

_os.a1

walkthrough on securing a windows vm

IT1313 Operating Systems Administration: Group Assignment 1

by Kriston, Jia Xiang, Dhiraj, & Jun Lin

contents

preface && task allocations

What's going on exactly.



protection and backups

system security and account management

network stuff and access control

device protection and malware stuff

“presenting of own parts”

Individually present respective tasks.



conclusion

A summary on what we've done



preface && task allocations

What's going on exactly.

task allocations

The tasks were split according to their themes.



protection and backups

Kriston



system security and account management

Jia Xiang

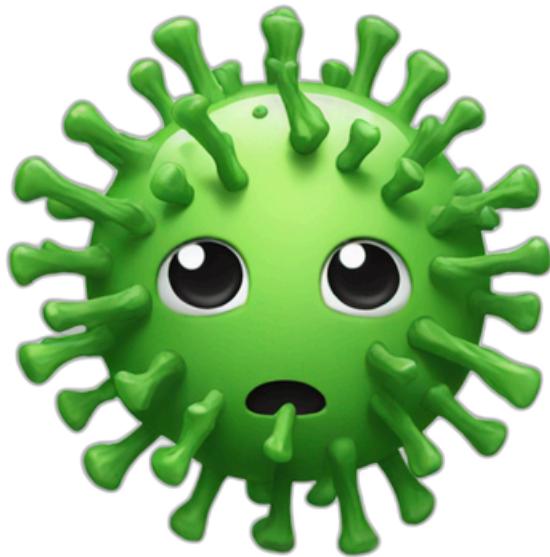
_task allocations

The tasks were split according to their themes.



network stuff and access control

Dhiraj



device protection and malware stuff

Jun Lin

preface: admin stuff

An overview of things.

Roles	
Jesalva Kriston Jomari Ballesteros, 231165R	Leader
Sim Jia Xiang, 241907M	Contributor
Joshy Dhiraj, 240136M	Contributor
Wong Jun Lin, 242844E	Contributor

preface: accounts

Some of the tasks are as easy as logging in and toggling a button, so the following login credentials were used:

Master Credentials	
Microsoft Account Email	osa_assignment_vm_acc@outlook.com
Microsoft Account Password	drab@-4meP7A0u6oPh1
Password for Windows	Th1s1sM!Yp@ssw0rd\$

preface: documentation

The steps mentioned in this presentation deck is **NOT** as detailed as the one in our Google Doc (to save space).

Please refer to the Google Doc, or submitted Word Doc for proper documentation.

This deck also isn't as easily navigable as our Google Doc.

Accessible here: [_os.a1](#)

The screenshot shows a Google Document window with the title '_os.a1'. The left sidebar displays a table of contents under 'Document tabs' with sections like 'Main Tab', '_os.a1', '_preface', '_tasks', and '_System security and a...'. The main content area contains several sections of text and a table:

- _os.a1**
- _preface**

This will be our group document for both documentation and checklists. I'll format it in the end, so don't worry about it now.
- _tasks**

The tasks are split according to their theme.

Most of it is not covered in class, so just google for solutions. **Remember to take STEP BY STEP screenshots as if you were making a guide for noobs (but don't overdo it).**

For anything password-related remember to use upper/lowercase, numbers, special char.

Feel free to add tables wherever in your documentation if it helps with organization, remember to save the links of websites you referred to and etc.

[Canva Link](#)

Some of the tasks are as easy as logging in and toggling a button, so use the following login credentials:

Master Credentials	
Microsoft Account Email	osa_assignment_vm_acc@outlook.com
Microsoft Account Password	drab@s-4meP7A0u6oPh1
Password for Windows	Th1s1sMYp@ssw0rd\$

_tasks

https://docs.google.com/document/d/1P4e12rnzFuslr-8iEmLSla-u5Du-RCUC8G_KT2N3x9g/edit?usp=sharing

preface: assumptions

- **Strong Passwords:** All user passwords are a minimum of 12 characters, incorporating upper/lowercase letters, numbers, and symbols.
- **Windows Version:** The VM was upgraded from Windows 10 Education to Windows 10 Pro using a GitHub script, enabling additional security features.
- **User Compliance:** Users follow security guidelines, like using complex passwords and avoiding unauthorized software.
- **Default Windows Settings:** The VM setup uses standard Windows settings, with no prior custom security configurations.

preface: *limitations*

- **Virtualization Constraints:** Limited access to hardware-based security features like Intel VT-x/EPT or AMD-V/RVI in virtual environments.
- **Windows Hello Restrictions:** Only PIN unlock is used; Face and Fingerprint options are unavailable in this VM environment.
- **Hardware-Dependent Features:** Features like Secure Boot and TPM may have limited functionality depending on virtual hardware support.

_ “presenting of own parts”

Individually present respective tasks.

_protection & backups



by Kriston

tasks

done by Kriston

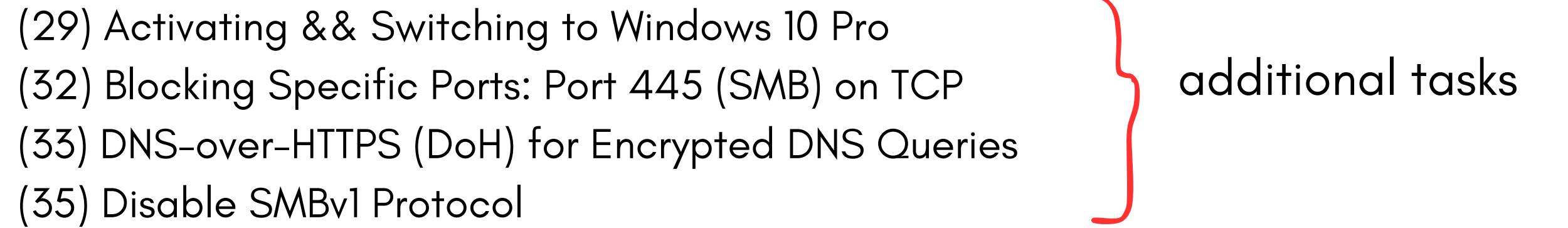
- (18) App Management - Only allow the installation of approved applications from controlled software repositories or application marketplaces
- (19) Application Control - Whitelisting and blacklisting of executables or apps
- (22) Enable Windows Hello
- ~~(23) Enable Windows Sandbox (Not completed)~~
- (24) Enable Windows Secure Boot
 - (a) Enable TPM if available
 - ~~(b) Create personal security certificates if necessary (Not completed)~~
- (25) Enable Windows BitLocker Encryption
- (26) Enable File Backups
- (27) Enable Restore Points

base tasks

protection and backups

tasks

done by Kriston

- (29) Activating && Switching to Windows 10 Pro
 - (32) Blocking Specific Ports: Port 445 (SMB) on TCP
 - (33) DNS-over-HTTPS (DoH) for Encrypted DNS Queries
 - (35) Disable SMBv1 Protocol
- 
- } additional tasks

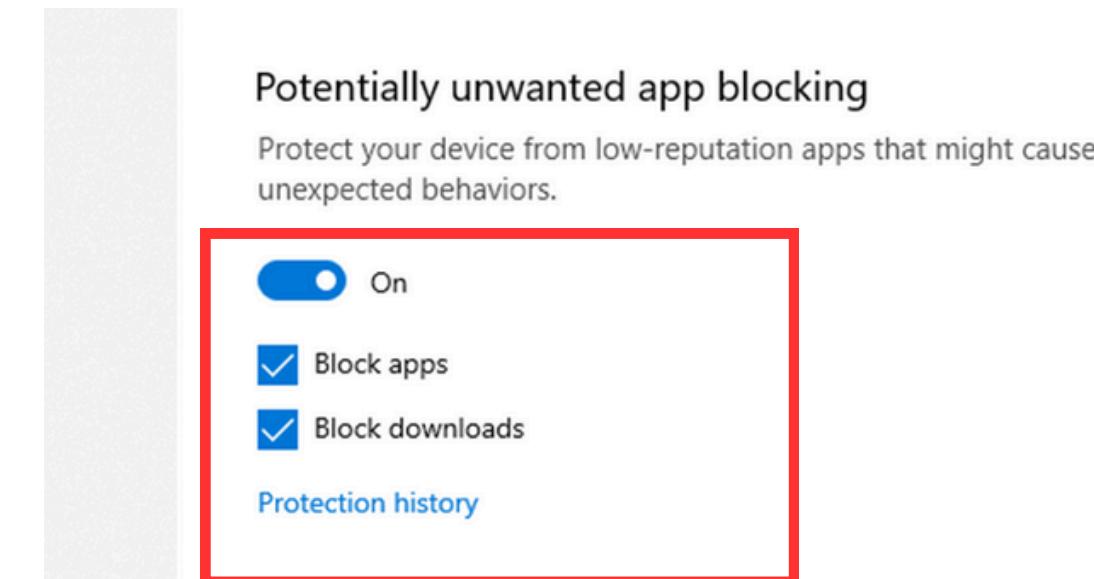
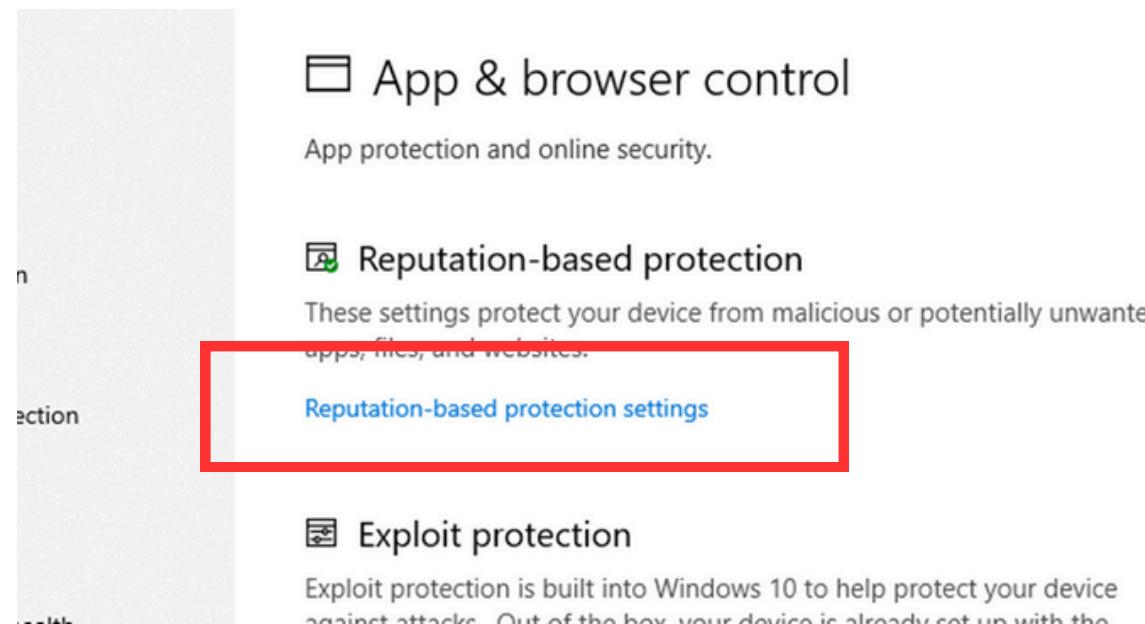
protection and backups

tasks

(18) App Management – Only allow the installation of approved applications from controlled software repositories or application marketplaces

1. In Windows Security > App & browser control tab > select Reputation-based protection settings.

Scroll to find Potentially unwanted app-blocking. Toggle the setting on, and you're set after.



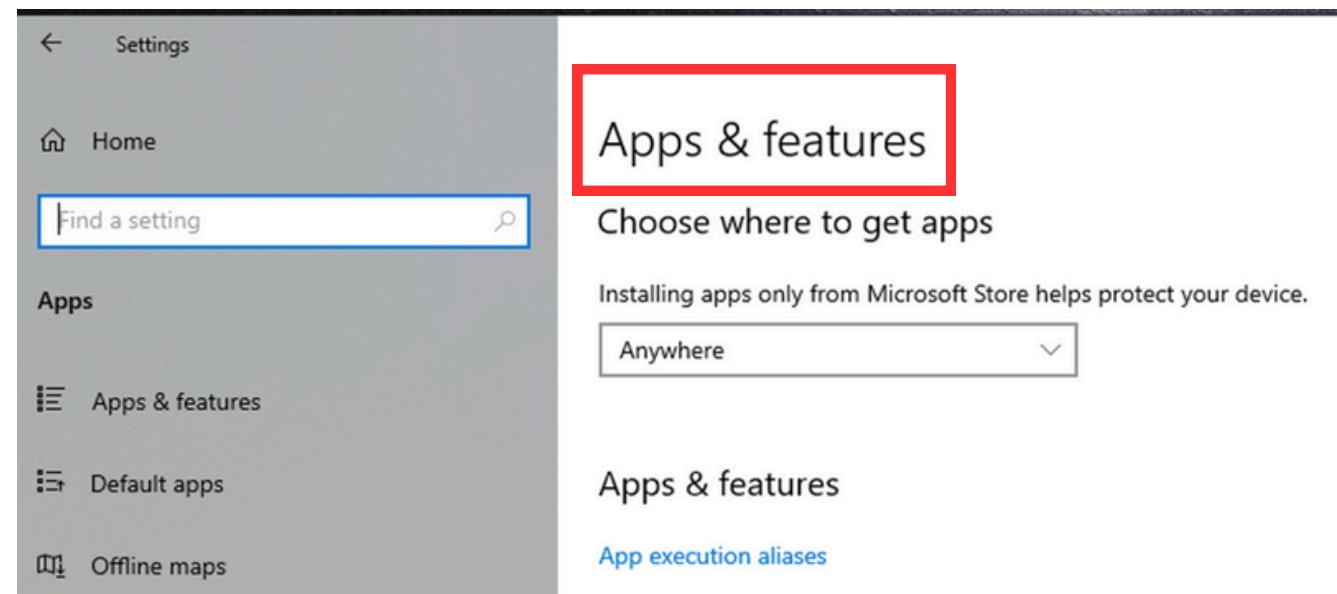
This protects your device from unexpected behaviors caused by low-reputation apps.

