator
Open file location
Pin to Start
Pin to taskbar



```
Microsoft Windows [Version 10.0.22000.778]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>netsh wlan show wlanreport
Generating report ...
Querying WLAN Events ...
Running ipconfig ...
Running netsh wlan show all ...
Querying Wireless Profiles ...
Querying System and User Certificates ...
Querying User Info ...
Querying Network Devices ...

Report written to: C:\ProgramData\Microsoft\Windows\WlanReport\wlan-report-latest.html
done.


C:\WINDOWS\system32>_
```

Netsh wlan show wlanreport

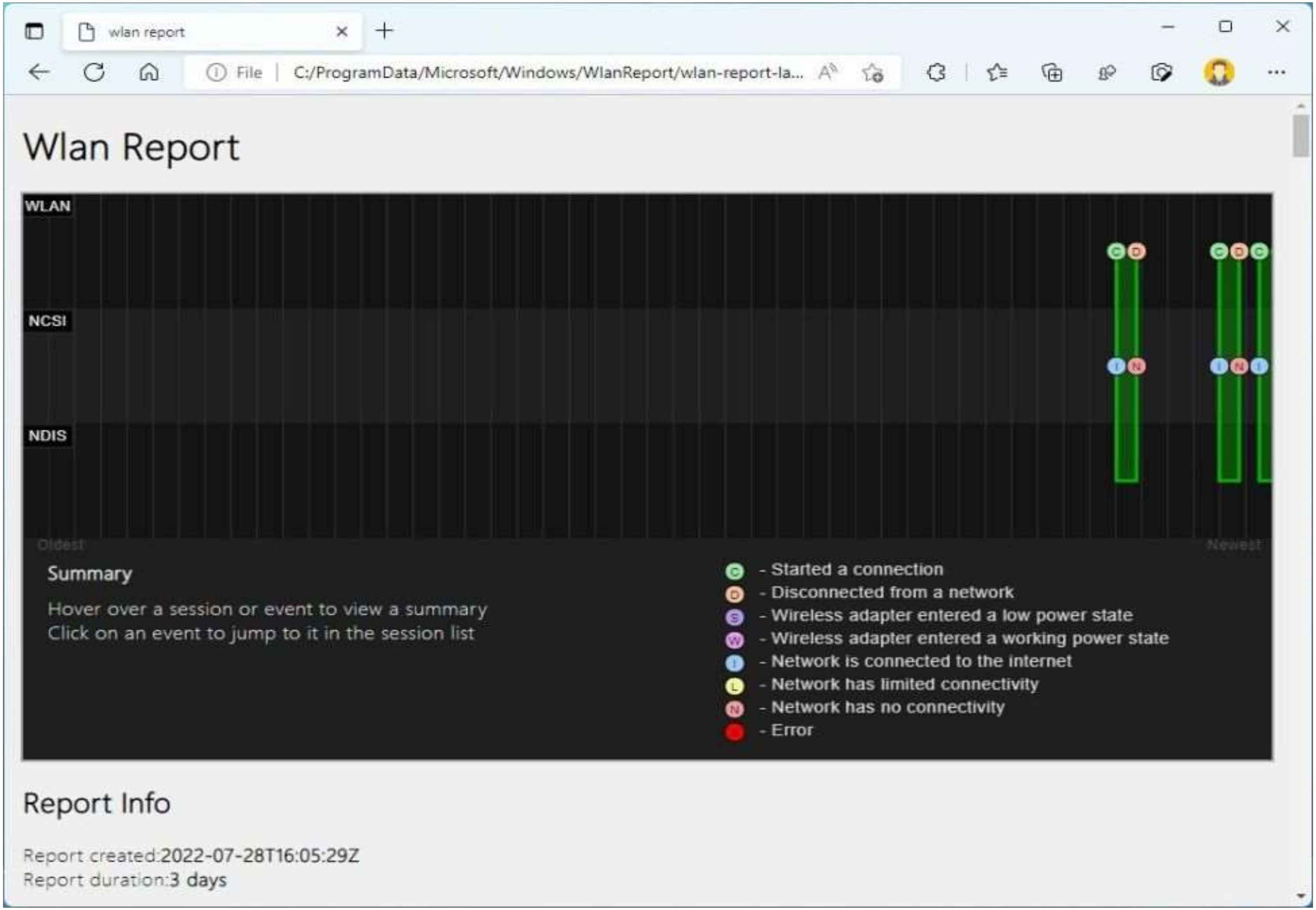


C:\ProgramData\Microsoft\Windows\WlanReport\wlan-report-latest.html

file:///C:/ProgramData/Microsoft/Windows/WlanReport/wlan-report-latest.html

C:\ProgramData\Microsoft\Windows\WlanReport\wlan-report-latest.html - Bing Search

