

Windows 10 checklist

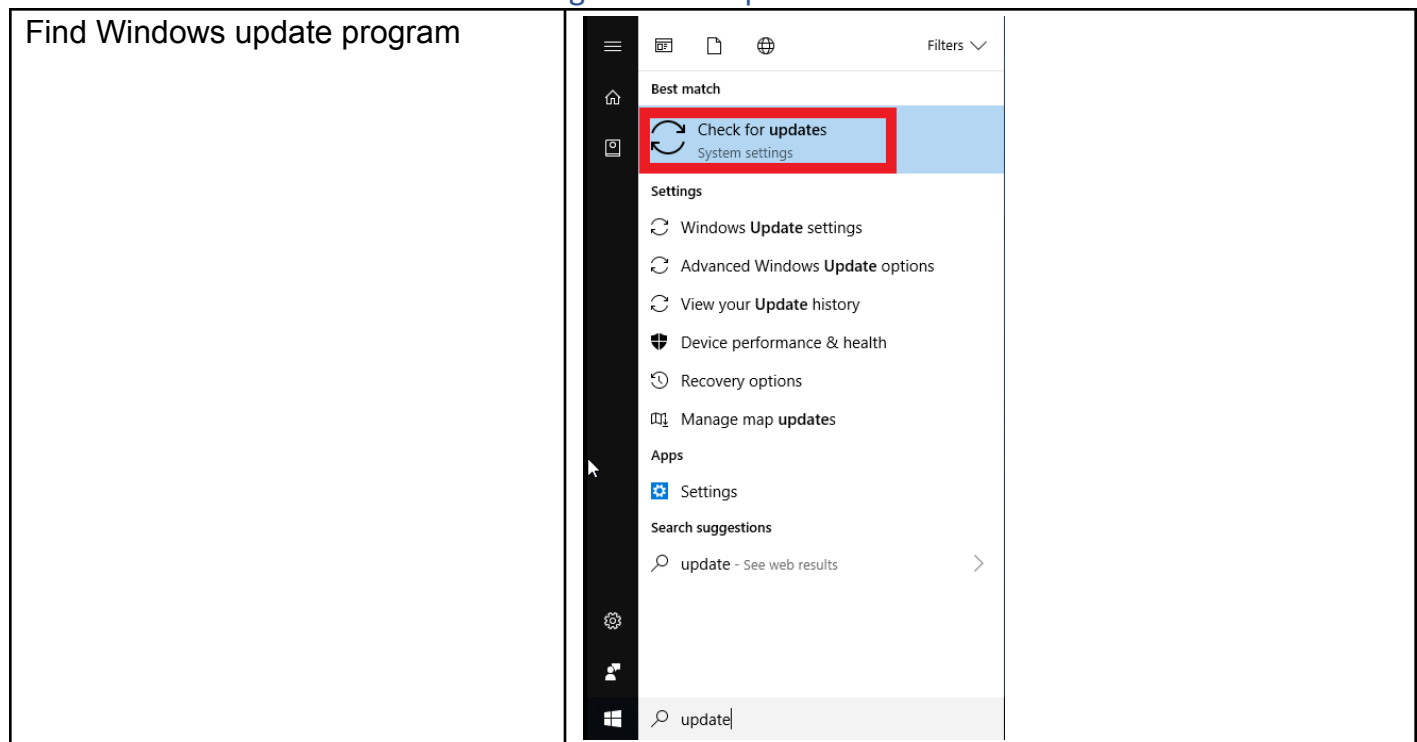
Table of contents

Topic	Page number
checklist	1
Windows updates	2
Firefox updates	3
Disabling users	4-5
Changing user groups	8
disabling services	9-10
Removing hidden unwanted content	11-12
Turning on Windows firewall	13-14
changing user account control settings	15
setting password policy	16-18
setting lockout policy	19
audit policy	20-21
firewall rules	22

1. Readme
2. Check and perform updates for Windows and all programs
3. Check authorized users and admins against readme and disable violators
4. Give all normal users a strong password, but write it down, and use a password generator to make it
5. Remove programs that shouldn't be there
6. Disable unneeded services
7. Remove ban content (Movies, videos, pictures, etc.)
8. Enable firewall
9. Set user account control to high
10. Set password policy
11. Set lockout policy
12. Set adult policy
13. Disable some firewall rules

14. Run / enable Windows Defender scans
15. Look for suspicious programs running in the background and remove them
16. Look for suspicious listening ports and remove them

Checking windows updates



Click check for updates now, if there are any, install and restart your computer

Windows Update



You're up to date

Last checked: Yesterday, 5:35 PM

Check for updates

[Change active hours](#)

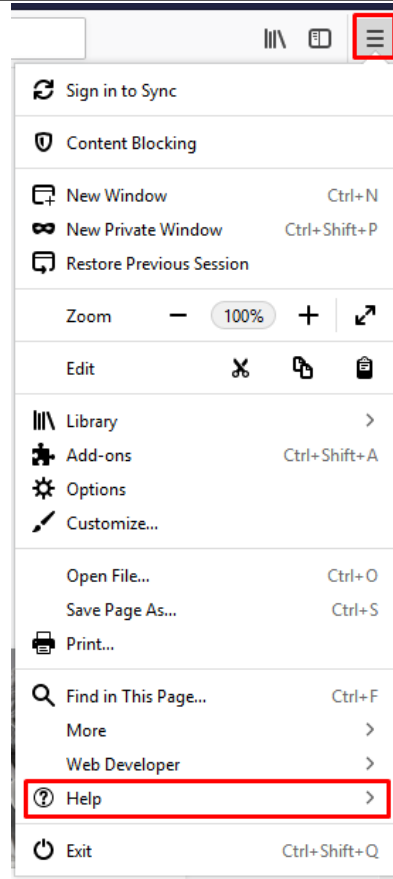
[View update history](#)

[Advanced options](#)

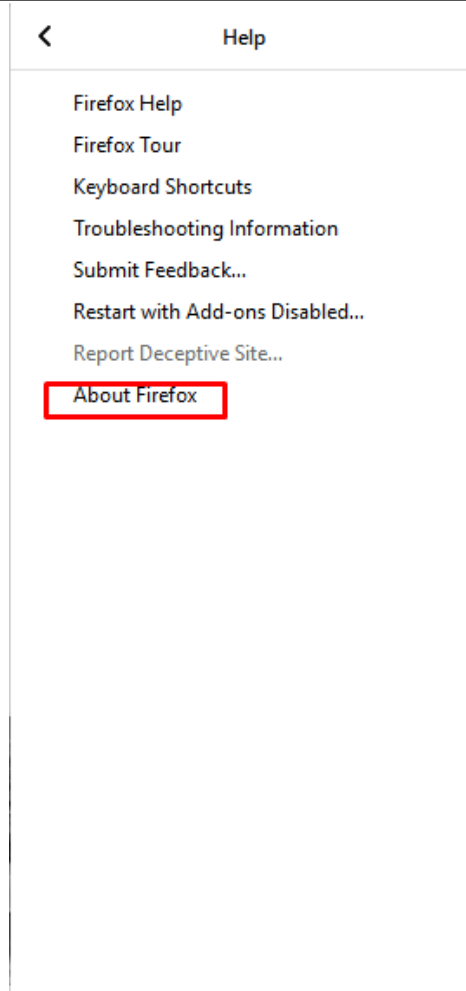
Checking Firefox updates

Click the three bars on the side in Firefox

Then click help



click about Firefox

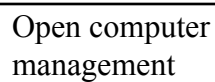


Here it will show you if your browser is up to date or not and will give you a download link if it isn't

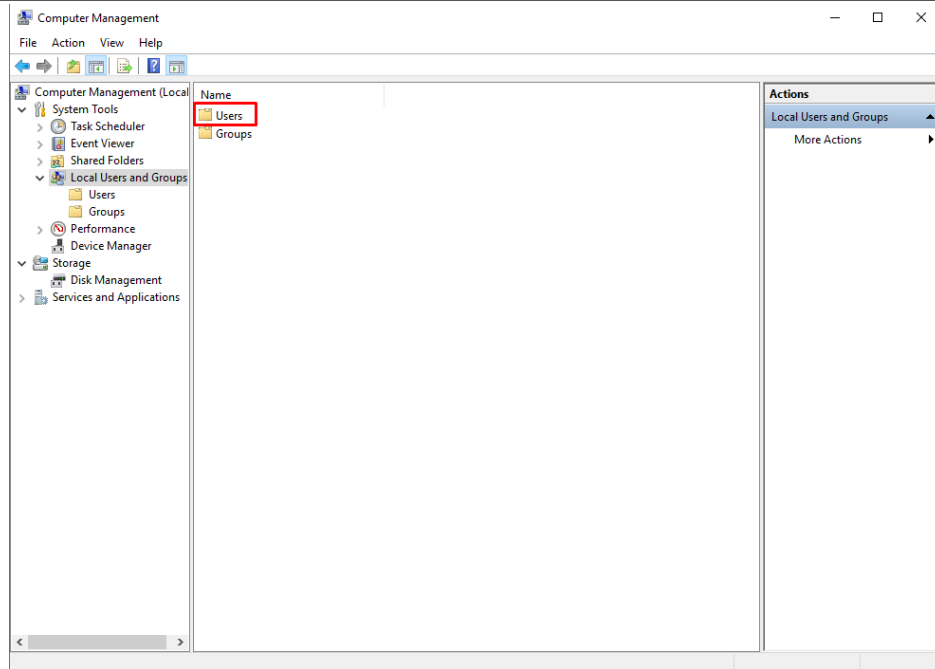
Note that I already have the latest version at the time