protection and backups

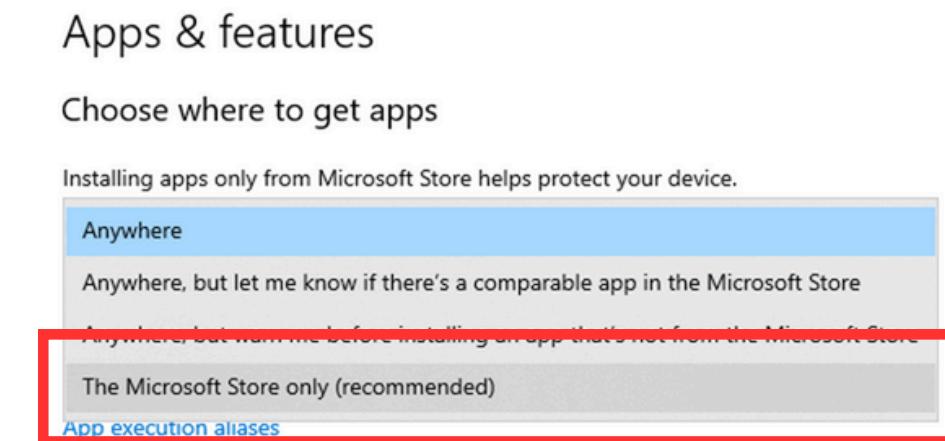
tasks

(18) App Management – Only allow the installation of approved applications from controlled software repositories or application marketplaces

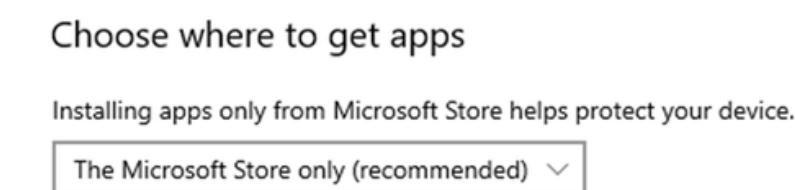
2. Visit Settings > Apps > Apps & features



Under "Choose where to get apps", choose "The Microsoft Store only (recommended)".



After that, you are all set, only apps from The Microsoft Store will be allowed.

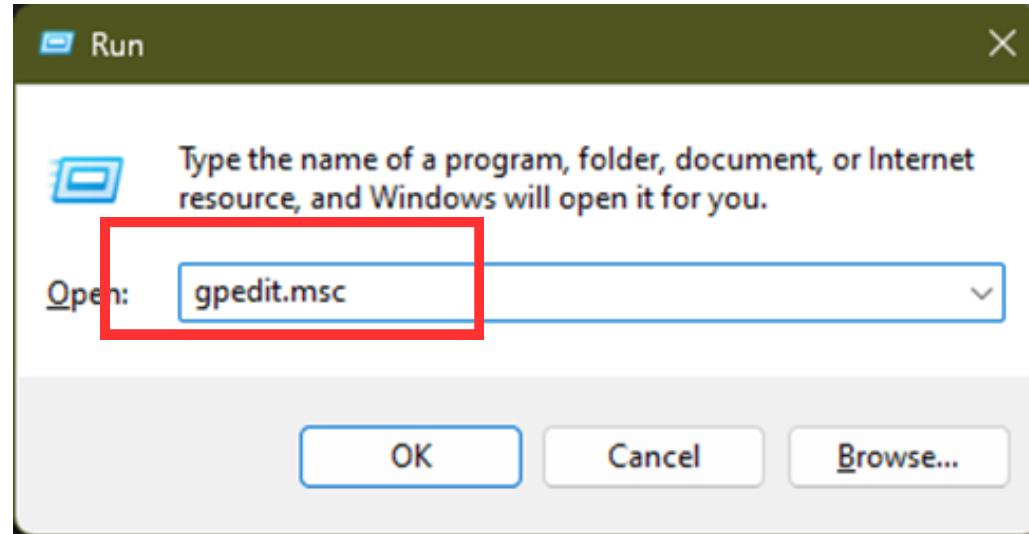


protection and backups

tasks

(18) App Management – Only allow the installation of approved applications from controlled software repositories or application marketplaces

3. Restrict App Sources Using Group Policy

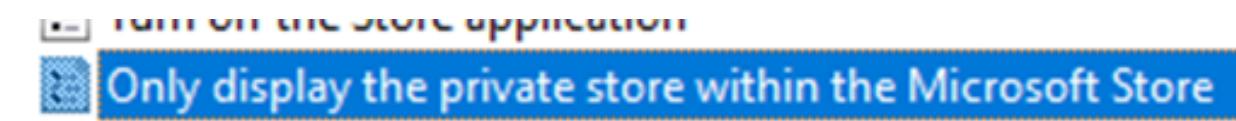


Win + R > gpedit.msc > OK

Navigate to Computer Configuration > Administrative Templates > Windows Components > Store

protection and backups

Find the setting "Only display the private store within the Microsoft Store app".



Double-click the setting, set it to Enabled, > OK. This restricts access to only approved applications from a designated private Microsoft Store.

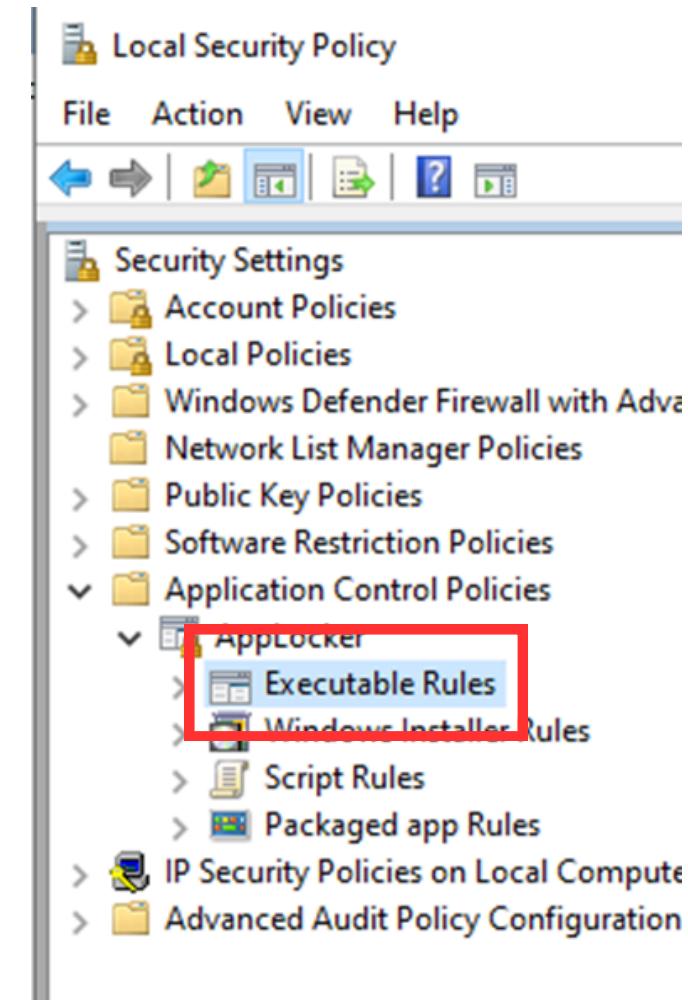


tasks

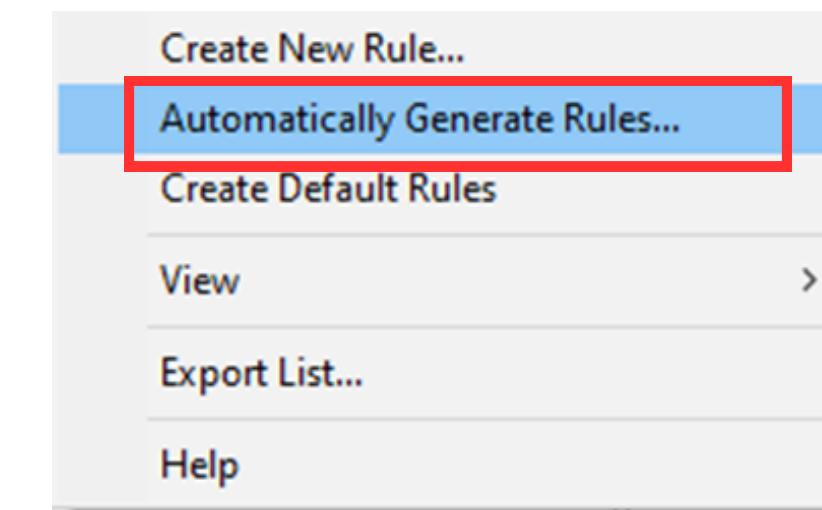
(18) App Management – Only allow the installation of approved applications from controlled software repositories or application marketplaces

4. Configure AppLocker for Whitelisting

Go to Local Security Policy.> Application Control Policies > select AppLocker.



Right-click on Executable Rules and choose Automatically Generate Rules.