Cut and Paste URL with file


wlan report
File
C:/ProgramData/Microsoft/Windows/WlanReport/wlan-report-la...
WLAN
NCSI
NDIS
Oldest
Newest

Wlan Report

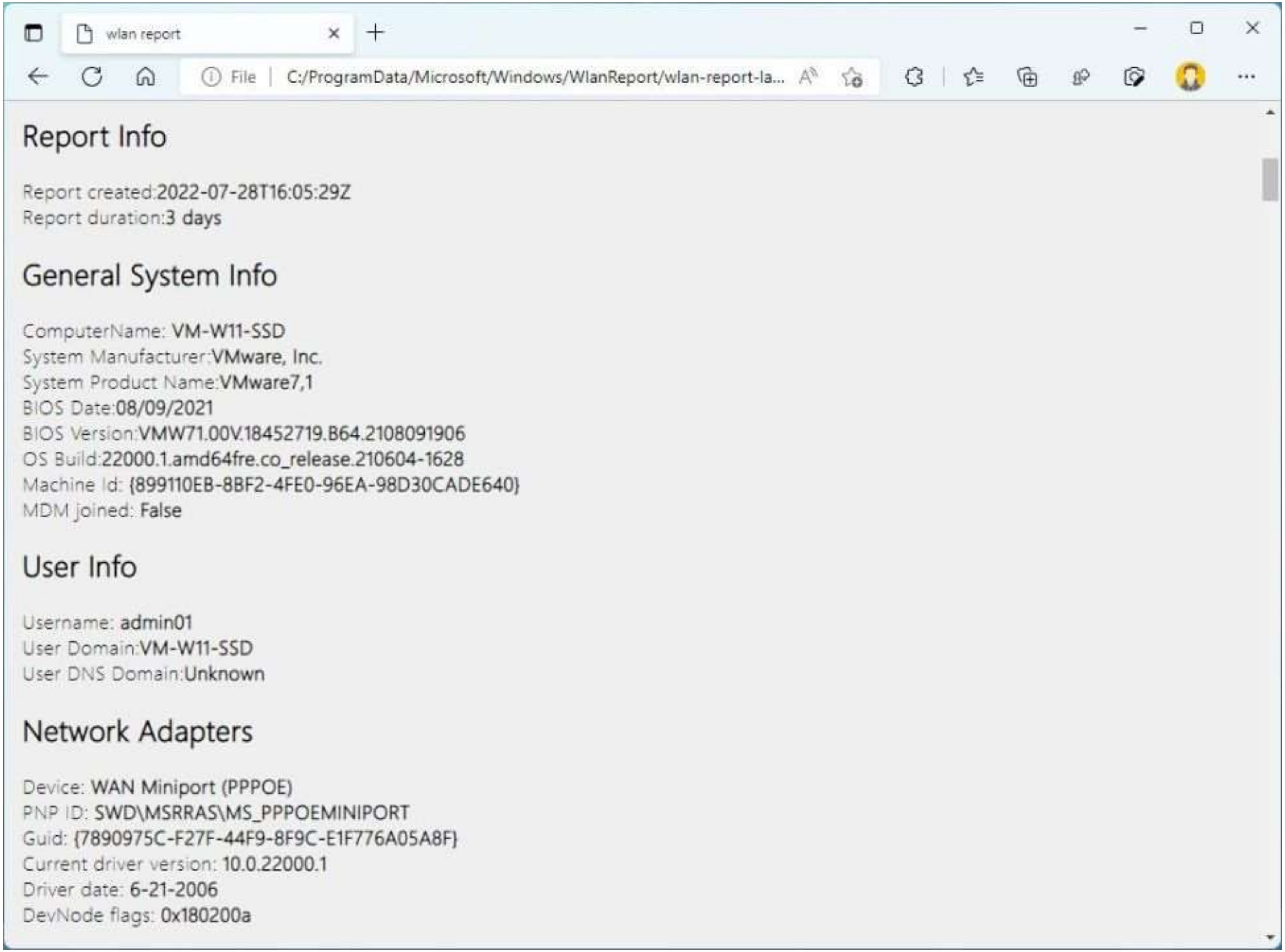
Summary

Hover over a session or event to view a summary
Click on an event to jump to it in the session list