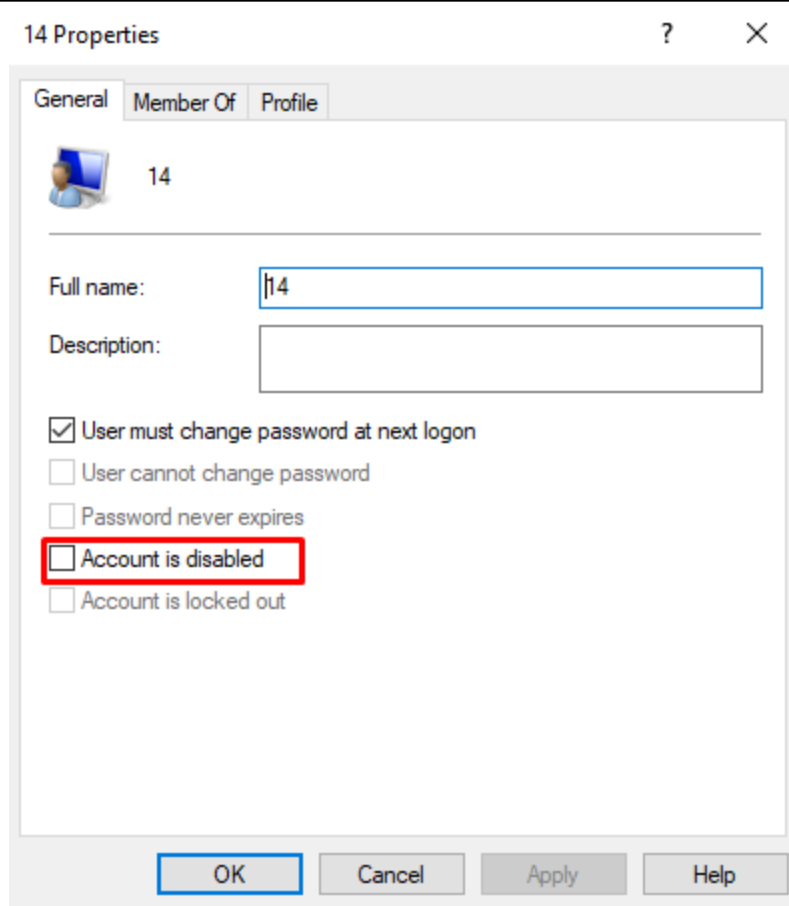
Go to
administrative tools



Click local users and groups and click users and click the account you want to disable



check account is disabled and apply



Moving groups

Go to the “Member Of” tab and type the user group you want to put them in

Select Groups

Select this object type:

Groups

Object Types...

From this location:

DESKTOP-MUQ8RT6

Locations...

Enter the object names to select (examples):