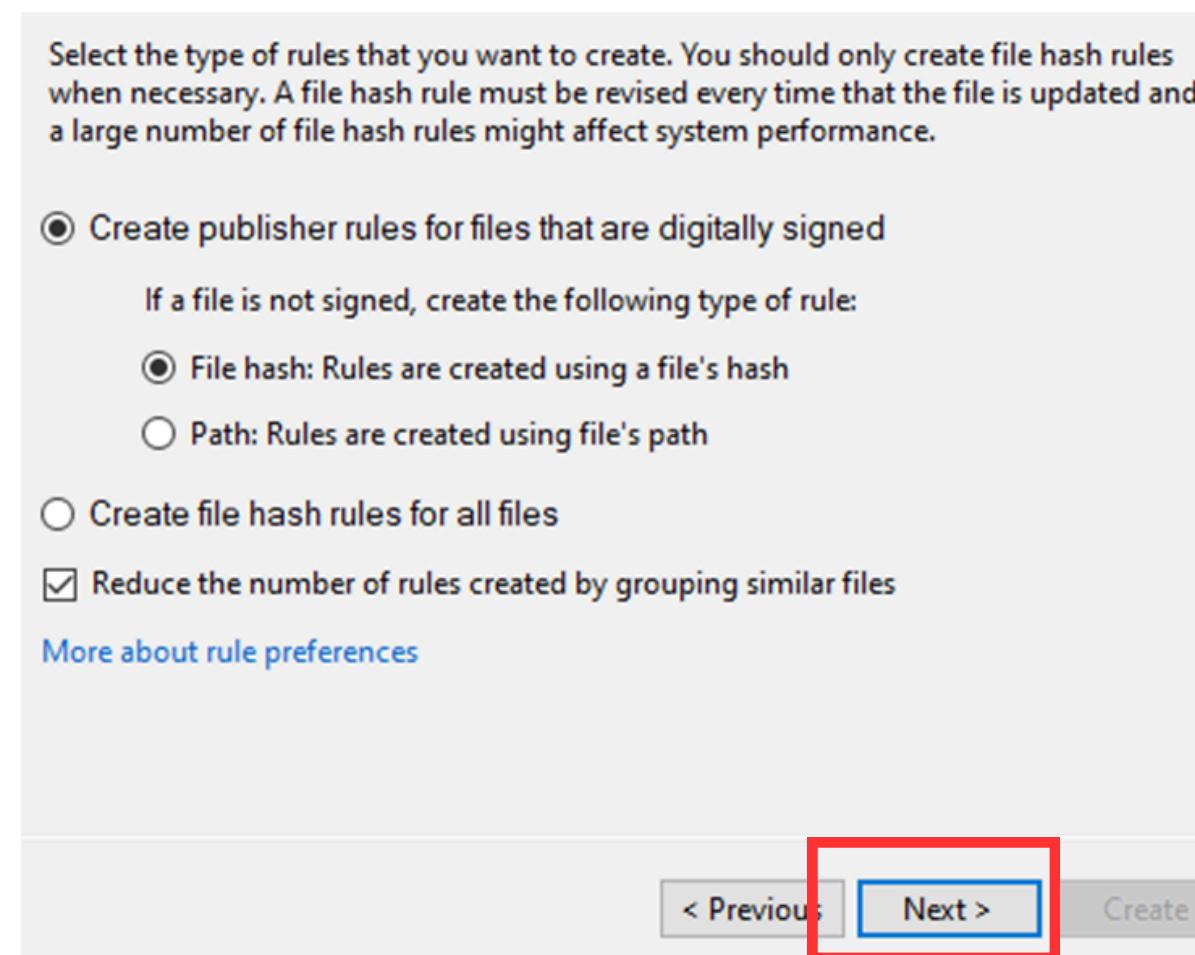


protection and backups

tasks

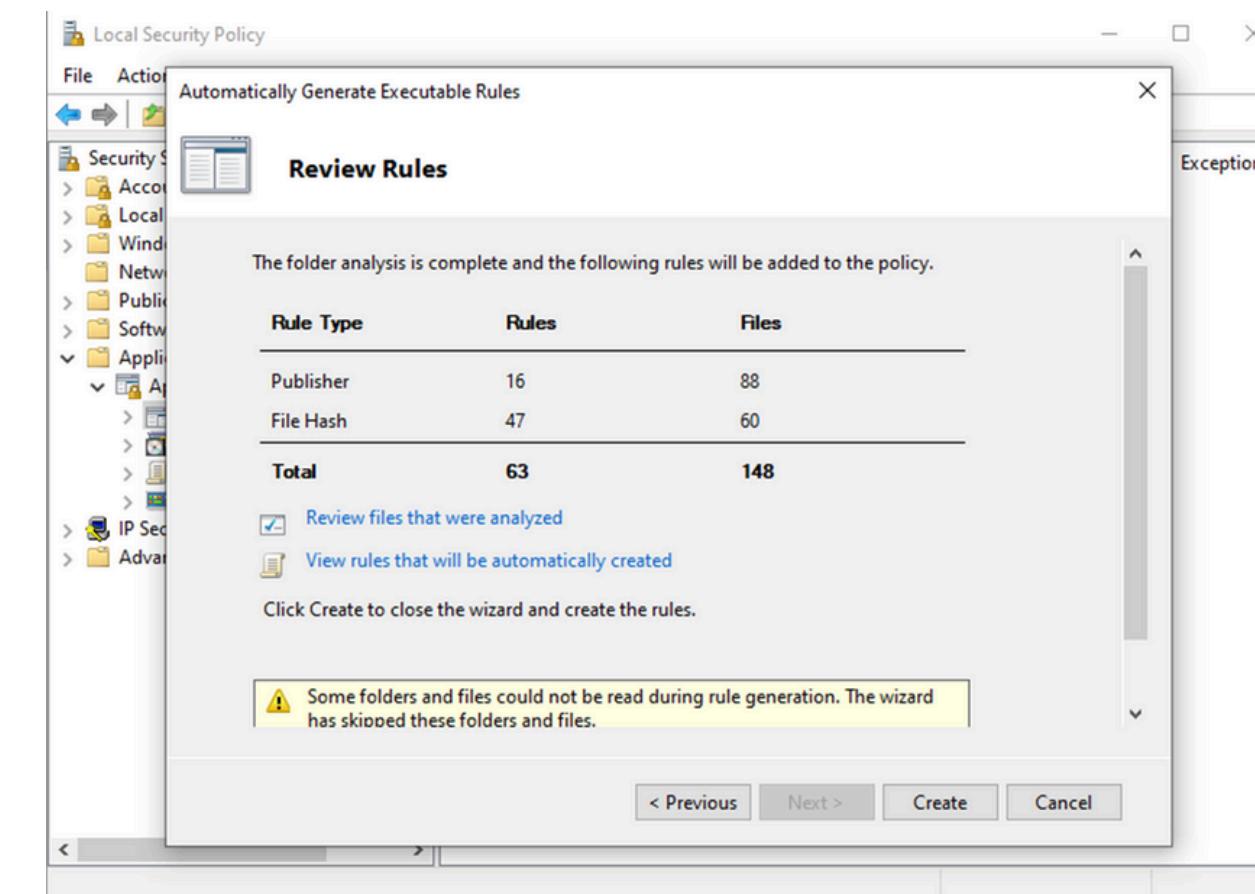
(18) App Management – Only allow the installation of approved applications from controlled software repositories or application marketplaces

4. Follow the wizard > Next > Follow the defaults



protection and backups

Review the list of generated rules. You'll see file paths or hash rules created based on the applications in the selected directory.

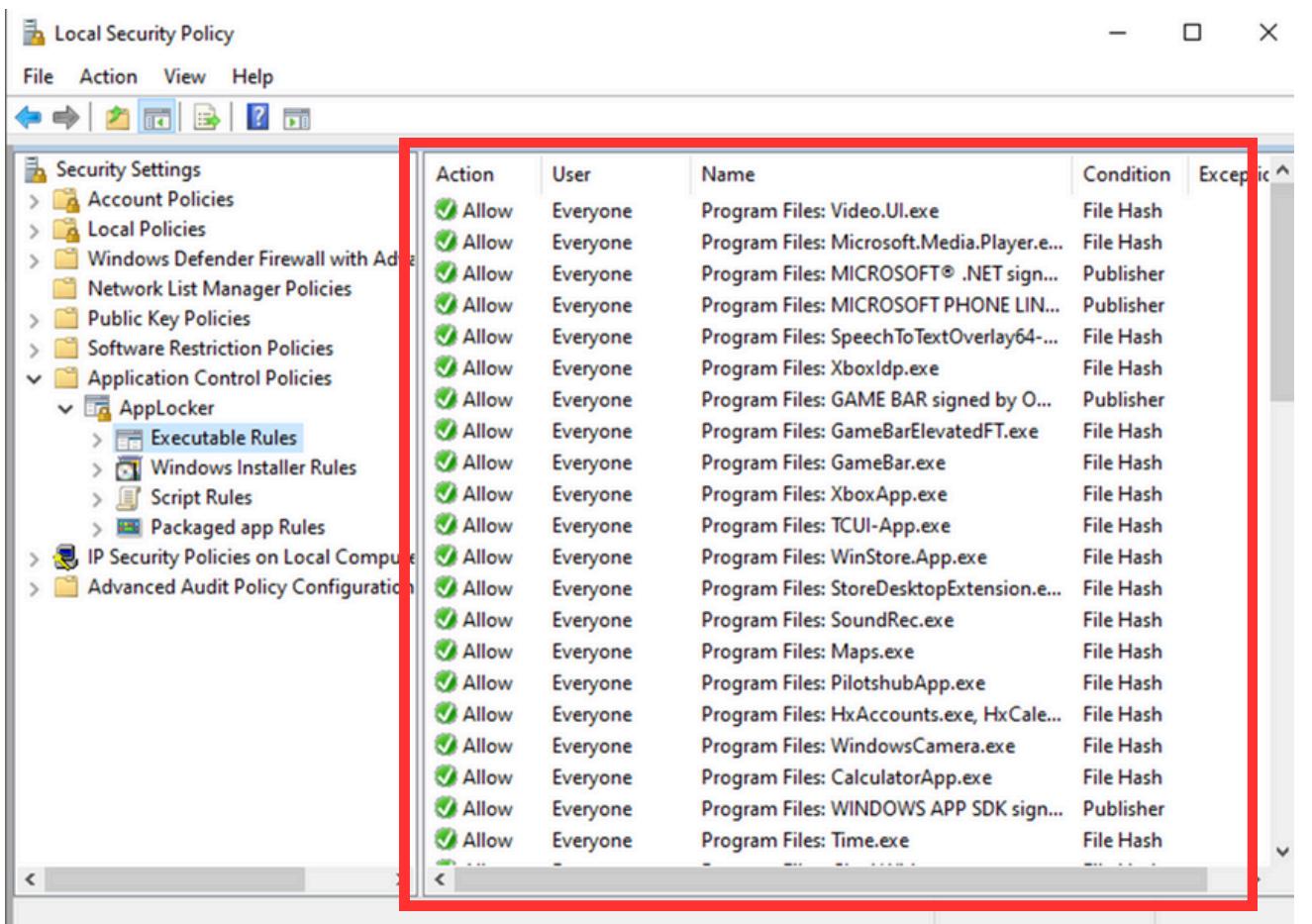


Edit as per your specific needs, etc.

tasks

(18) App Management – Only allow the installation of approved applications from controlled software repositories or application marketplaces

4. Confirmation of our Executable Rules.



The screenshot shows the Windows Local Security Policy snap-in. On the left, the navigation pane is visible with various policy categories like Account Policies, Local Policies, and Application Control Policies. Under Application Control Policies, the 'AppLocker' node is expanded, and its 'Executable Rules' sub-node is selected. A red box highlights the main content area, which is a table listing executable rules. The table has columns for Action (Allow), User (Everyone), Name (the path to the executable file), Condition (File Hash or Publisher), and Exception (empty). There are approximately 25 rows in the table, each representing a different executable file that has been whitelisted.

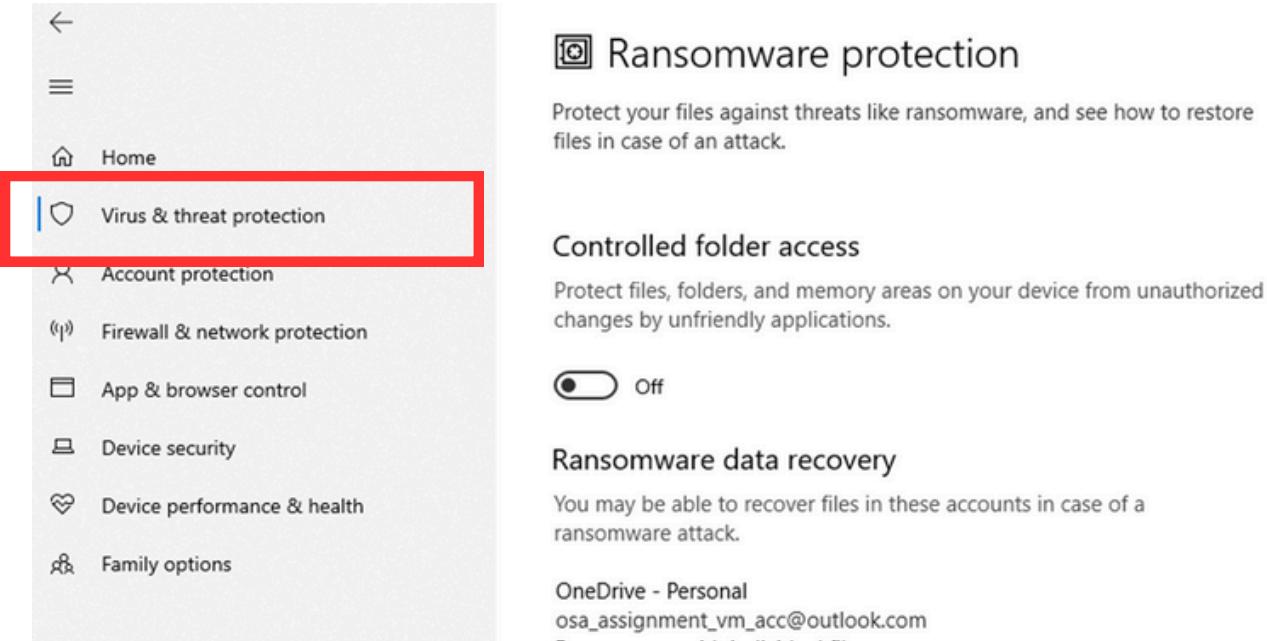
Action	User	Name	Condition	Exception
Allow	Everyone	Program Files: Video.Ui.exe	File Hash	
Allow	Everyone	Program Files: Microsoft.Media.Player.e...	File Hash	
Allow	Everyone	Program Files: MICROSOFT® .NET sign...	Publisher	
Allow	Everyone	Program Files: MICROSOFT PHONE LIN...	Publisher	
Allow	Everyone	Program Files: SpeechToTextOverlay64...	File Hash	
Allow	Everyone	Program Files: XboxIdp.exe	File Hash	
Allow	Everyone	Program Files: GAME BAR signed by O...	Publisher	
Allow	Everyone	Program Files: GameBarElevatedFT.exe	File Hash	
Allow	Everyone	Program Files: GameBar.exe	File Hash	
Allow	Everyone	Program Files: XboxApp.exe	File Hash	
Allow	Everyone	Program Files: TCUI-App.exe	File Hash	
Allow	Everyone	Program Files: WinStore.App.exe	File Hash	
Allow	Everyone	Program Files: StoreDesktopExtension.e...	File Hash	
Allow	Everyone	Program Files: SoundRec.exe	File Hash	
Allow	Everyone	Program Files: Maps.exe	File Hash	
Allow	Everyone	Program Files: PilotshubApp.exe	File Hash	
Allow	Everyone	Program Files: HxAccounts.exe, HxCale...	File Hash	
Allow	Everyone	Program Files: WindowsCamera.exe	File Hash	
Allow	Everyone	Program Files: CalculatorApp.exe	File Hash	
Allow	Everyone	Program Files: WINDOWS APP SDK sign...	Publisher	
Allow	Everyone	Program Files: Time.exe	File Hash	