C - Started a connection
D - Disconnected from a network
S - Wireless adapter entered a low power state
W - Wireless adapter entered a working power state
I - Network is connected to the internet
L - Network has limited connectivity
N - Network has no connectivity
● - Error

Report Info

Report created:2022-07-28T16:05:29Z
Report duration:3 days



wlan report
File
C:/ProgramData/Microsoft/Windows/WlanReport/wlan-report-la...

Report Info

Report created:2022-07-28T16:05:29Z
Report duration:3 days

General System Info

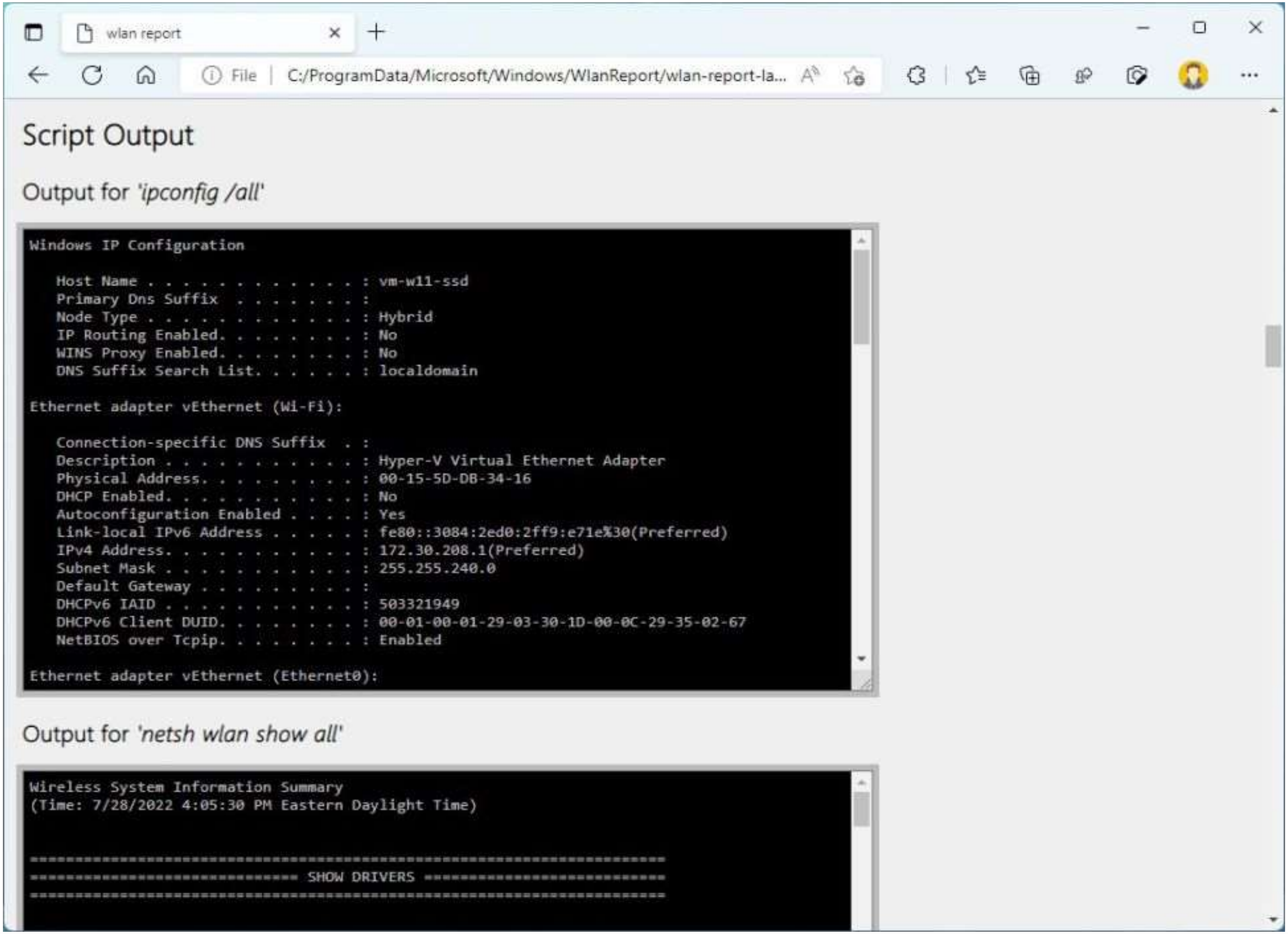
ComputerName: VM-W11-SSD
System Manufacturer:VMware, Inc.
System Product Name:VMware7,1
BIOS Date:08/09/2021
BIOS Version:VMW71.00V.18452719.B64.2108091906
OS Build:22000.1.amd64fre.co_release.210604-1628
Machine Id: {899110EB-8BF2-4FE0-96EA-98D30CADE640}
MDM joined: False