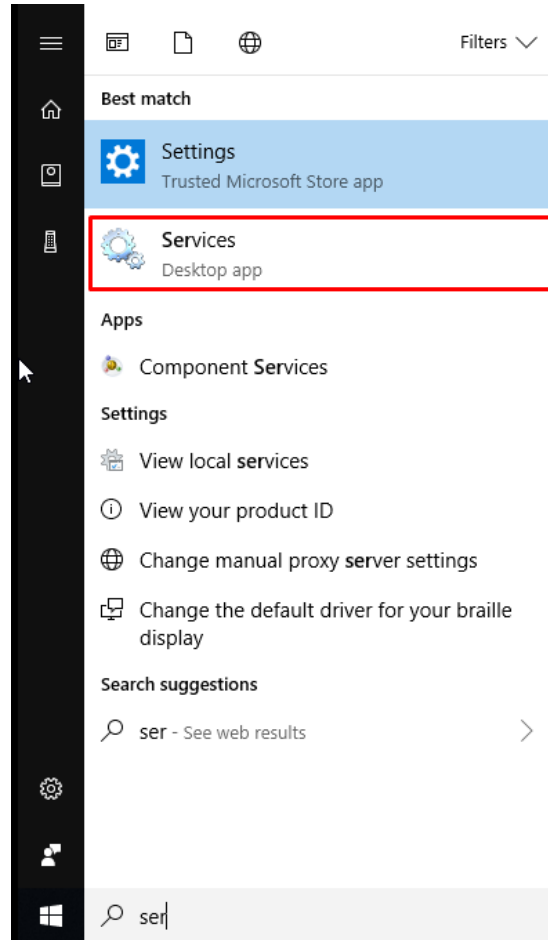
administrators

Check Names

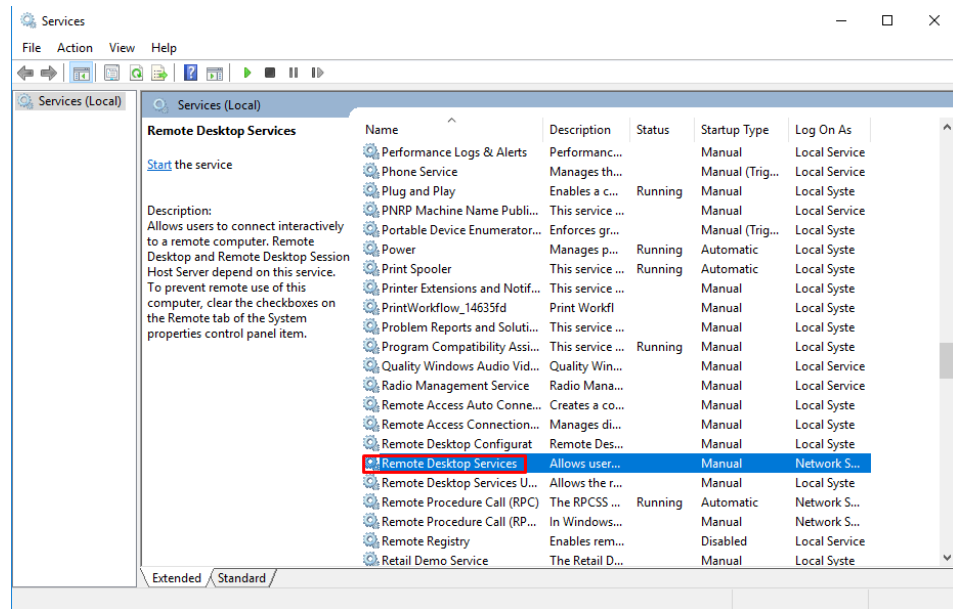
Advanced... OK Cancel

Disabling services

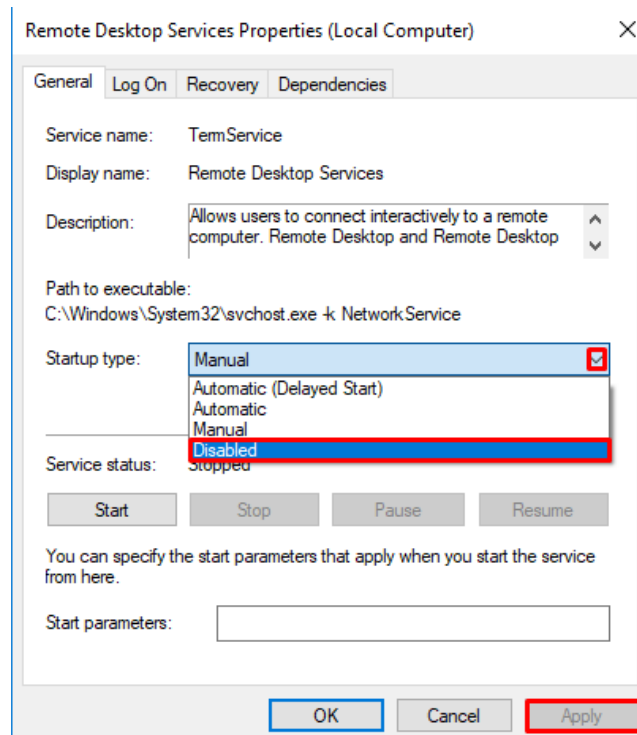
Go to the services program



find the service
you want to disable
and click on it

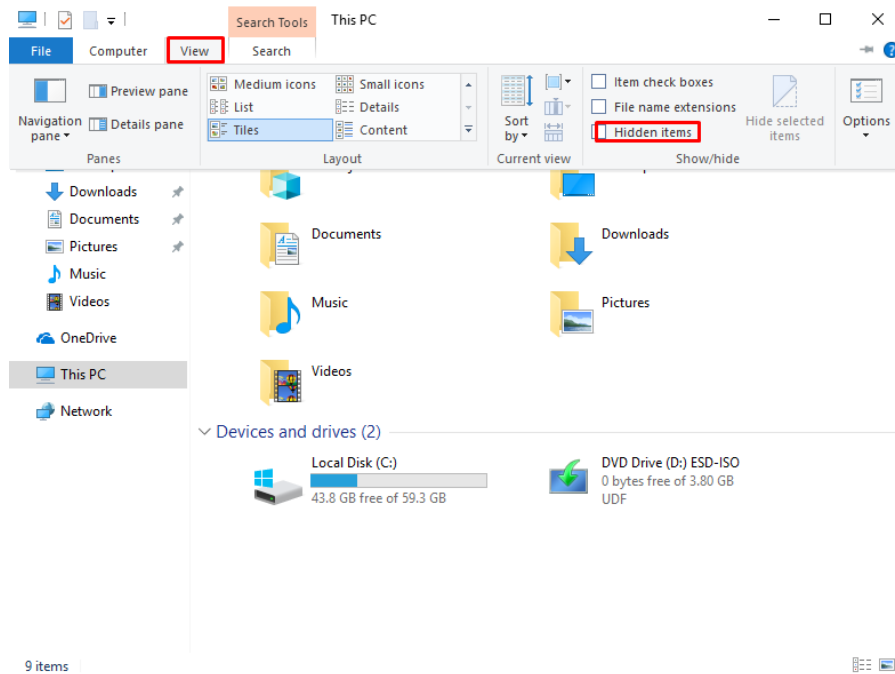


select disabled
from the drop
down menu and
then click apply



Removing hidden unwanted software

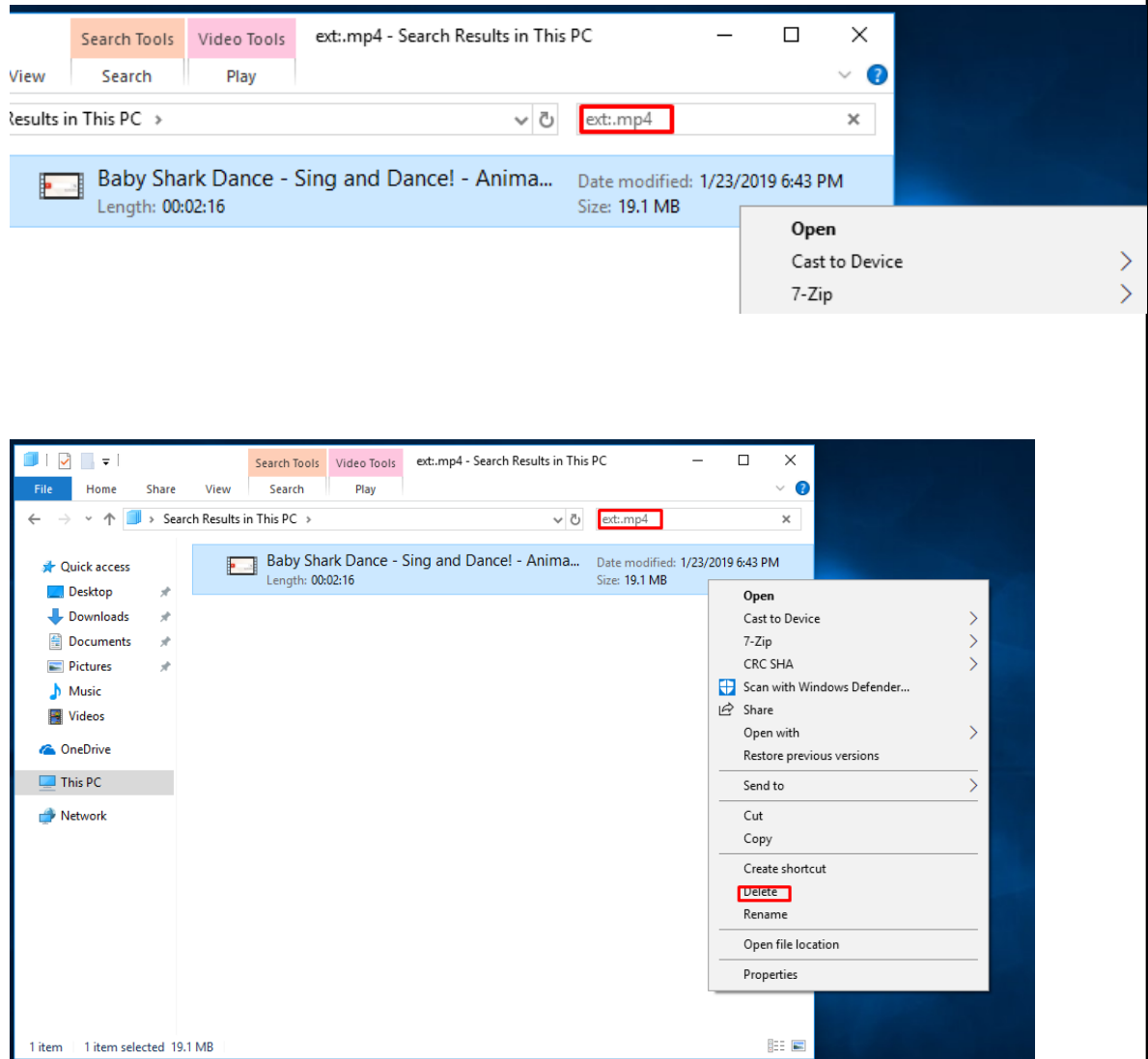
In the file explorer, go to This PC and then go to the view tab, in this tab select “show hidden items” box



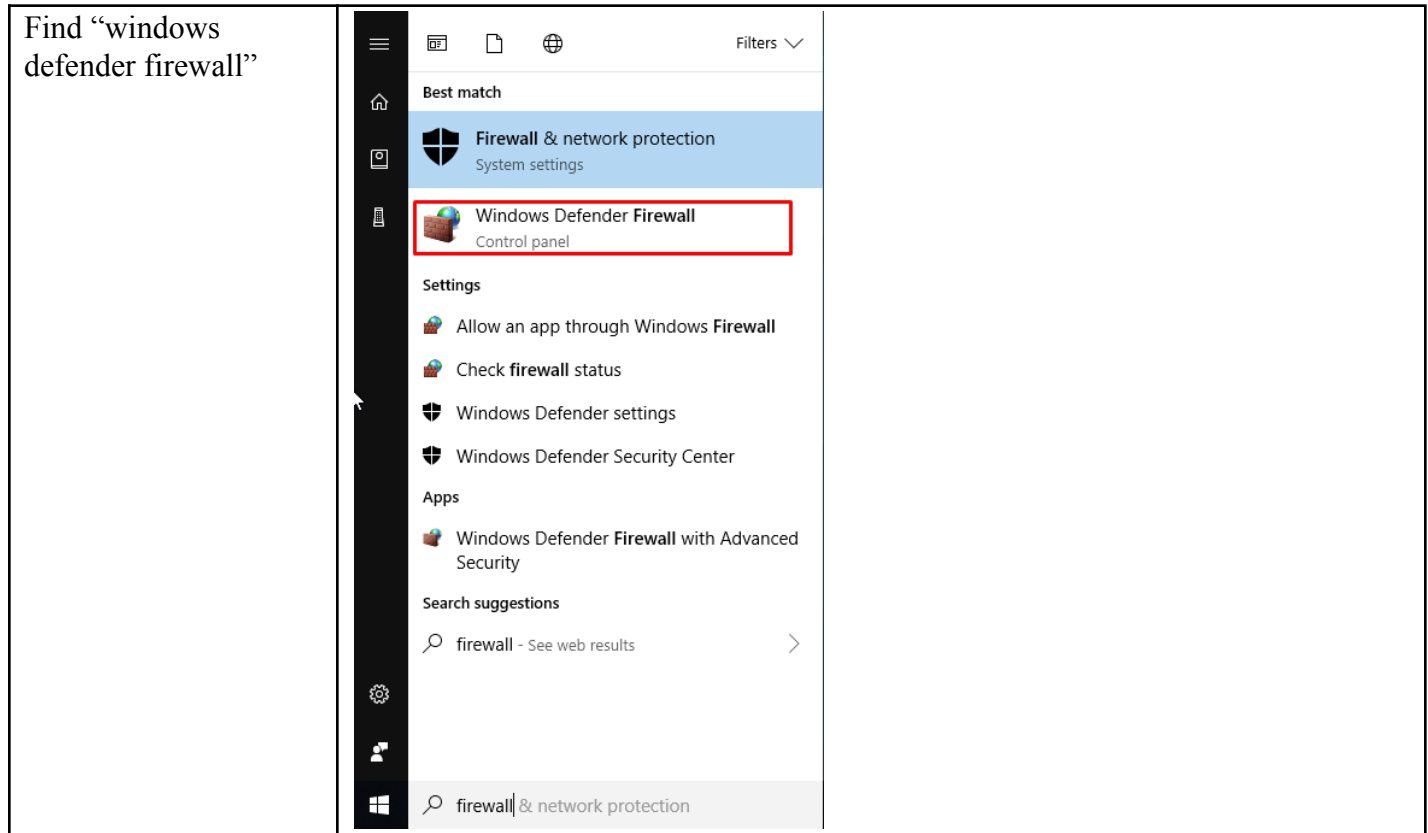
After you do that step, type “ext:FILETIPE” and search