protection and backups

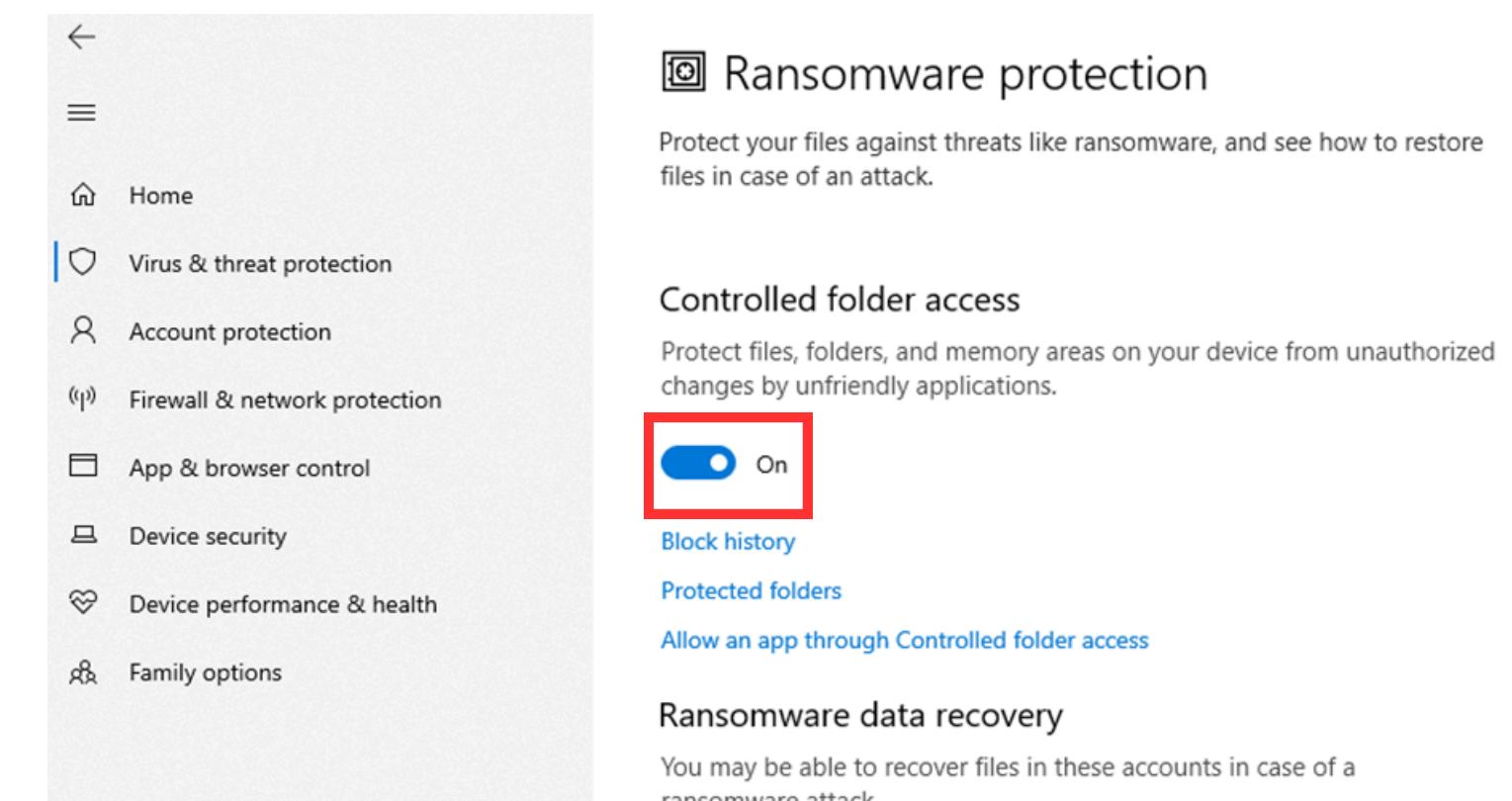
tasks

(19) Application Control - Whitelisting and blacklisting of executables or apps

1. In Windows Security, visit the Virus & threat protection tab, visit Ransomware protection settings.



2. Simply enable the Controlled folder access.



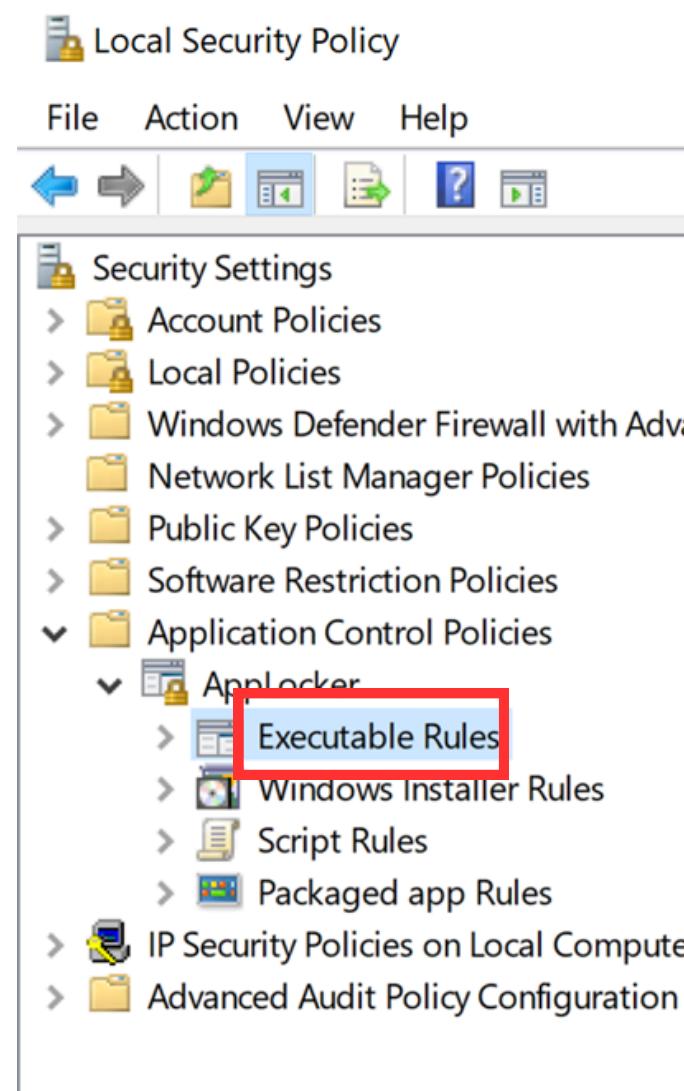
protection and backups

tasks

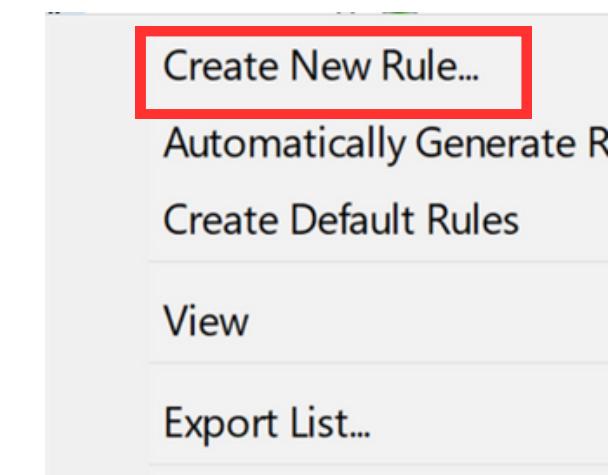
(19) Application Control - Whitelisting and blacklisting of executables or apps

3. Visit Local Security Policy,
Win + R > secpol.msc > OK

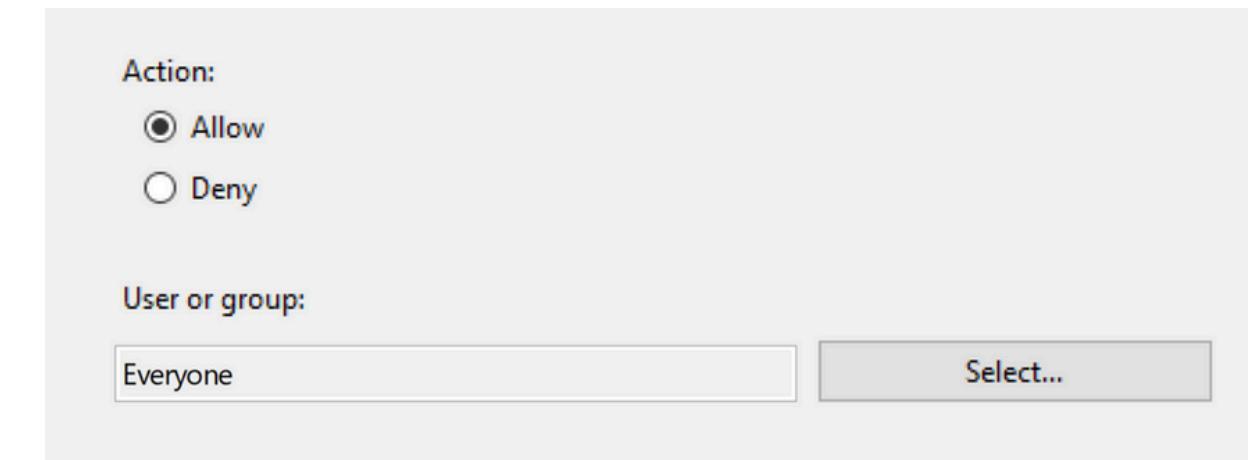
Application Control Policies >
AppLocker > Right-click
Executable Rules



Create New Rule...



Choose Allow as the action and specify everyone > Next.



protection and backups

tasks

(19) Application Control - Whitelisting and blacklisting of executables or apps

3. Choose to specify the Path > Next.

Select the type of primary condition that you would like to create.

Publisher
Select this option if the application you want to create the rule for is signed by the software publisher.

Path
Create a rule for a specific file or folder path. If you select a folder, all files in the folder will be affected by the rule.

File hash
Select this option if you want to create a rule for an application that is not signed.

Specify the following > Create:

Path:

C:\Program Files

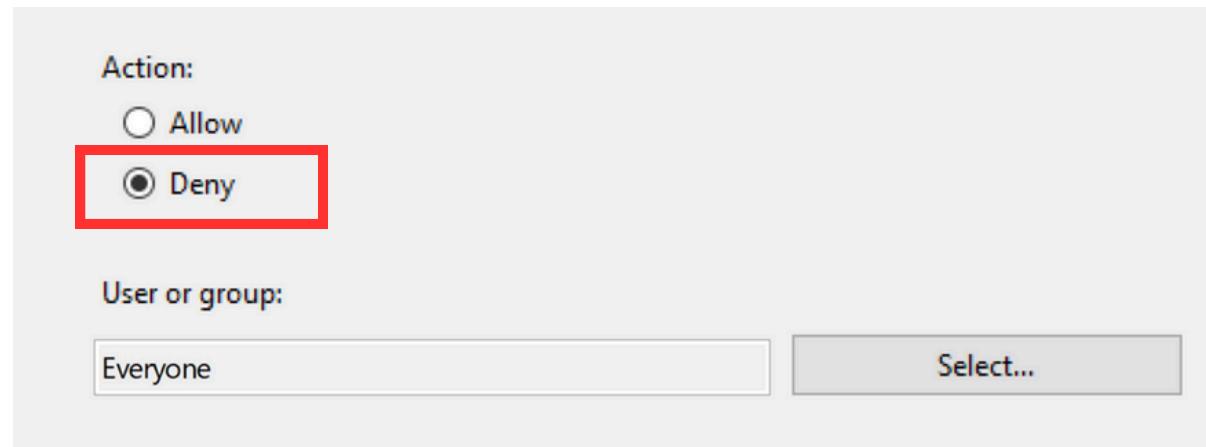
Browse Files... Browse Folders...

protection and backups

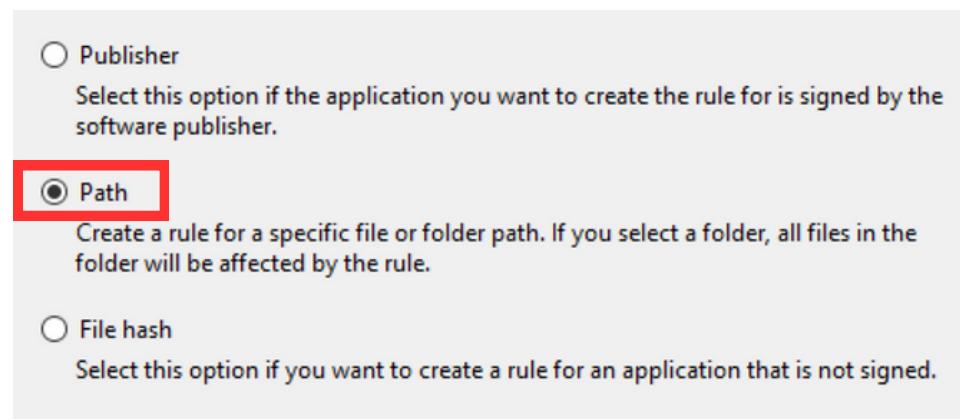
tasks

(19) Application Control - Whitelisting and blacklisting of executables or apps

4. Blacklisting: Create another Executable Rule > Deny > Everyone

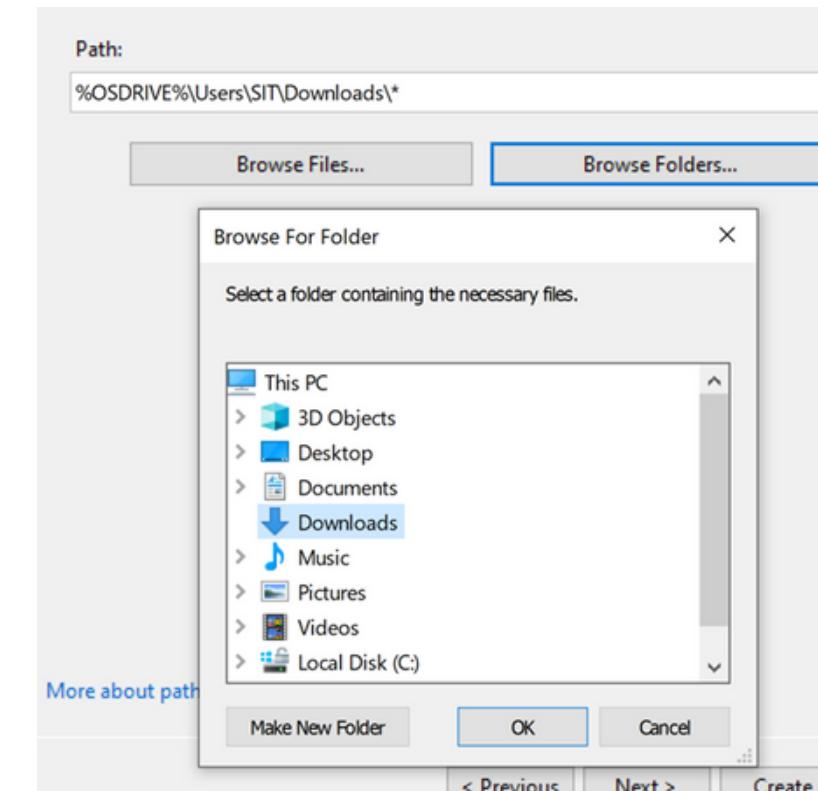


Select Path.



protection and backups

Browse Path > select the Downloads folder > OK.



Include *.exe at the end (targets all .exe files in the Downloads folder).

%OSDRIVE%\Users\SIT\Downloads*.exe

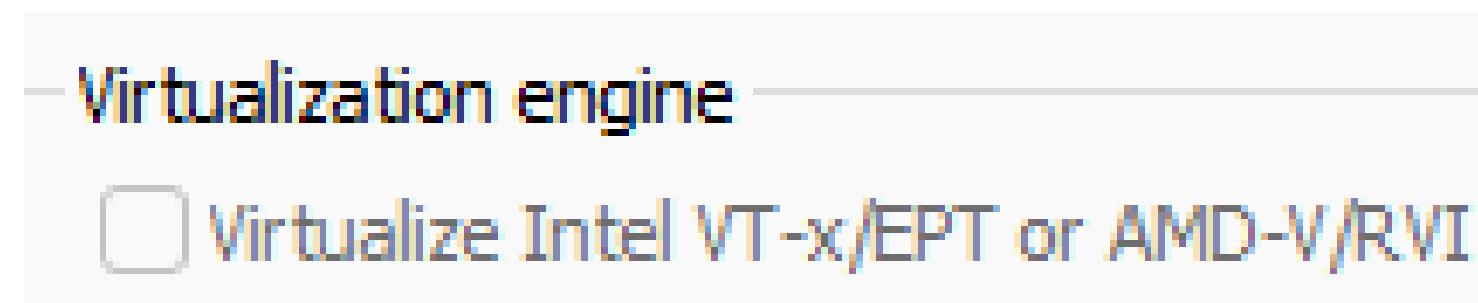
Next > Complete the Wizard

tasks

(23) Enable Windows Sandbox

Not completed due to:

Virtualization Constraints. Limited access to hardware-based security features like Intel VT-x/EPT or AMD-V/RVI in virtual environments.