User Info

Username: admin01
User Domain:VM-W11-SSD
User DNS Domain:Unknown

Network Adapters

Device: WAN Miniport (PPPOE)
PNP ID: SWD\MSRRAS\MS_PPPOEMINIPORT
Guid: {7890975C-F27F-44F9-8F9C-E1F776A05A8F}
Current driver version: 10.0.22000.1
Driver date: 6-21-2006
DevNode flags: 0x180200a



wlan report
File
C:/ProgramData/Microsoft/Windows/WlanReport/wlan-report-la...

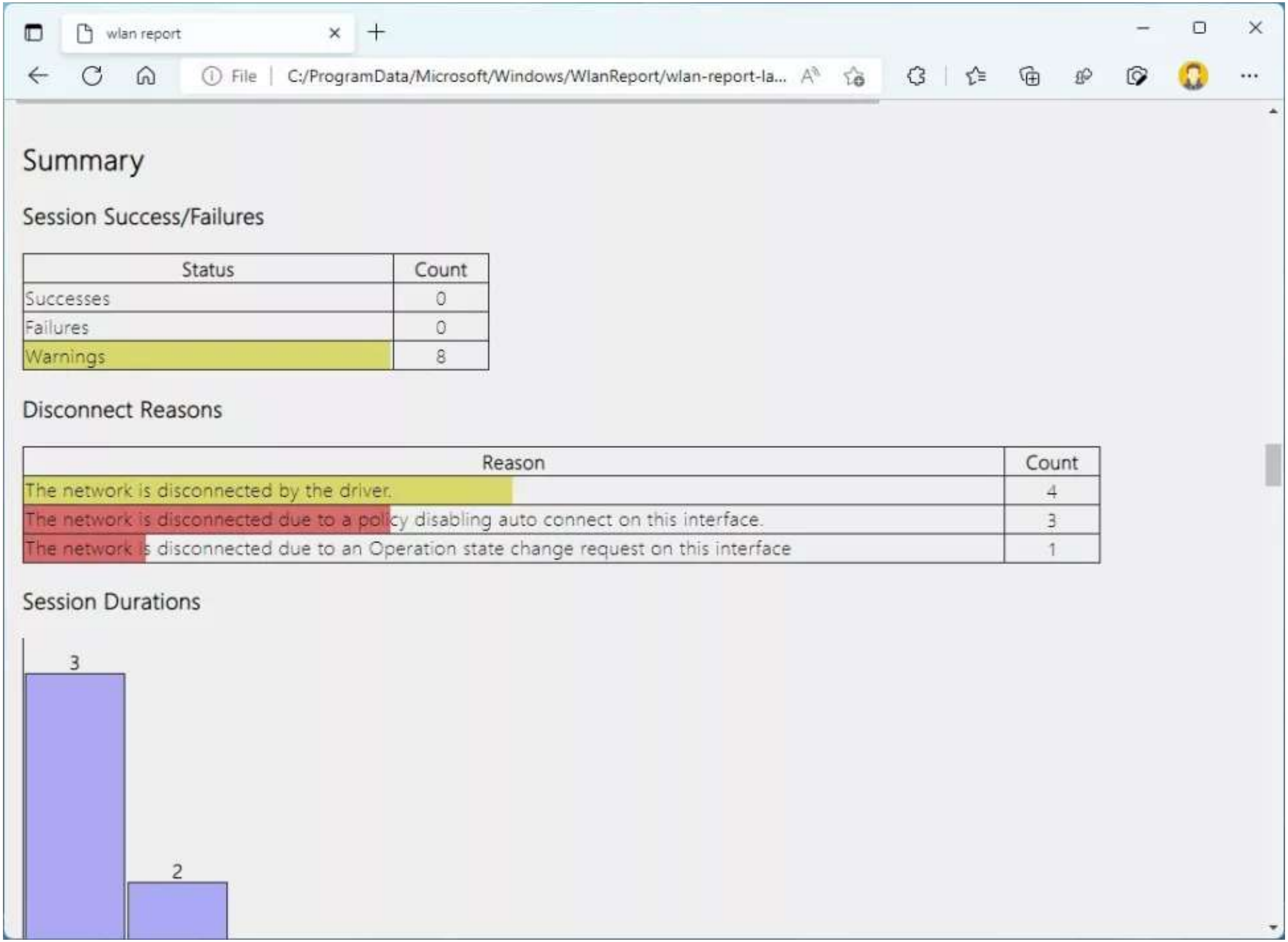
Script Output

Output for *'ipconfig /all'*

```
Windows IP Configuration

   Host Name . . . . . . . . . . . . : vm-w11-ssd
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : localdomain

Ethernet adapter vEthernet (Wi-Fi):

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Hyper-V Virtual Ethernet Adapter
   Physical Address. . . . . . . . . : 00-15-5D-DB-34-16
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::3084:2ed0:2ff9:e71e%30(Preferred)
   IPv4 Address. . . . . . . . . . . : 172.30.208.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 503321949
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-29-03-30-1D-00-0C-29-35-02-67
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter vEthernet (Ethernet0):
```

Output for *'netsh wlan show all'*

```
Wireless System Information Summary
(Time: 7/28/2022 4:05:30 PM Eastern Daylight Time)


=======================================================================
============================== SHOW DRIVERS ===========================
=======================================================================
```



wlan report
File
C:/ProgramData/Microsoft/Windows/WlanReport/wlan-report-la...