If any kind of ban content comes up, right-click and delete it

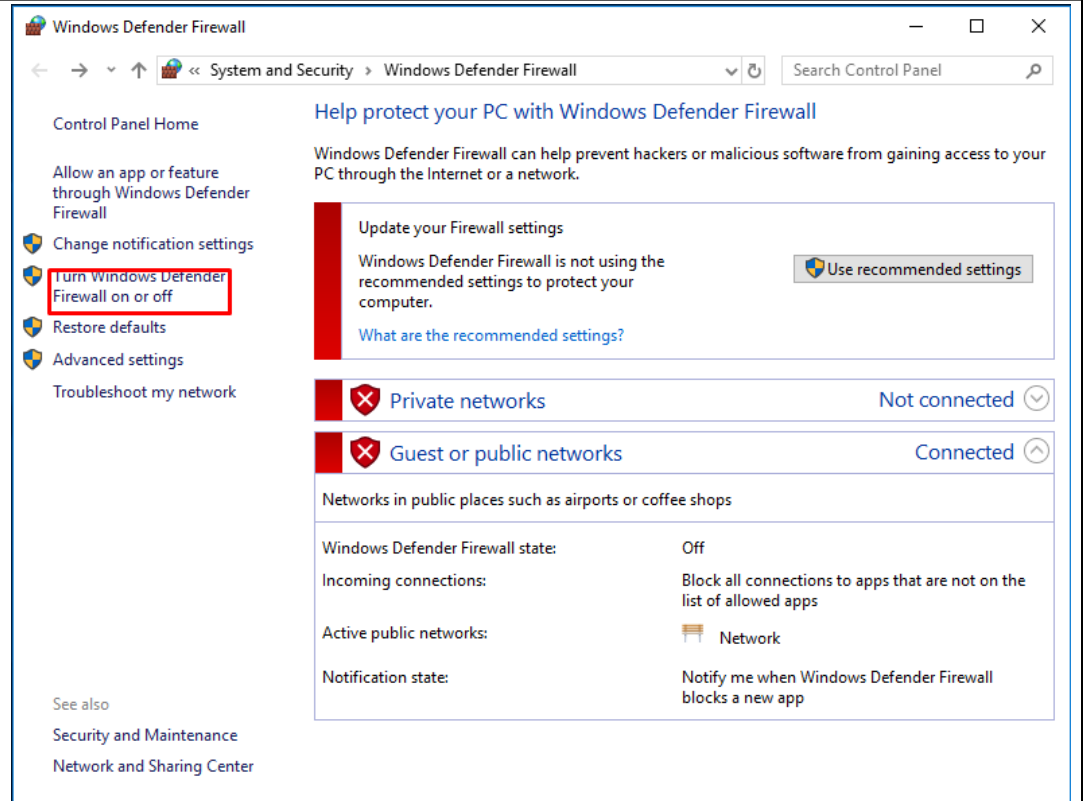
** replace FILETIPE with the extension of the file you want to find



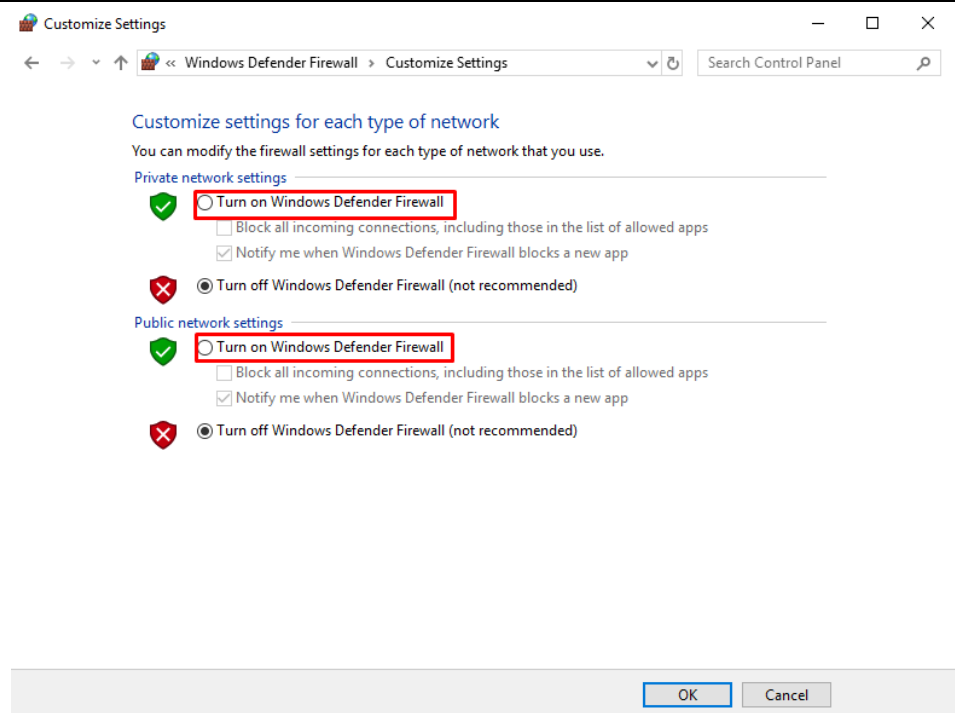
Turing on windows firewall



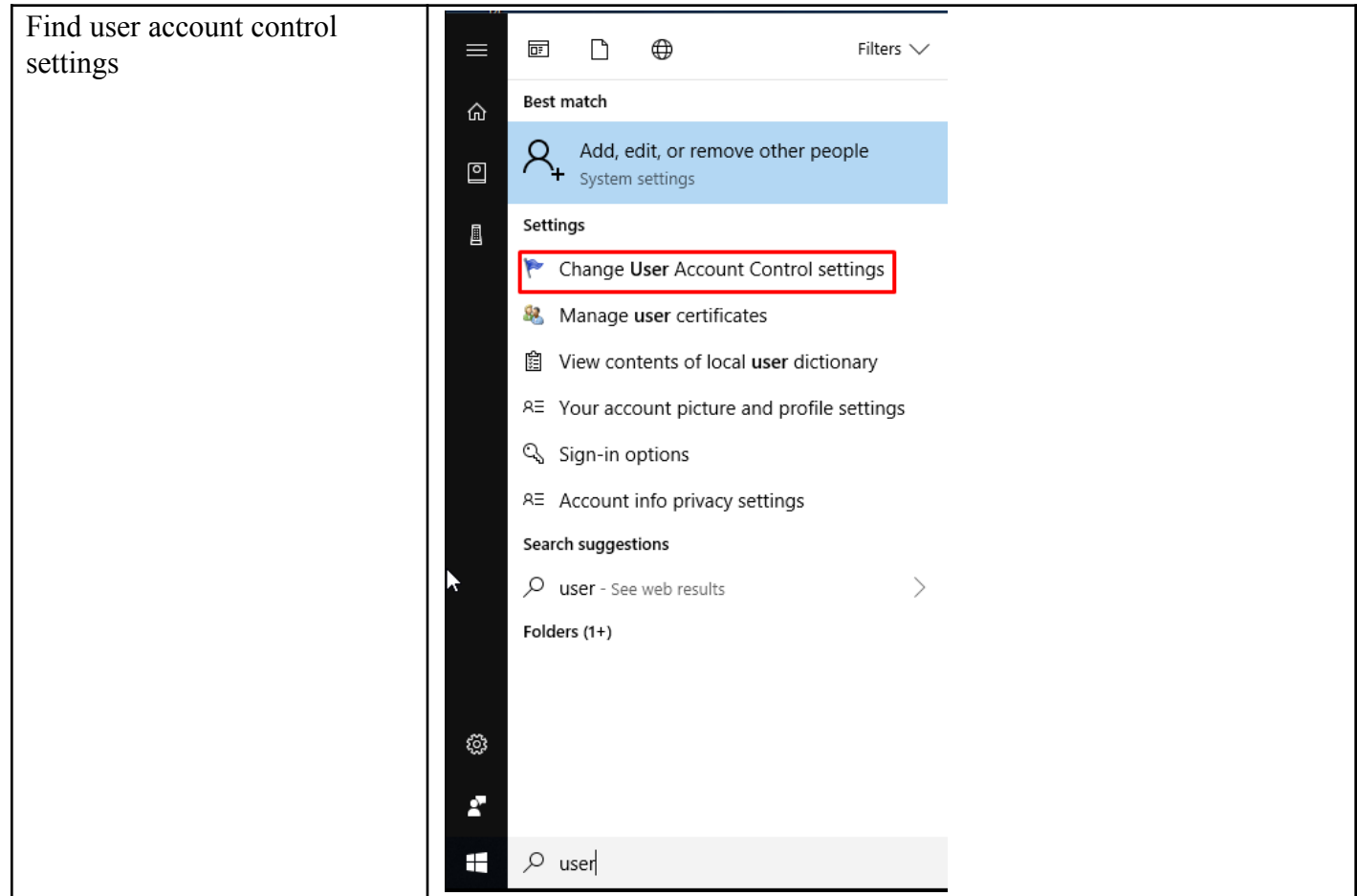
Select “turn windows defender firewall on or off”