Enabling the option in VMware will result in the VM failing to power on.

protection and backups

tasks

(24) Enable Windows Secure Boot

1. Launch Powershell as Administrator

> Run get-disk to check the partition style

> In our case, it's MBR

> We need to convert it into GPT

> We do so by running MBR2GPT.EXE /convert /allowfullOS

(You may have to run the command twice.)

> Power down the VM after.

The screenshot shows a Windows PowerShell window titled "Administrator: Windows PowerShell". The window displays the following commands and their output:

```
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> get-disk
Number Friendly Name Serial Number HealthStatus OperationalStatus Total Size Partition Style
---- -- -- -- -- -- -- --
0 VMware, VM... Healthy Online 60 GB MBR

PS C:\WINDOWS\system32> MBR2GPT.EXE /convert /allowfullOS
MBR2GPT will now attempt to convert the default boot disk.
If conversion is successful the disk can only be booted in GPT mode.
These changes cannot be undone!

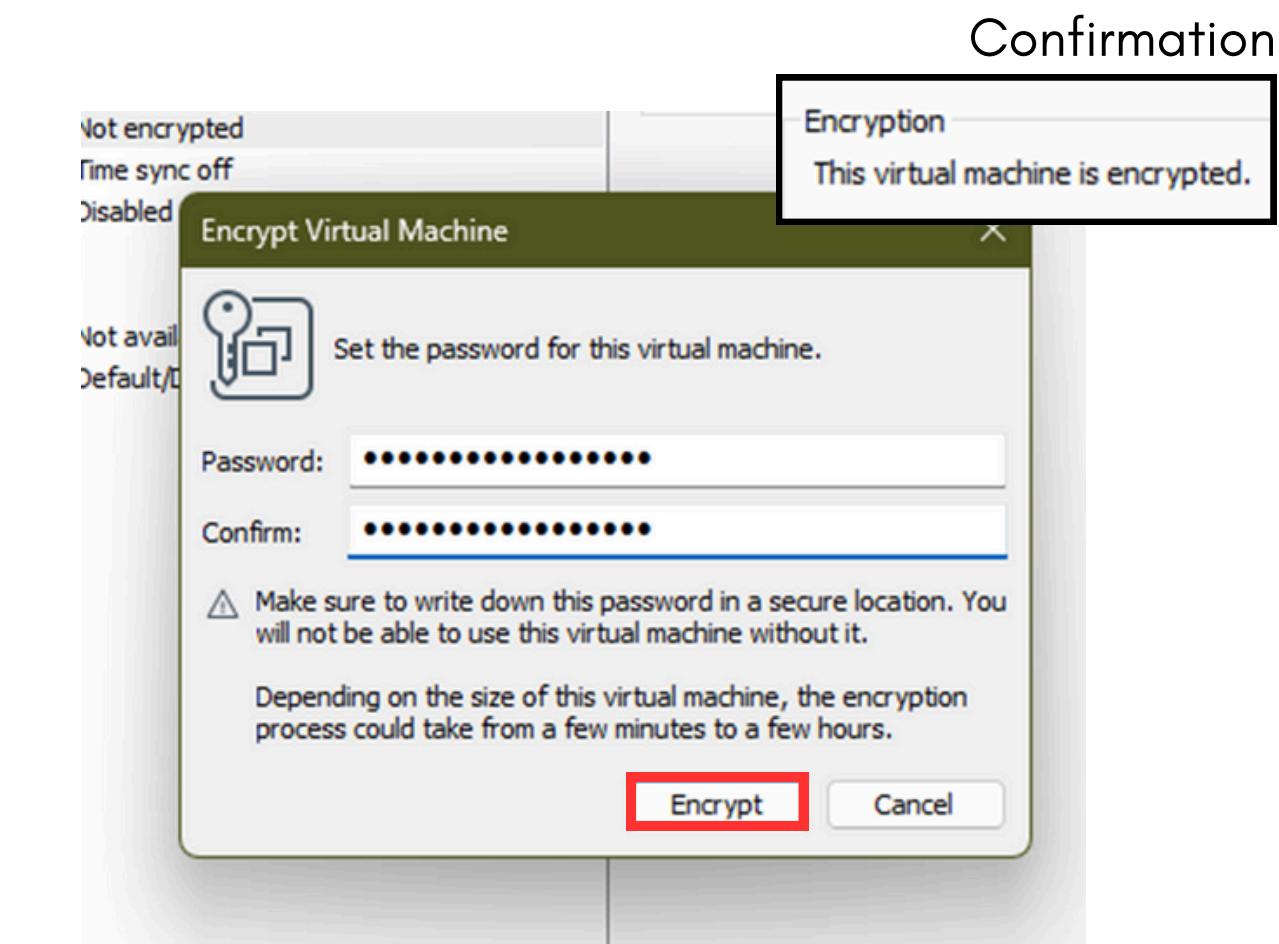
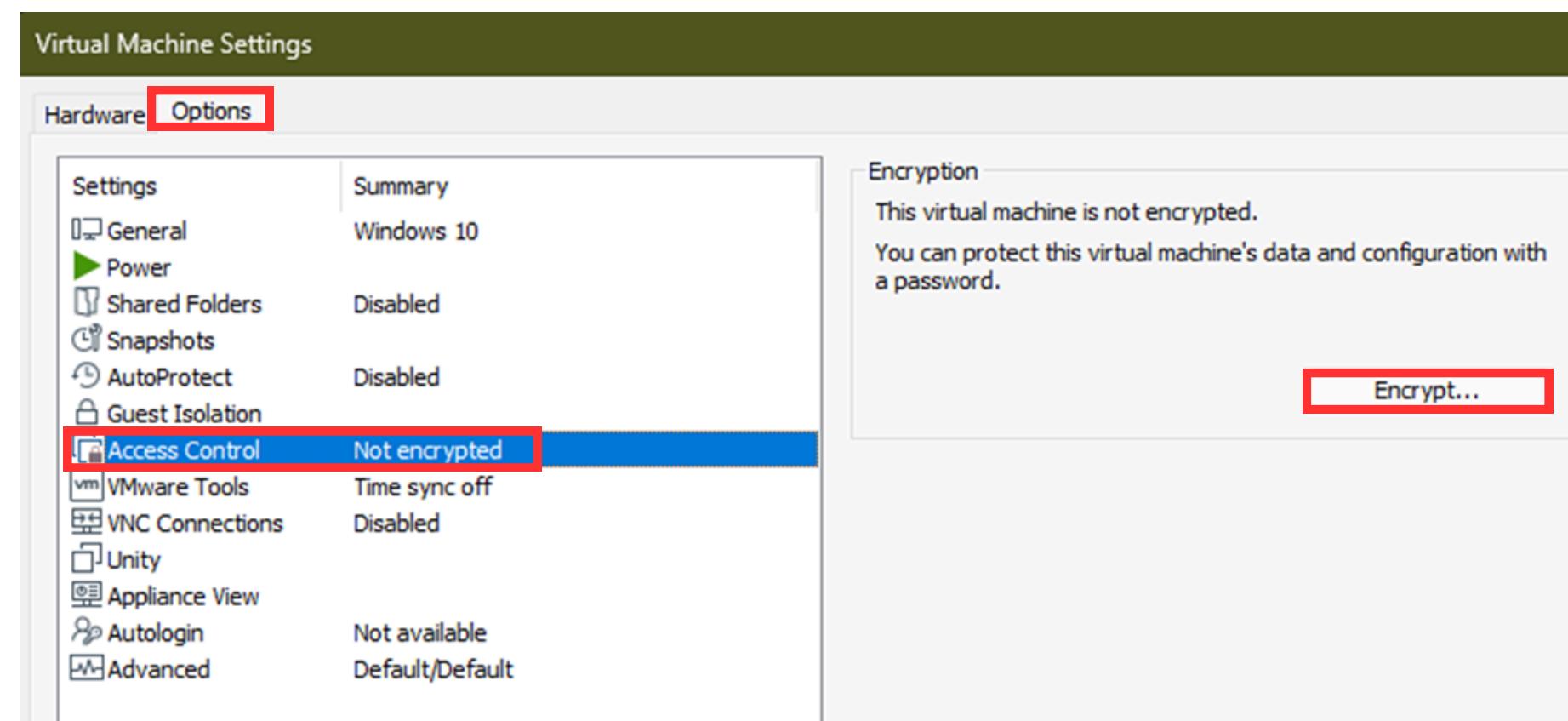
MBR2GPT: Attempting to convert disk 0
MBR2GPT: Retrieving layout of disk
MBR2GPT: Validating layout, disk sector size is: 512 bytes
All BitLocker-encrypted volumes on the disk must have protection suspended.
Cannot get volume information to restore drive letter mapping.
MBR2GPT: Conversion failed
PS C:\WINDOWS\system32> MBR2GPT.EXE /convert /allowfullOS
MBR2GPT will now attempt to convert the default boot disk.
If conversion is successful the disk can only be booted in GPT mode.
These changes cannot be undone!

MBR2GPT: Attempting to convert disk 0
MBR2GPT: Retrieving layout of disk
MBR2GPT: Validating layout, disk sector size is: 512 bytes
MBR2GPT: Trying to shrink the OS partition
```

__tasks

(24) Enable Windows Secure Boot

2. On VMware, access the VM's Settings > Options > Access Control > Encrypt the VM > Fill in a strong password E.g. Th1s1sMYP@ssw0rd\$ > Encrypt