Summary

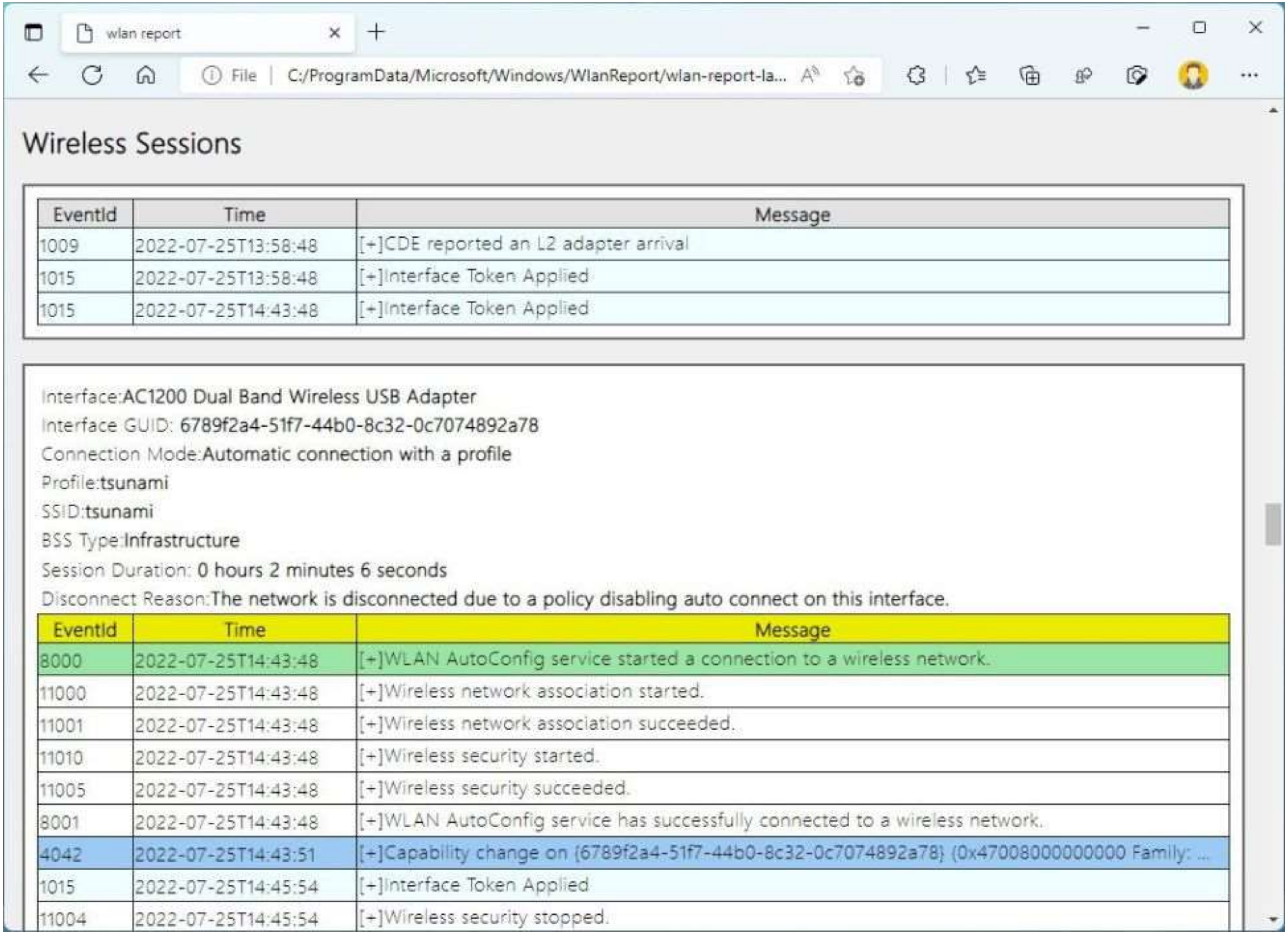
Session Success/Failures

Status	Count
Successes	0
Failures	0
Warnings	8

Disconnect Reasons

Reason	Count
The network is disconnected by the driver.	4
The network is disconnected due to a policy disabling auto connect on this interface.	3
The network is disconnected due to an Operation state change request on this interface	1

Session Durations


wlan report
File
C:/ProgramData/Microsoft/Windows/WlanReport/wlan-report-la...

Wireless Sessions

EventId	Time	Message
1009	2022-07-25T13:58:48	[+]CDE reported an L2 adapter arrival
1015	2022-07-25T13:58:48	[+]Interface Token Applied
1015	2022-07-25T14:43:48	[+]Interface Token Applied

Interface:AC1200 Dual Band Wireless USB Adapter
Interface GUID: 6789f2a4-51f7-44b0-8c32-0c7074892a78
Connection Mode:Automatic connection with a profile
Profile:tsunami
SSID:tsunami
BSS Type:Infrastructure
Session Duration: 0 hours 2 minutes 6 seconds
Disconnect Reason:The network is disconnected due to a policy disabling auto connect on this interface.

EventId	Time	Message
8000	2022-07-25T14:43:48	[+]WLAN AutoConfig service started a connection to a wireless network.
11000	2022-07-25T14:43:48	[+]Wireless network association started.
11001	2022-07-25T14:43:48	[+]Wireless network association succeeded.
11010	2022-07-25T14:43:48	[+]Wireless security started.
11005	2022-07-25T14:43:48	[+]Wireless security succeeded.
8001	2022-07-25T14:43:48	[+]WLAN AutoConfig service has successfully connected to a wireless network.
4042	2022-07-25T14:43:51	[+]Capability change on {6789f2a4-51f7-44b0-8c32-0c7074892a78} (0x47008000000000 Family: ...
1015	2022-07-25T14:45:54	[+]Interface Token Applied
11004	2022-07-25T14:45:54	[+]Wireless security stopped.

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