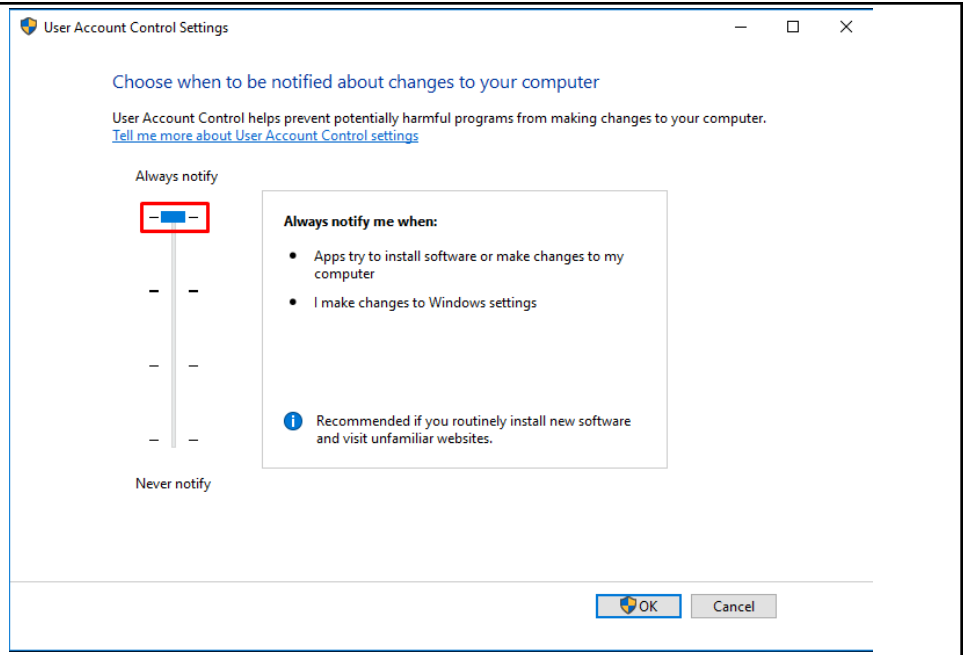
select turn on windows defender firewall on both the public and private network