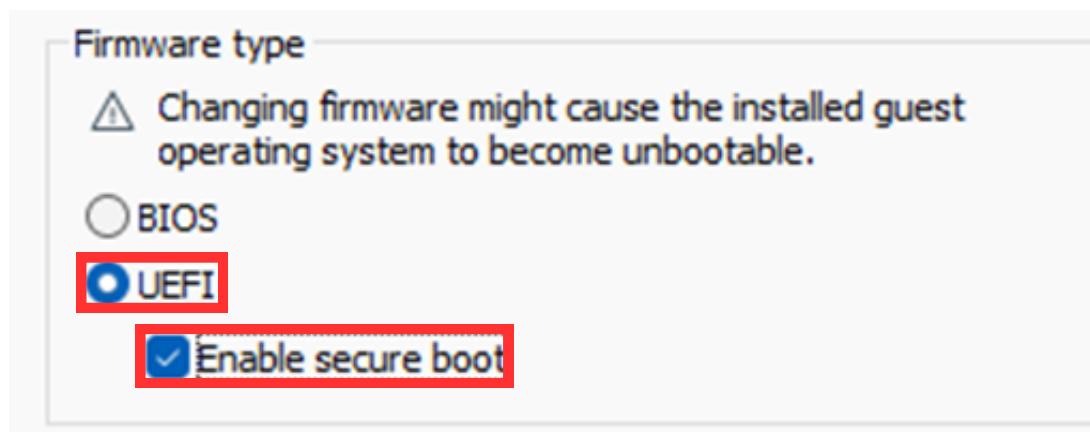


protection and backups

tasks

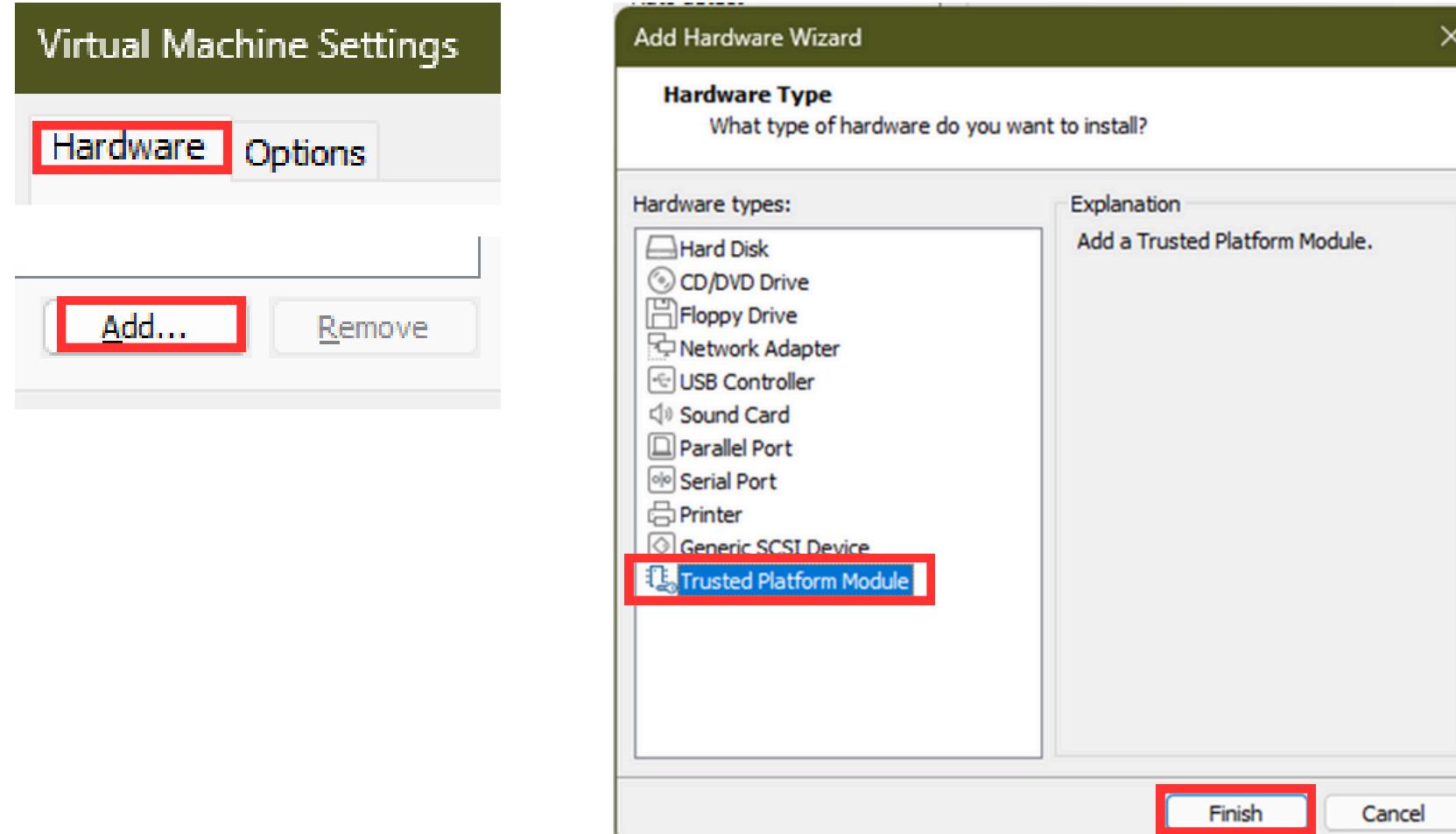
(24) Enable Windows Secure Boot

3. On the same Options tab > Advanced > Firmware type > Switch from BIOS to UEFI with secure boot enabled.



protection and backups

3. On the Hardware tab > Add... > Trusted Platform Module > Finish

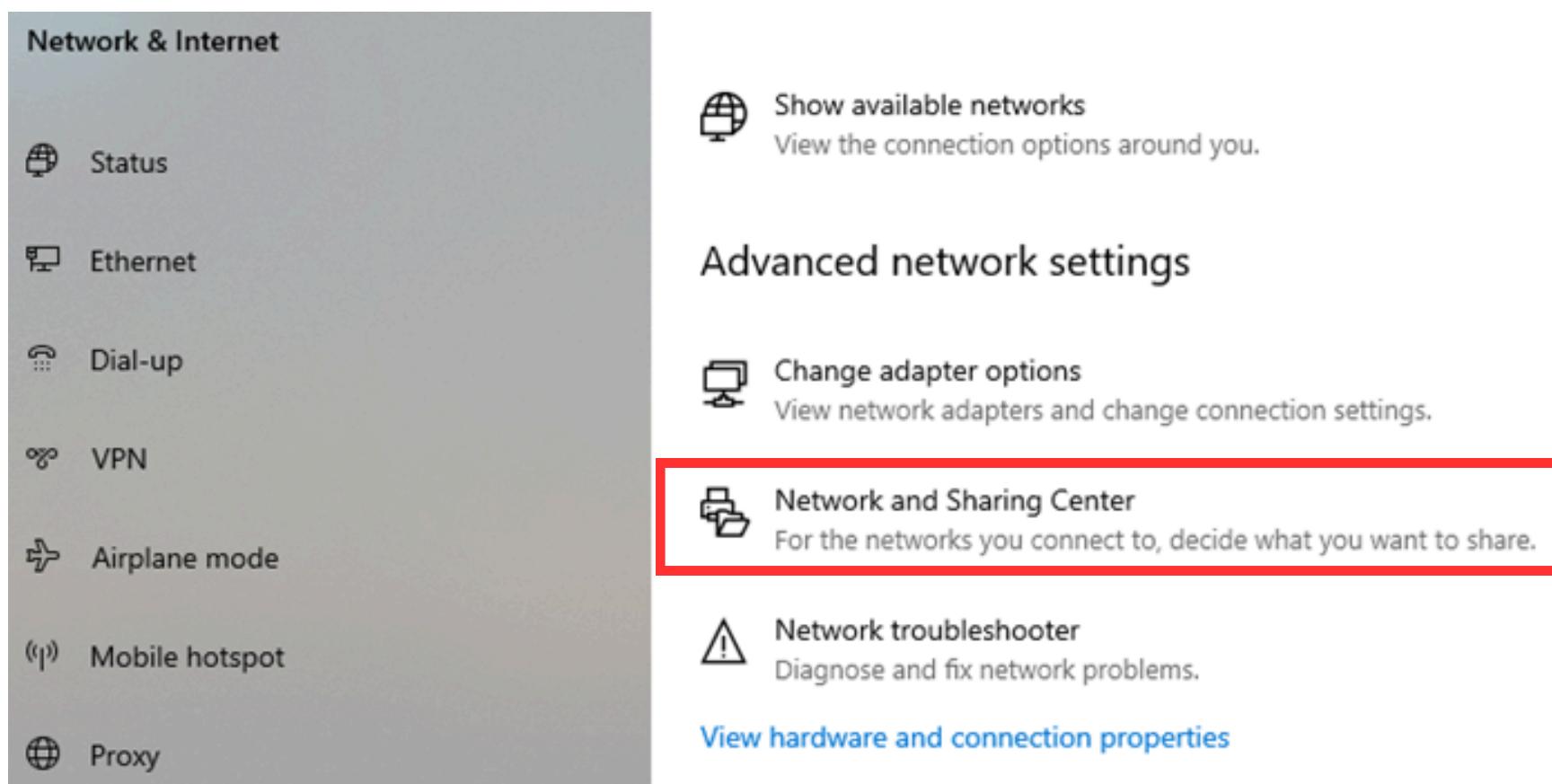


You will now be able to boot with UEFI + Secure Boot + have a TPM (more security).

_tasks

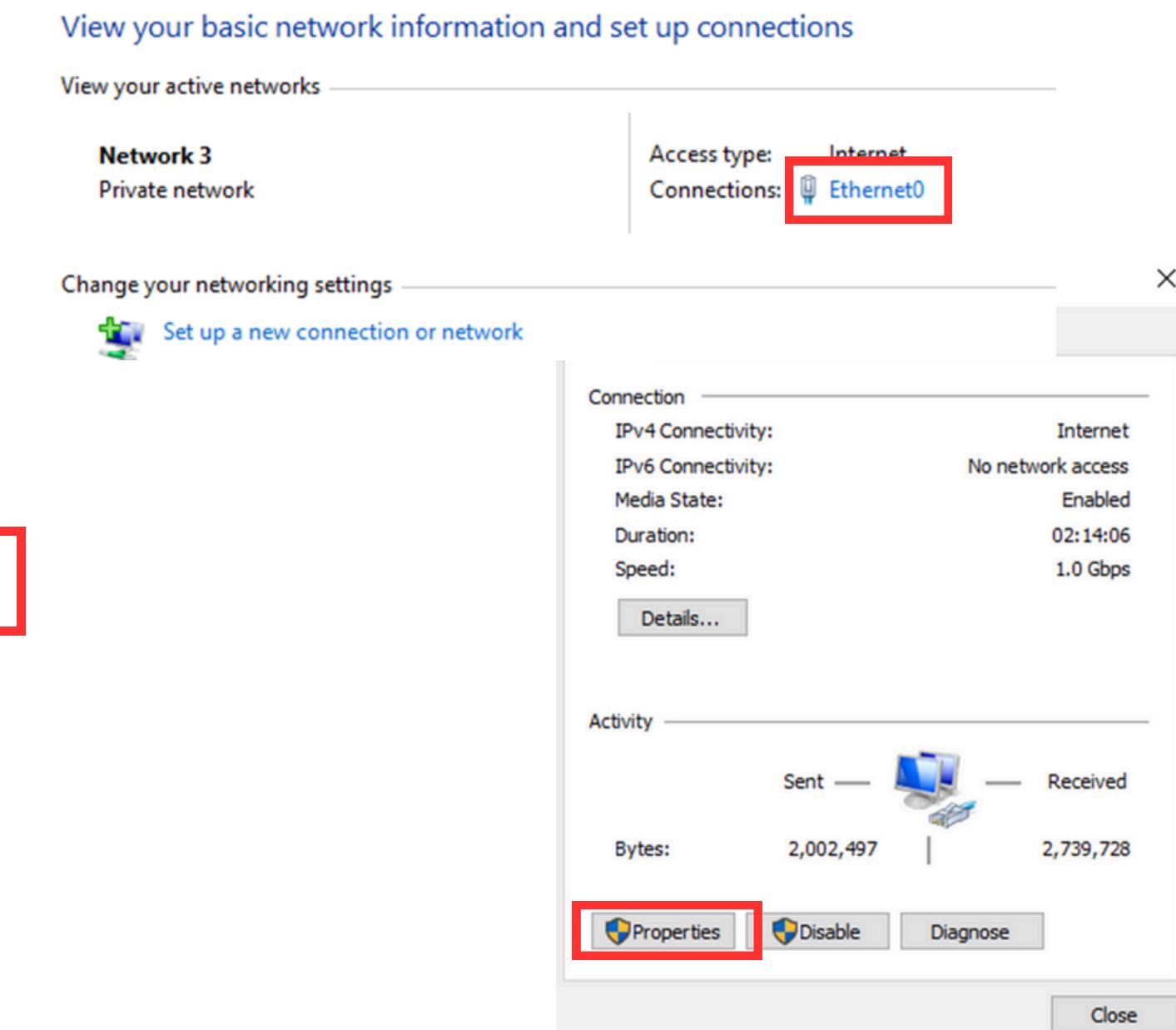
(33) DNS-over-HTTPS (DoH) for Encrypted DNS Queries

1. Settings > Network & Internet > Advanced network settings > Network and Sharing Center



protection and backups

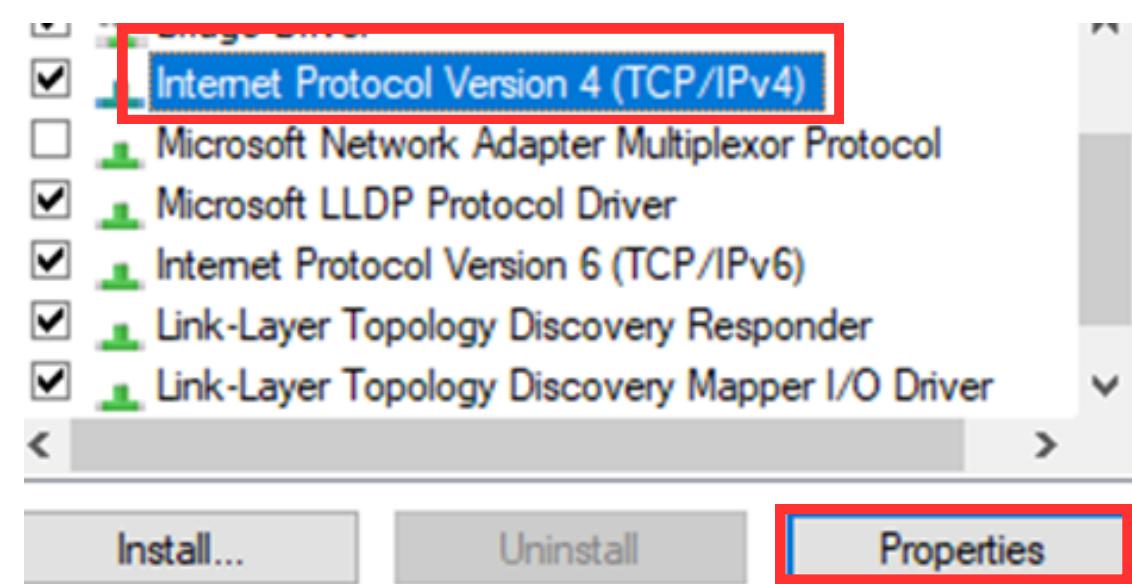
2. Click on your network (Ethernet0) > Properties



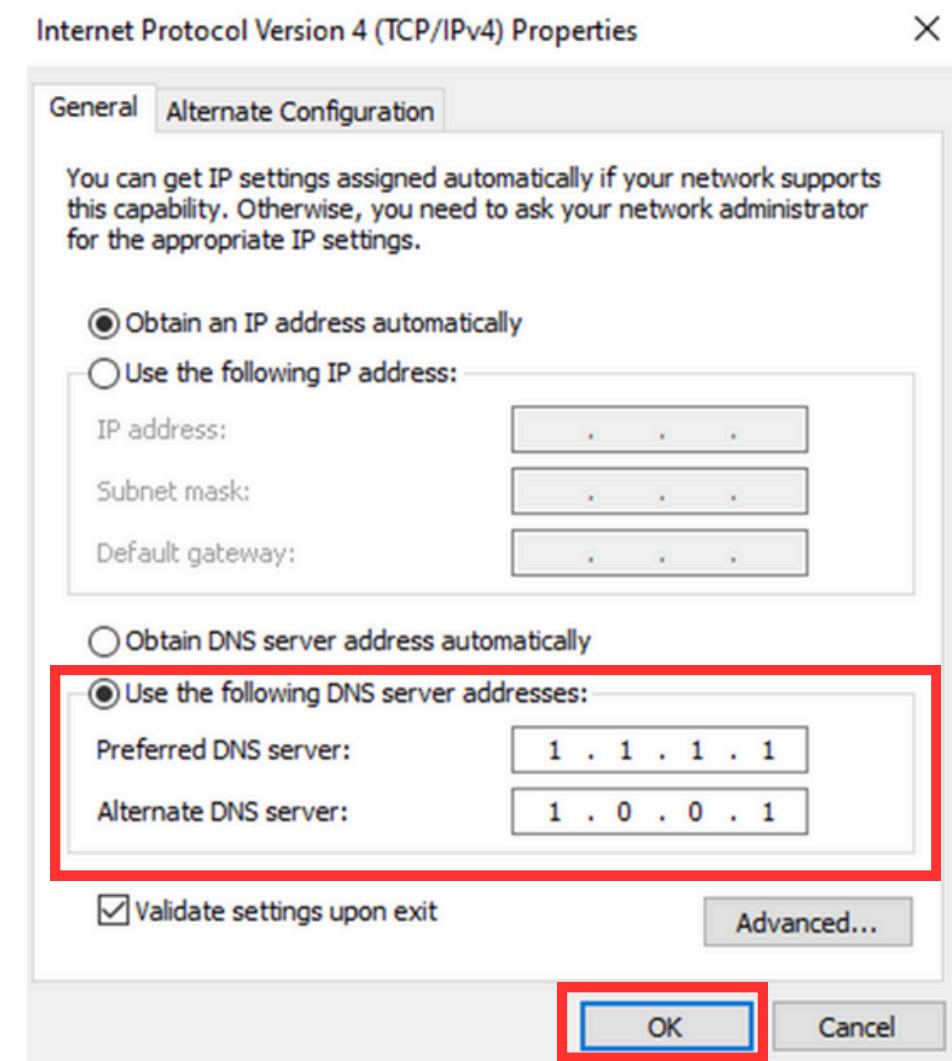
tasks

(33) DNS-over-HTTPS (DoH) for Encrypted DNS Queries

2. Now head to Internet Protocol 4 (TCP/IPv4) > Properties



Enter the following DNS addresses (both are Cloudflare DNS-s) > OK.



All in all, Encrypts DNS queries to prevent outsiders from tracking or tampering with the websites you access.

protection and backups

system security and account management



by Jia Xiang

tasks

done by Jia Xiang

- (1) Verify that All Disk Partitions are Formatted with NTFS
- (2) Ensure Guest Account is Disabled
- (3) Disable or Delete Unnecessary Accounts
- (4) Use Account Passwords
- (5) Set Stronger Password Policies
- (6) Set Account Lockout Policy
- (16) Secure System from PowerShell Exploits

- (30) Create groups for easier account management

- (a) Group Creation
 - (b) Adding Members

- (31) Implementing Role-Based Access control

base tasks

additional tasks

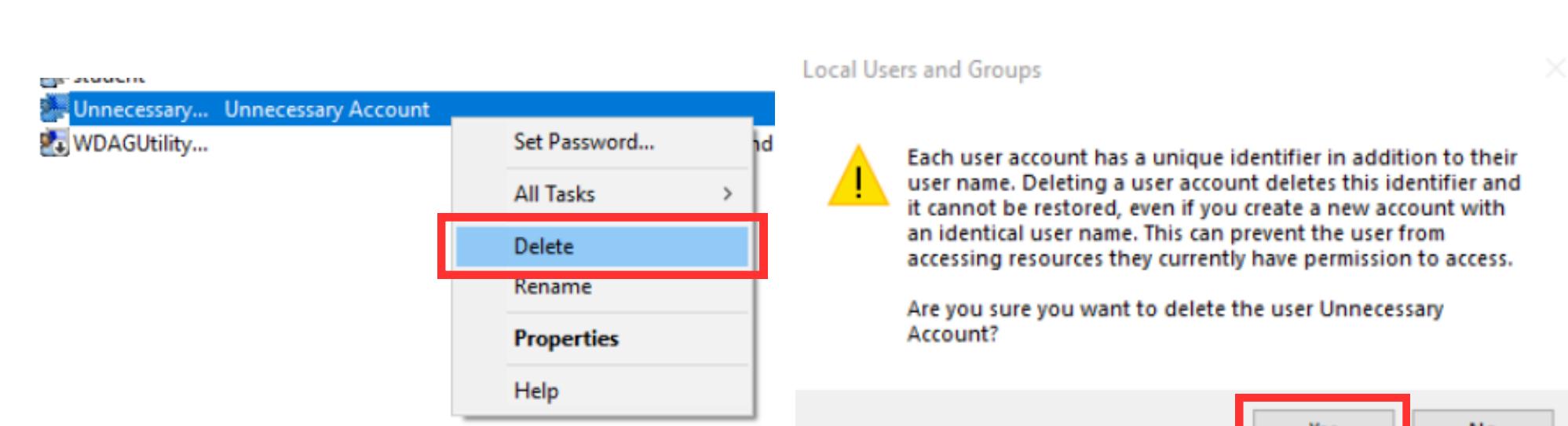
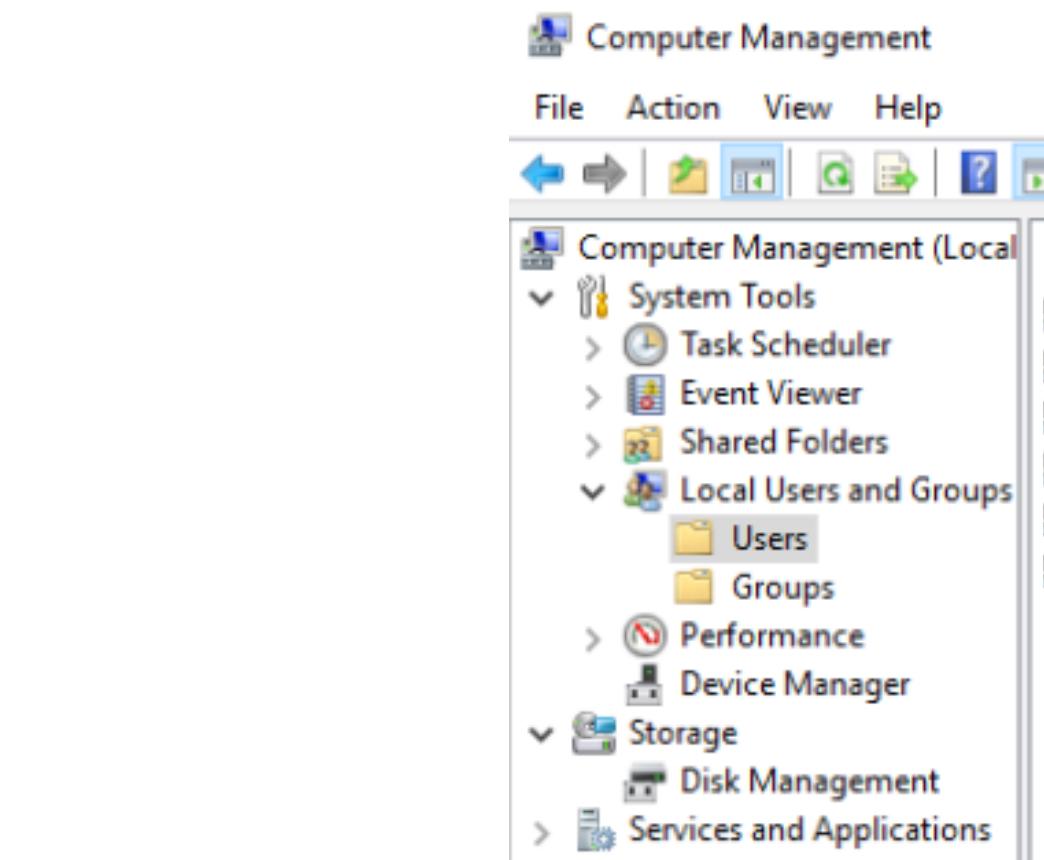
system security and account management