changing user account control settings

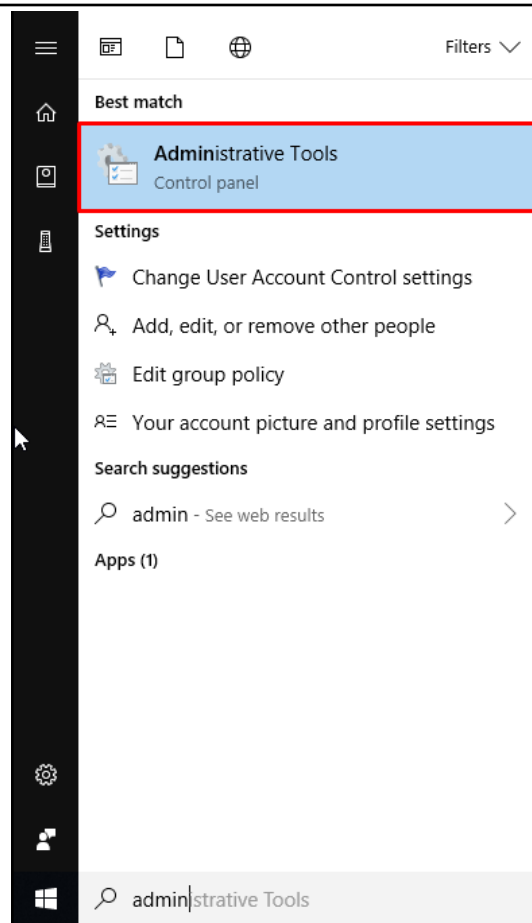


set it to the highest level and apply changes

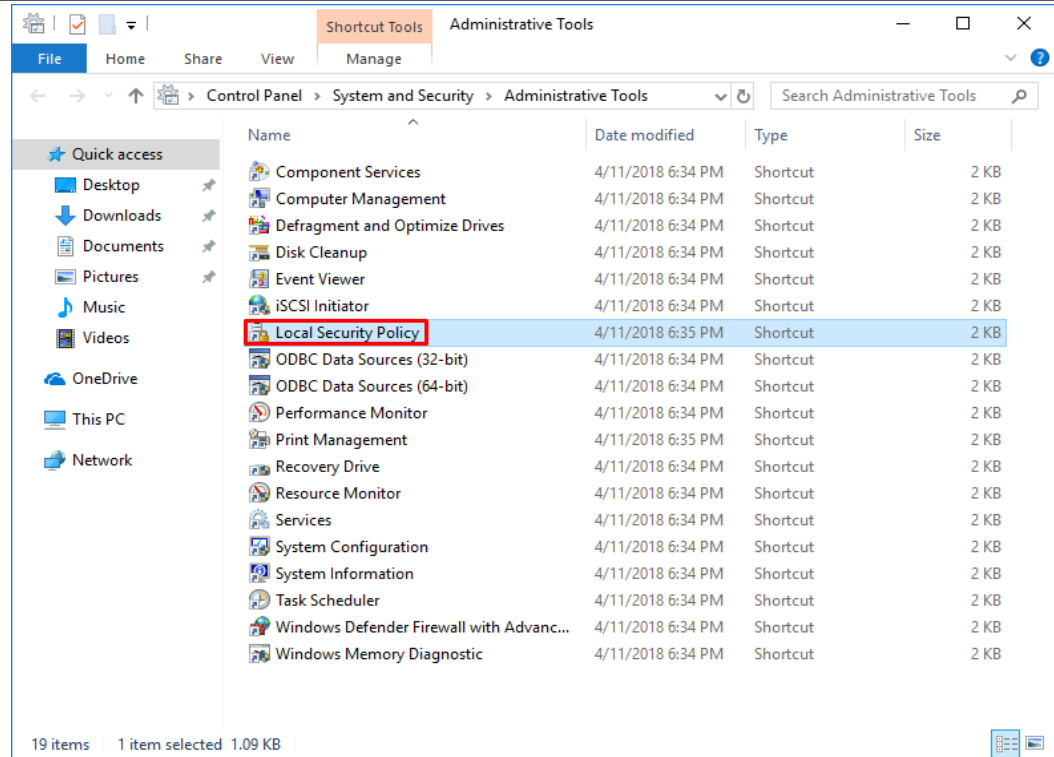


Setting password policy

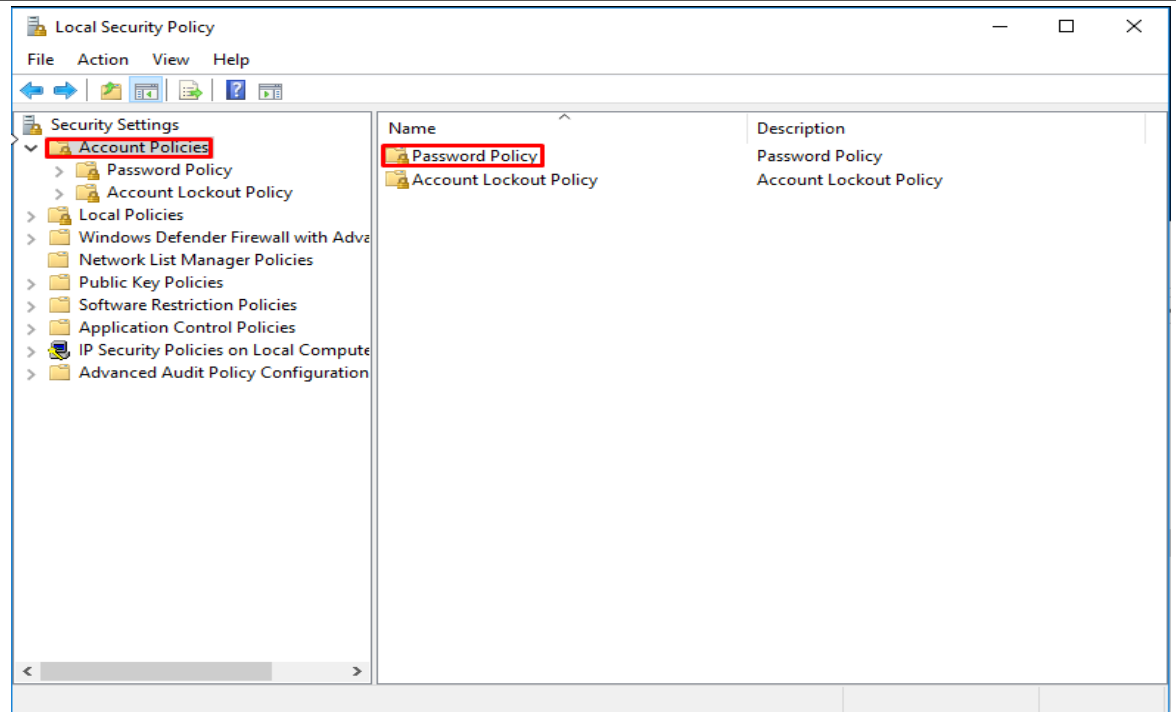
Go to administrative tools



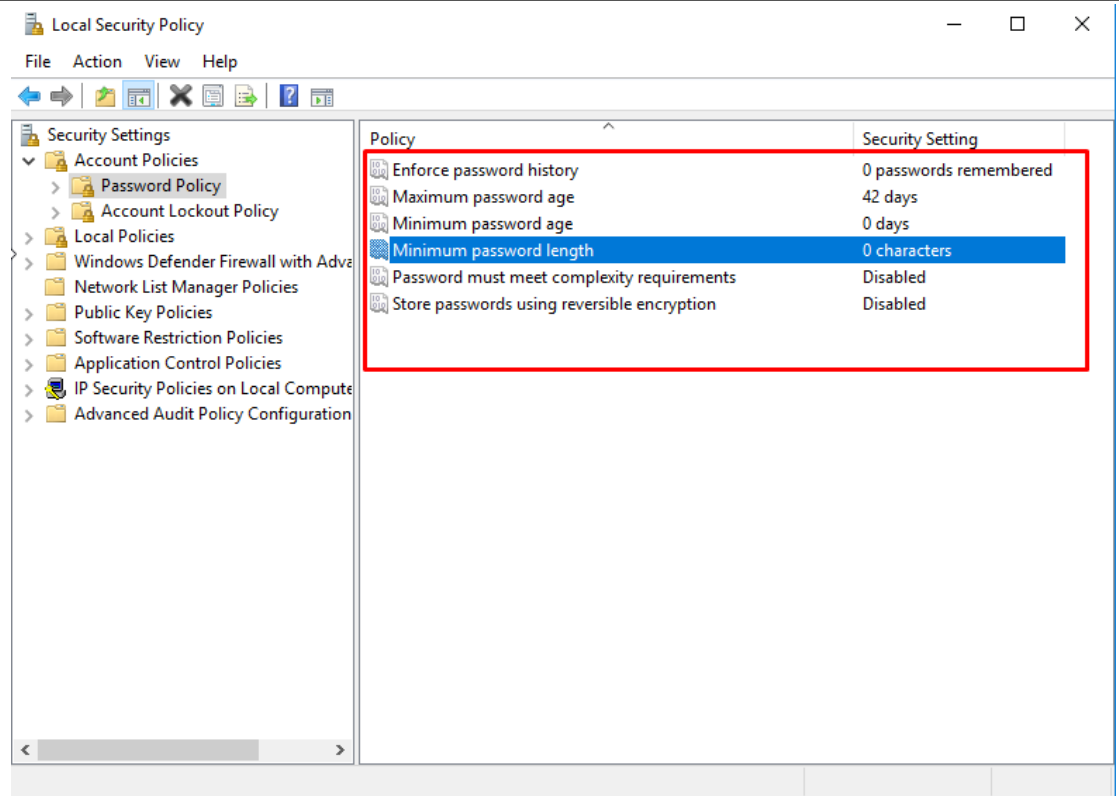
Open local security policy



Inside of account policies, click password policy

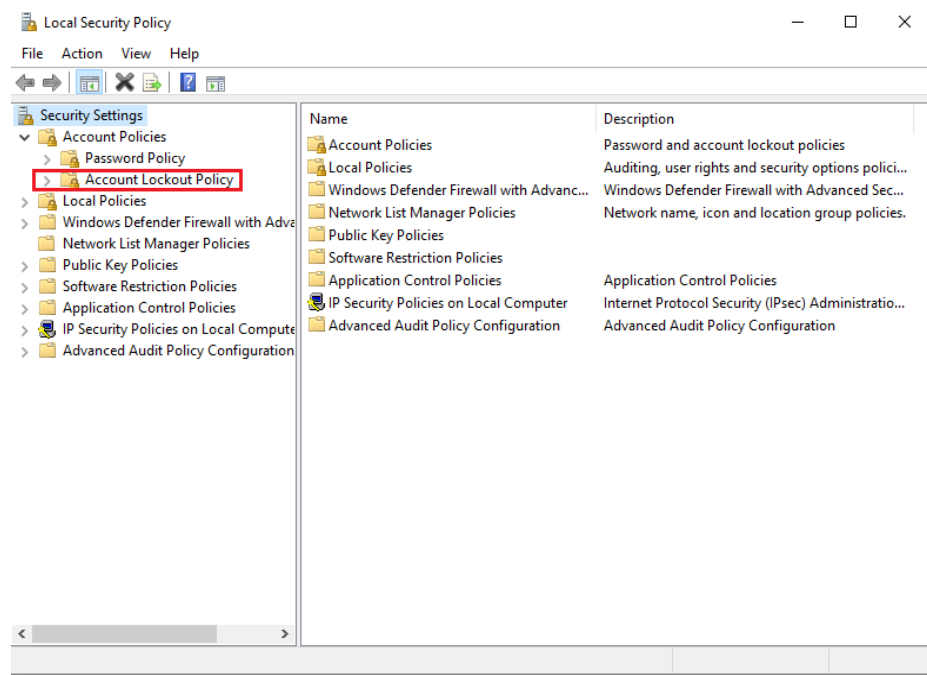


set the numbers on the password policy to 24, 60, 1, 10, Enabled, Disabled

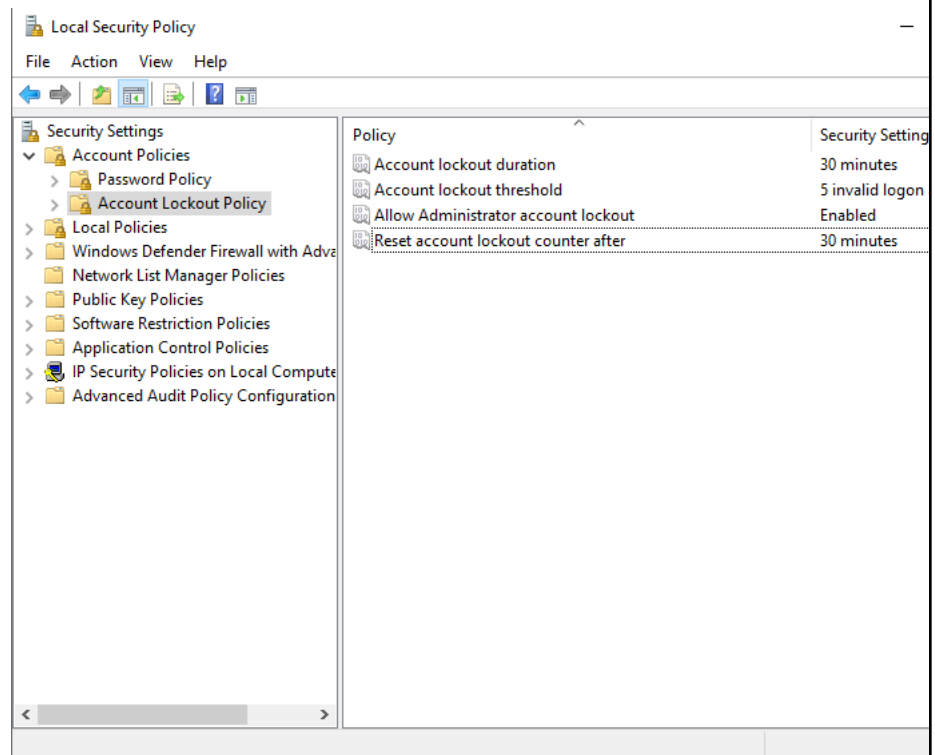


Lockout policy

Go to local policies
then account policies,
then lockout policy.

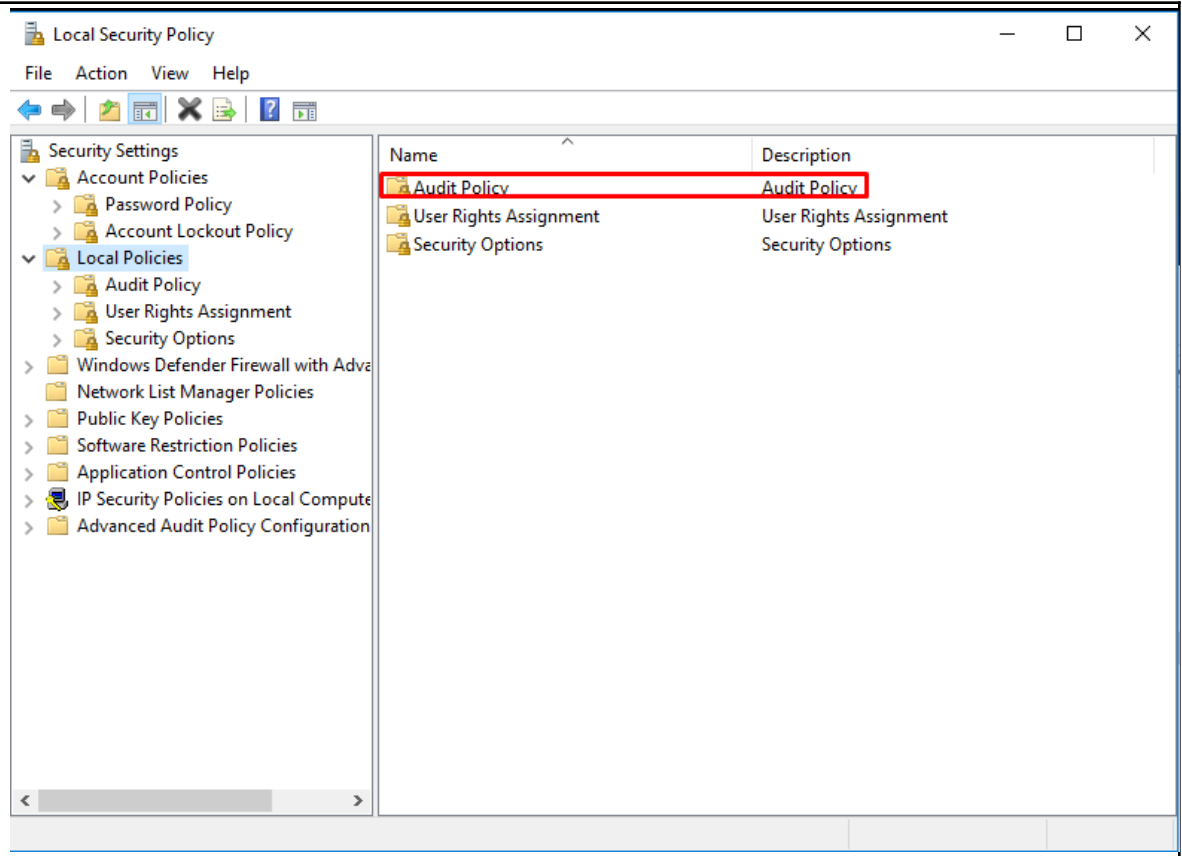


Set the values to what
you want, the one
shown in the picture
is a pretty secure one.

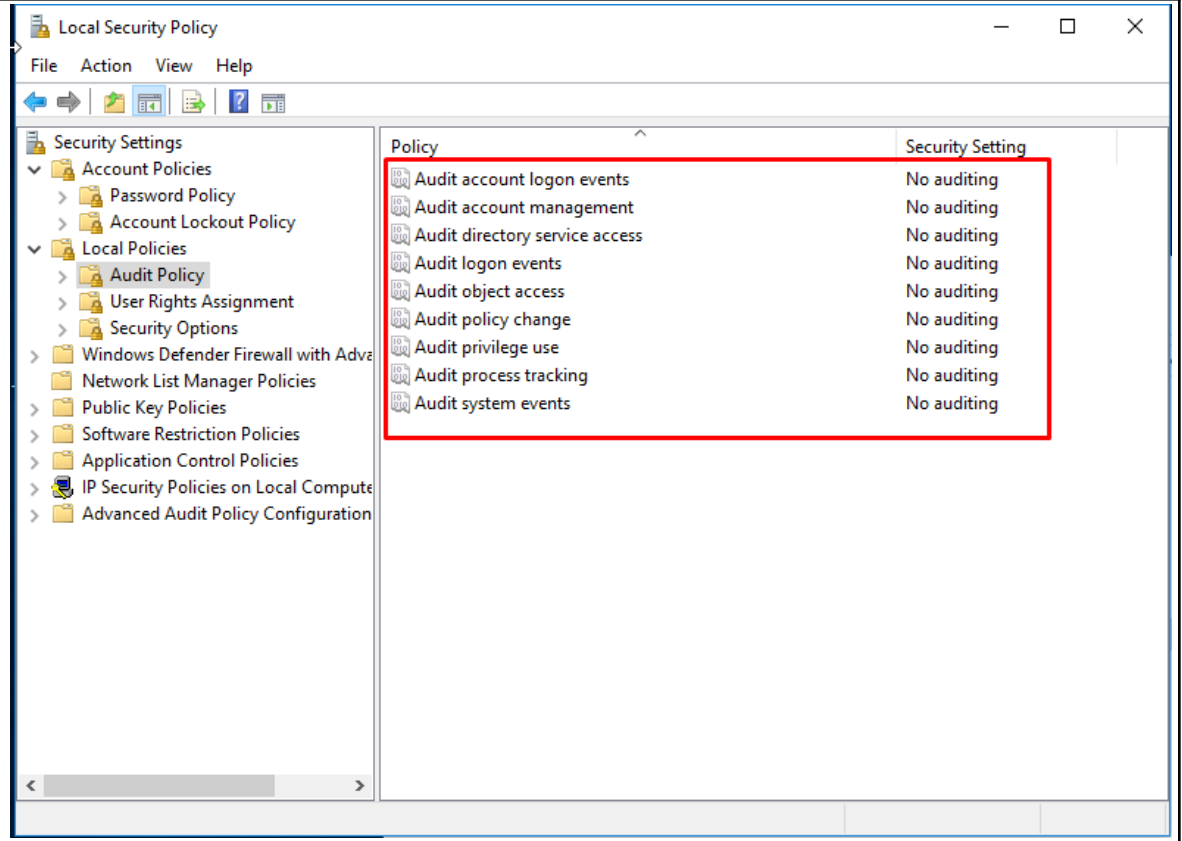


Audit policy

Go to local policies and then audit policies

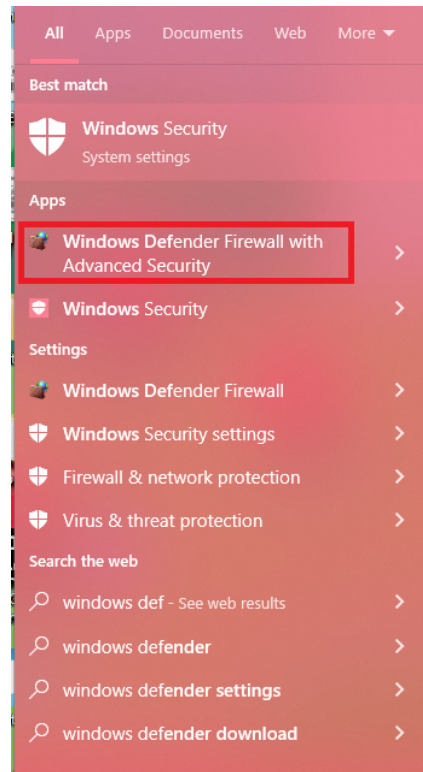


set everything
to auditing



Firewall rules

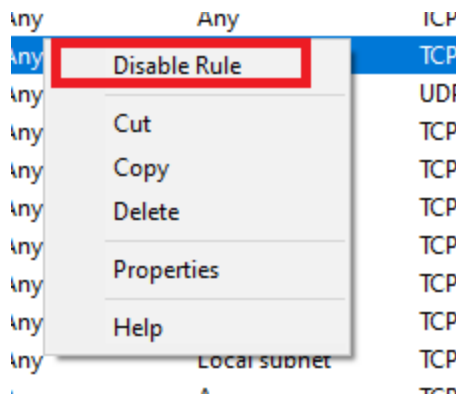
Open Windows Defender firewall with advanced security



Find a port you want to disable, in my example I will use RDP on port 3389

Remote Assistance (DCOM-In)	Remote Assistance	Domain	Yes	Allow	No	%System...	Any	Any	TCP
Remote Assistance (PNRP-In)	Remote Assistance	Domain	Yes	Allow	No	%system...	Any	Any	UDP
Remote Assistance (PNRP-In)	Remote Assistance	Public	No	Allow	No	%system...	Any	Any	UDP
Remote Assistance (RA Server TCP-In)	Remote Assistance	Domain	Yes	Allow	No	%System...	Any	Any	TCP
Remote Assistance (SSDP TCP-In)	Remote Assistance	Domain	Yes	Allow	No	System	Any	Local subnet	TCP
Remote Assistance (SSDP UDP-In)	Remote Assistance	Domain	Yes	Allow	No	%System...	Any	Local subnet	UDP
Remote Assistance (TCP-In)	Remote Assistance	Domain	Yes	Allow	No	%System...	Any	Any	TCP
Remote Assistance (TCP-In)	Remote Assistance	Public	No	Allow	No	%System...	Any	Any	TCP
Remote Desktop - (TCP-In)	Remote Desktop	All	No	Allow	No	%System...	Any	Any	TCP
Remote Desktop - User Mode (TCP-In)	Remote Desktop	All	Yes	Allow	No	%System...	Any	Any	TCP
Remote Desktop - User Mode (TCP-In)	Remote Desktop	All	Yes	Allow	No	%system...	Any	Any	UDP
Remote Desktop - (TCP-WS-In)	Remote Desktop (WebSocket)	All	No	Allow	No	System	Any	Any	TCP
Remote Desktop - (TCP-WS-In)	Remote Desktop (WebSocket)	All	No	Allow	No	System	Any	Any	TCP

Now simply right click and choose disable rule



Finding and disabling bad listening ports

Open cmd and type
netstat -a -o -n -b

This shows you the information of what ports are listening, the PID, and also the program name.

You can easily see if something is “Sus”


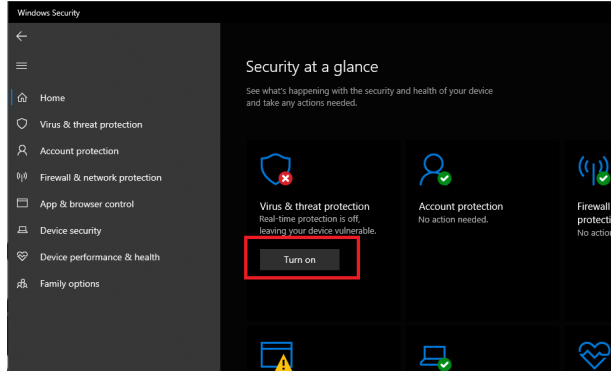
```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19045.3448]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>netstat -a -o -n -b

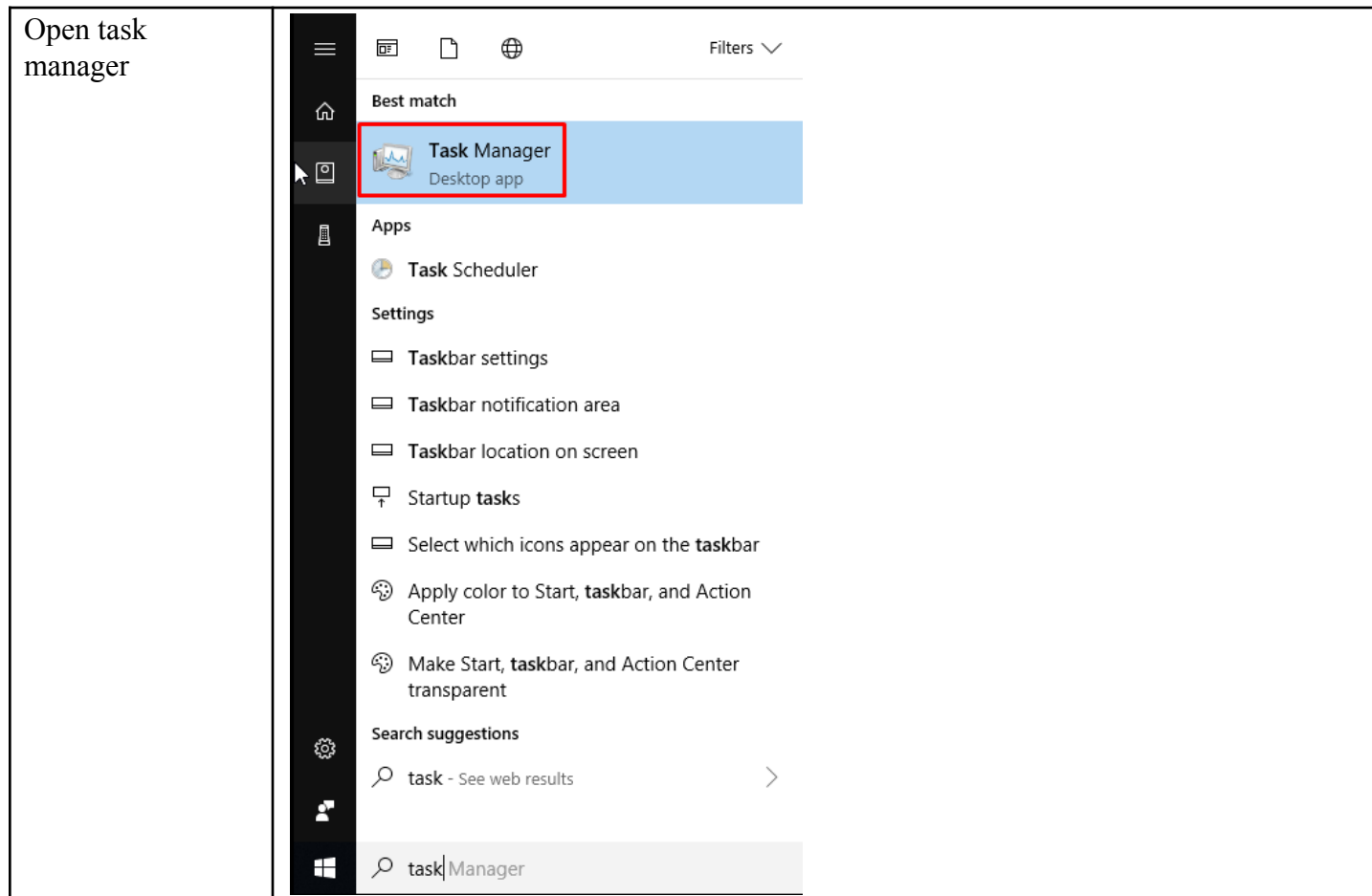
Active Connections

  Proto Local Address           Foreign Address         State       PID
  TCP    0.0.0.0:135              0.0.0.0:0               LISTENING   1096
  RpcSs
  [svchost.exe]
  TCP    0.0.0.0:445              0.0.0.0:0               LISTENING   4
  Can not obtain ownership information
  TCP    0.0.0.0:903              0.0.0.0:0               LISTENING   5320
  [vmware-authd.exe]
  TCP    0.0.0.0:913              0.0.0.0:0               LISTENING   5320
  [vmware-authd.exe]
  TCP    0.0.0.0:3389             0.0.0.0:0               LISTENING   1388
  TermService
  [svchost.exe]
  TCP    0.0.0.0:5040             0.0.0.0:0               LISTENING   9916
  CDPSvc
  [svchost.exe]
  TCP    0.0.0.0:5357             0.0.0.0:0               LISTENING   4
  Can not obtain ownership information
  TCP    0.0.0.0:7680             0.0.0.0:0               LISTENING   20732
  Can not obtain ownership information
  TCP    0.0.0.0:49559            0.0.0.0:0               LISTENING   31588
  [LogiOptionsMgr.exe]
  TCP    0.0.0.0:49664            0.0.0.0:0               LISTENING   992
  [lsass.exe]
  TCP    0.0.0.0:49665            0.0.0.0:0               LISTENING   912
  Can not obtain ownership information
  TCP    0.0.0.0:49666            0.0.0.0:0               LISTENING   2004
  EventLog
  [svchost.exe]
  TCP    0.0.0.0:49667            0.0.0.0:0               LISTENING   1664
```

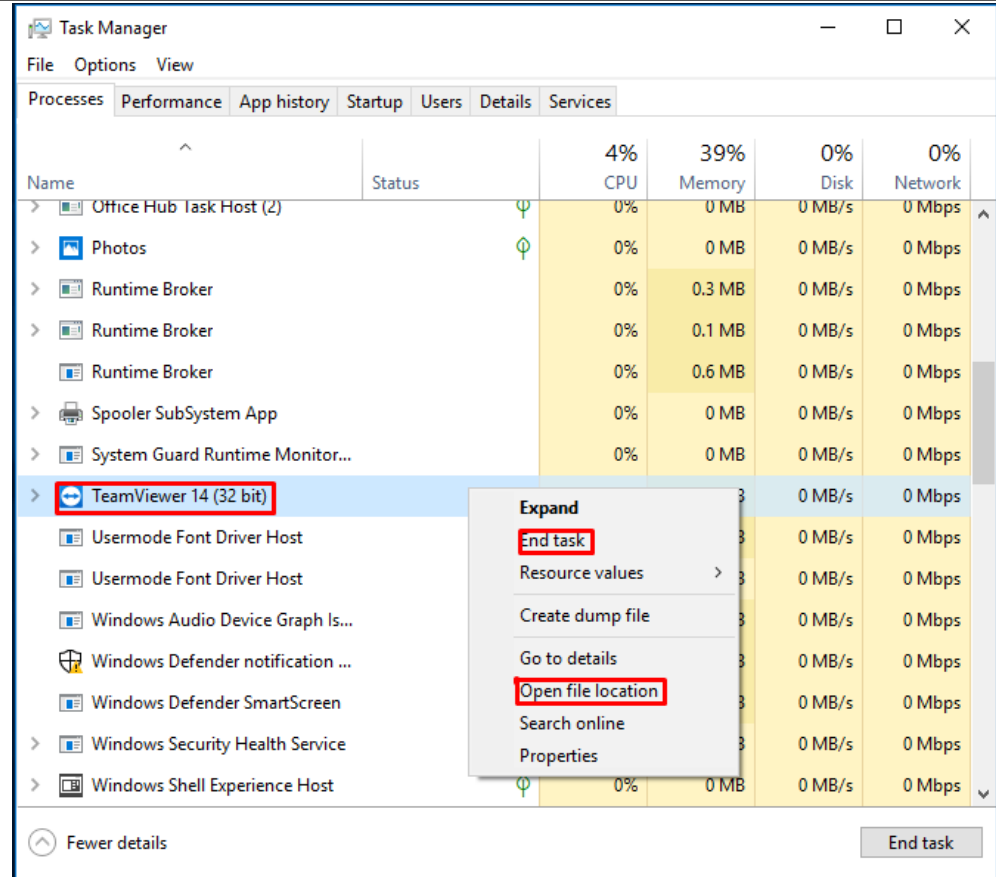
Turning on Windows Defender

<p>Open windows security</p>	 <p>The screenshot shows the Windows Search interface. The search bar at the top contains the text 'windows'. Below the search bar, the results are categorized into 'All', 'Apps', 'Documents', 'Web', and 'More'. Under the 'All' category, the 'Best match' is 'Windows PowerShell (x86)' (App). Below this, 'Windows Security' (System settings) is highlighted with a red box. Other results include 'Settings' (Windows Defender Firewall, Check for updates, Windows Security settings, Windows HD Color settings, Change your password, Firewall & network protection), 'Search the web' (windows - See web results), 'Documents (5+)', 'Folders (1+)', and 'Apps (12+)'. The search bar at the bottom shows 'windows' and 'PowerShell (x86)'.</p>
<p>turn on</p>	 <p>The screenshot shows the Windows Security app. The left sidebar contains a list of security features: Home, Virus & threat protection, Account protection, Firewall & network protection, App & browser control, Device security, Device performance & health, and Family options. The main area is titled 'Security at a glance' and shows three status cards: 'Virus & threat protection' (Real-time protection is off, leaving your device vulnerable, with a red 'Turn on' button highlighted), 'Account protection' (No action needed), and 'Firewall protection' (No action needed). The bottom of the screen shows three icons: a yellow warning triangle, a green checkmark, and a blue shield.</p>

Finding and stopping bad programs in the background



Find the program you want to stop and right click it to stop it, also click open file location



when you click
open file location,
find the program
and delete it