tasks

(3) Disable or Delete any unnecessary accounts

1. In Computer Management, navigate to “Users”.

Path: System Tools → Local Users and Groups → Users



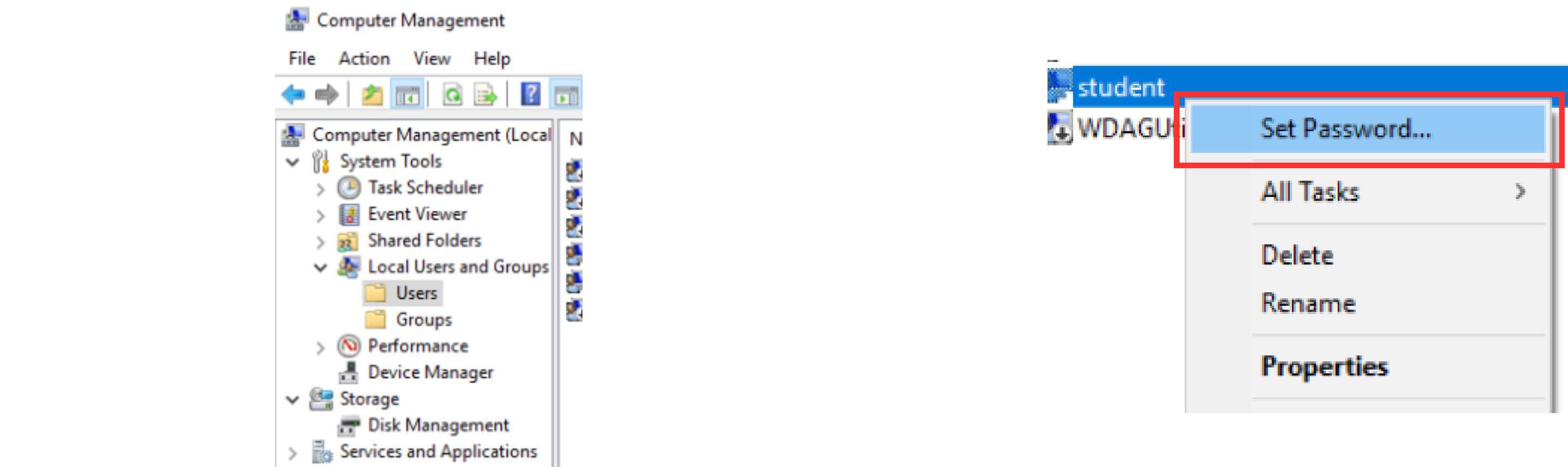
system security and account management

_tasks

(4) Use Account Password

1. In Computer Management, navigate to “Users”.

Path: System Tools → Local Users and Groups → Users

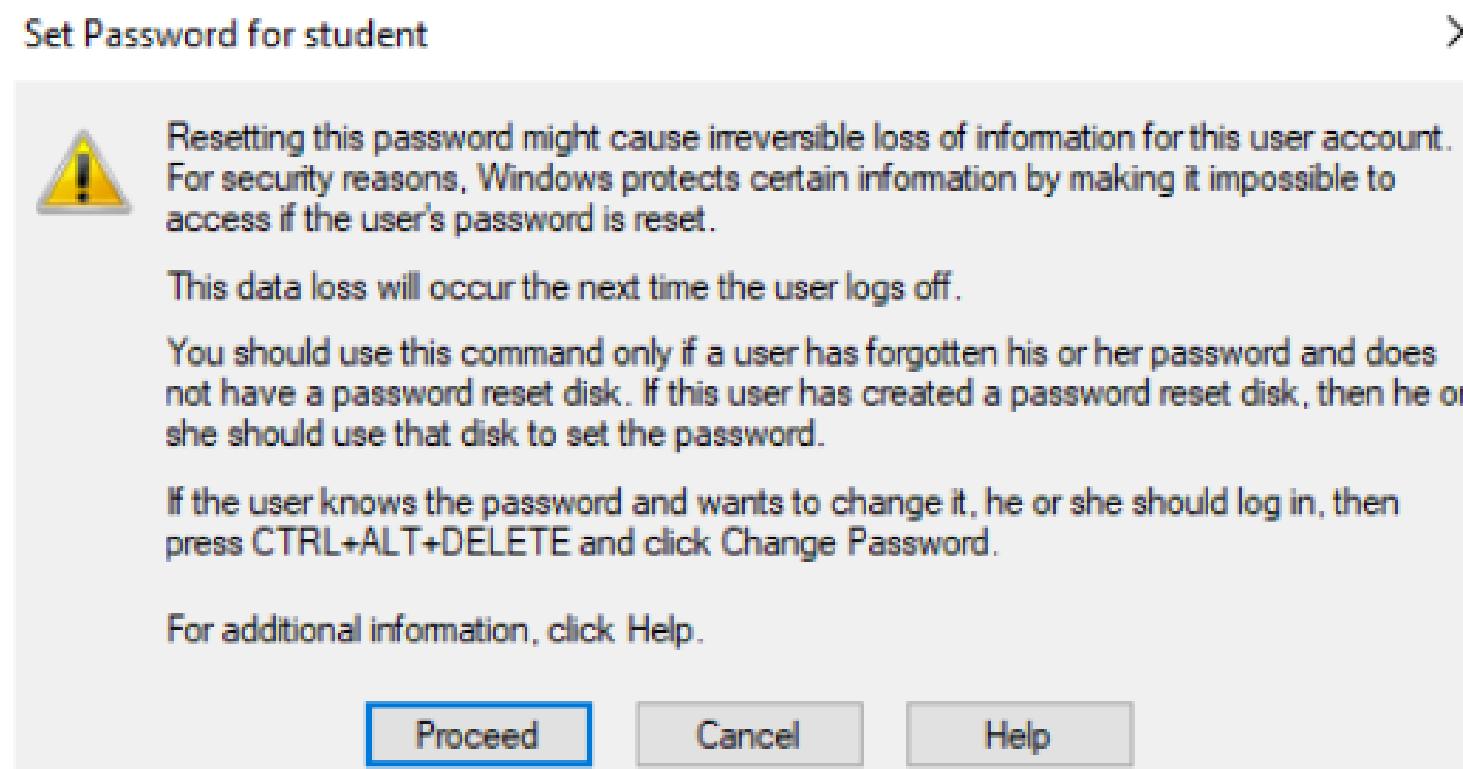


system security and account management

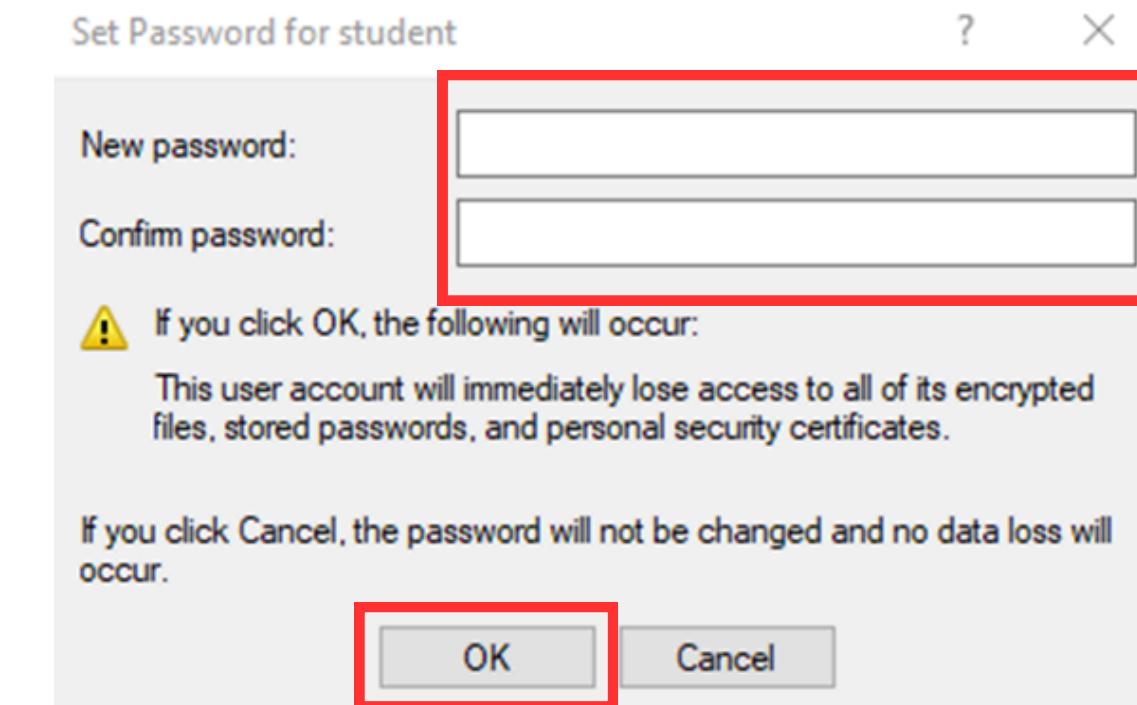
tasks

(4) Use Account Password

3. Click proceed and then set the password for the user



Click OK once the password is set

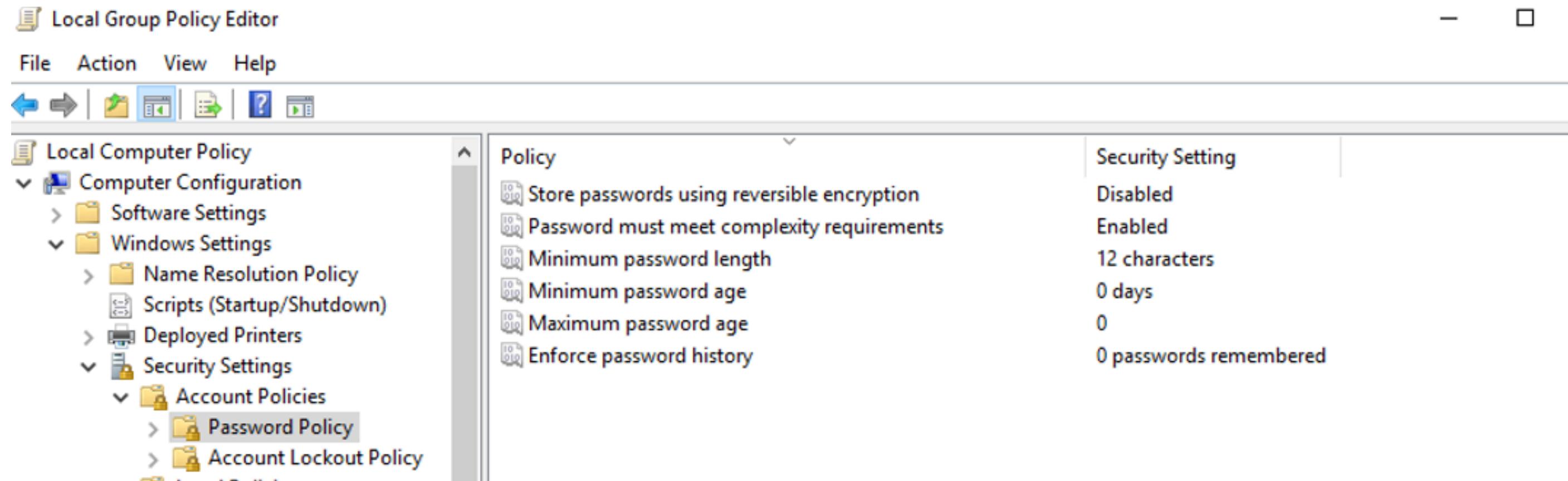


tasks

(5) Set Stronger Password Policies

1. In the Local Group Policy Editor, go to Password Policy.

Path: Computer Configuration → Windows Settings → Security Settings → Account Policy → Password Policy



tasks

(5) Set Stronger Password Policies

3. Set minimum password length to 12,

Set "Password must meet complexity requirements" to enabled,

Set "Store passwords using reversible encryption" to enabled

Click Apply in the window that pops up in after a change



Minimum password length

12 characters



Password must meet complexity requirements

Enabled



Store passwords using reversible encryption

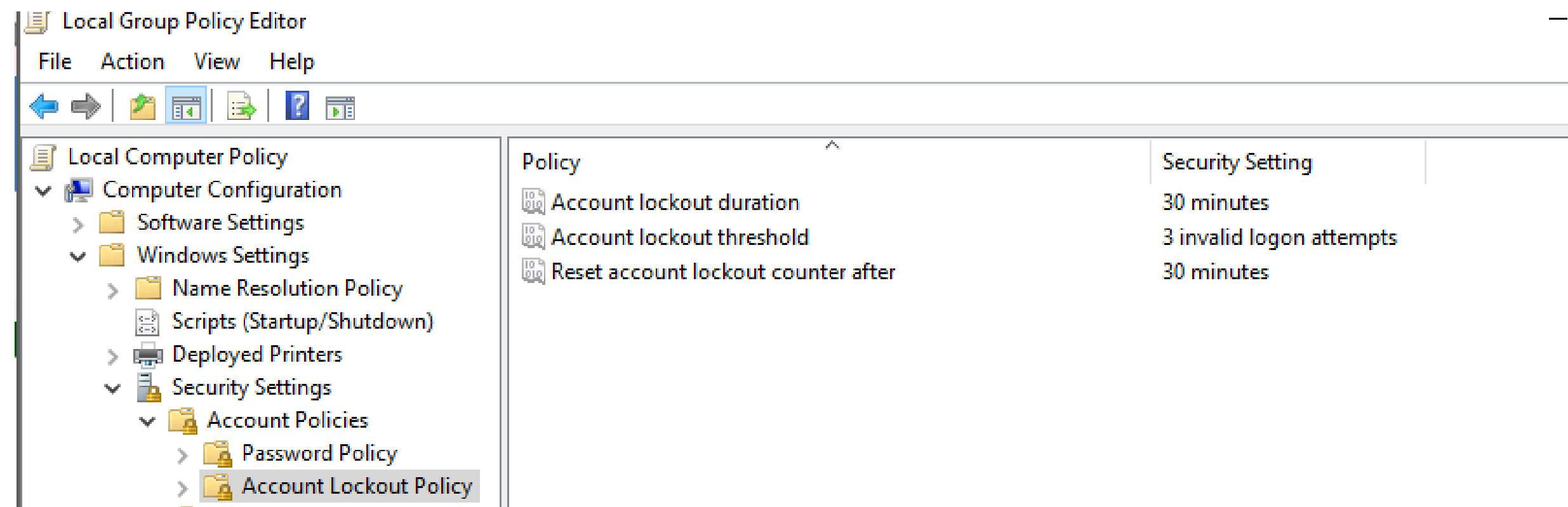
Enabled

tasks

(6) Set Stronger Password Policies

3. Inside of Local Group Policy Editor, go to Account Lockout Policy

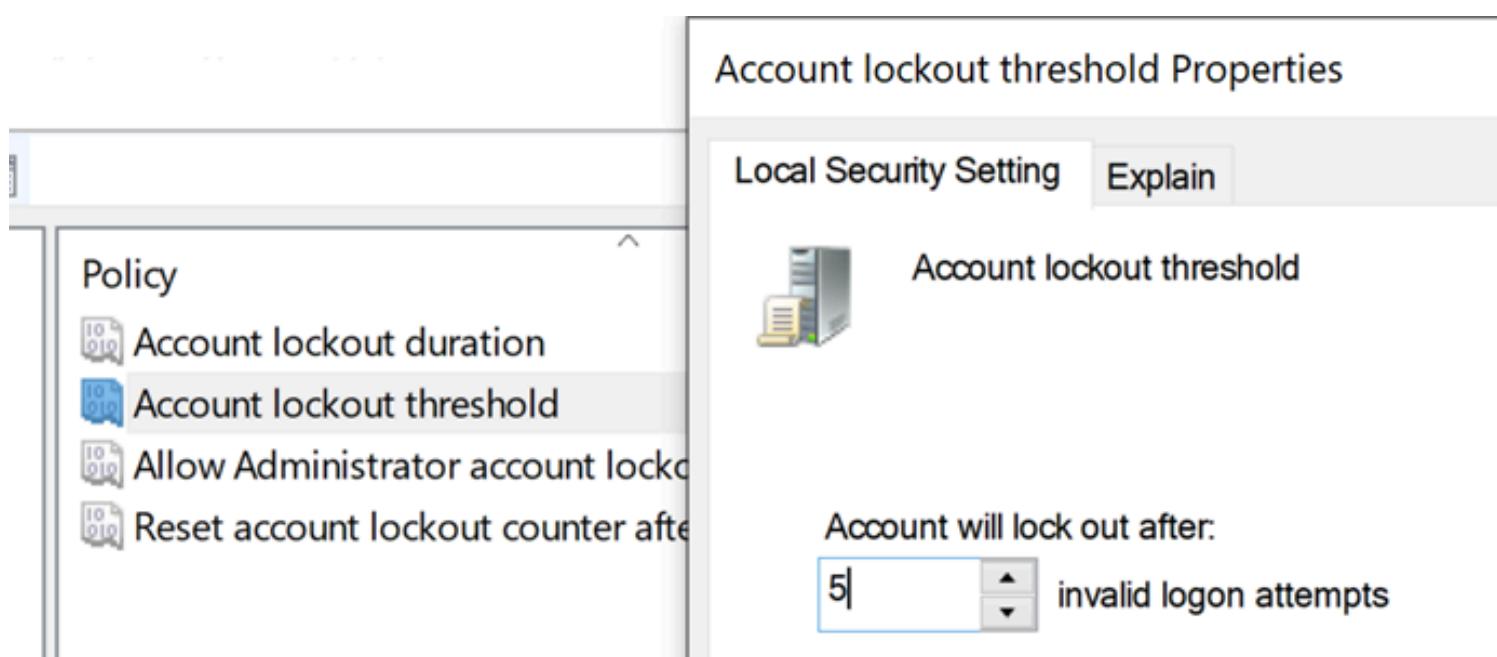
Path: Computer Configuration → Windows Settings → Security Settings → Account Policy → Account Lockout Policy



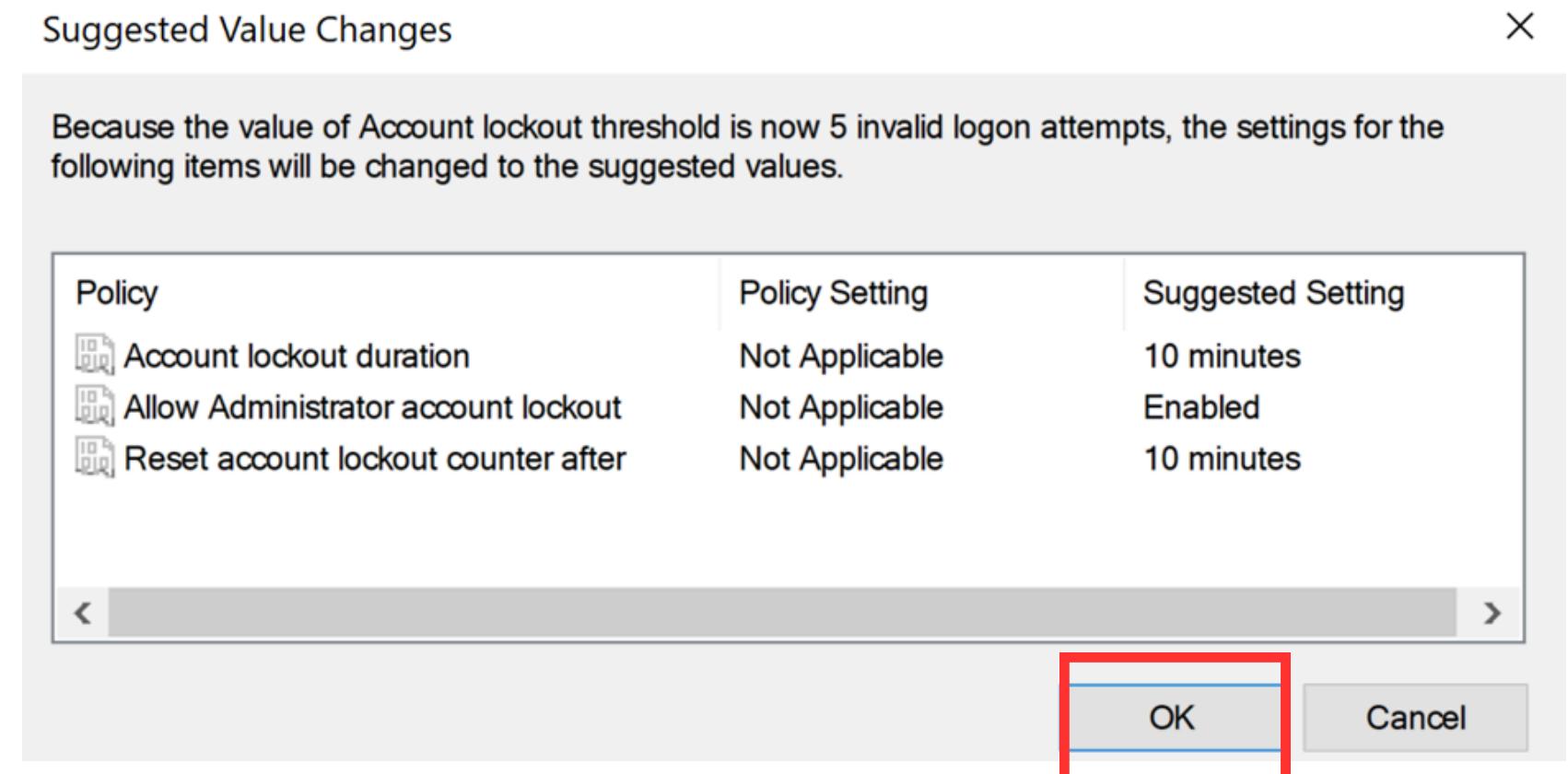
tasks

(6) Set Stronger Password Policies

3. Change “Account lockout threshold” from 0 to and click apply



Click OK to the prompt that pops up.

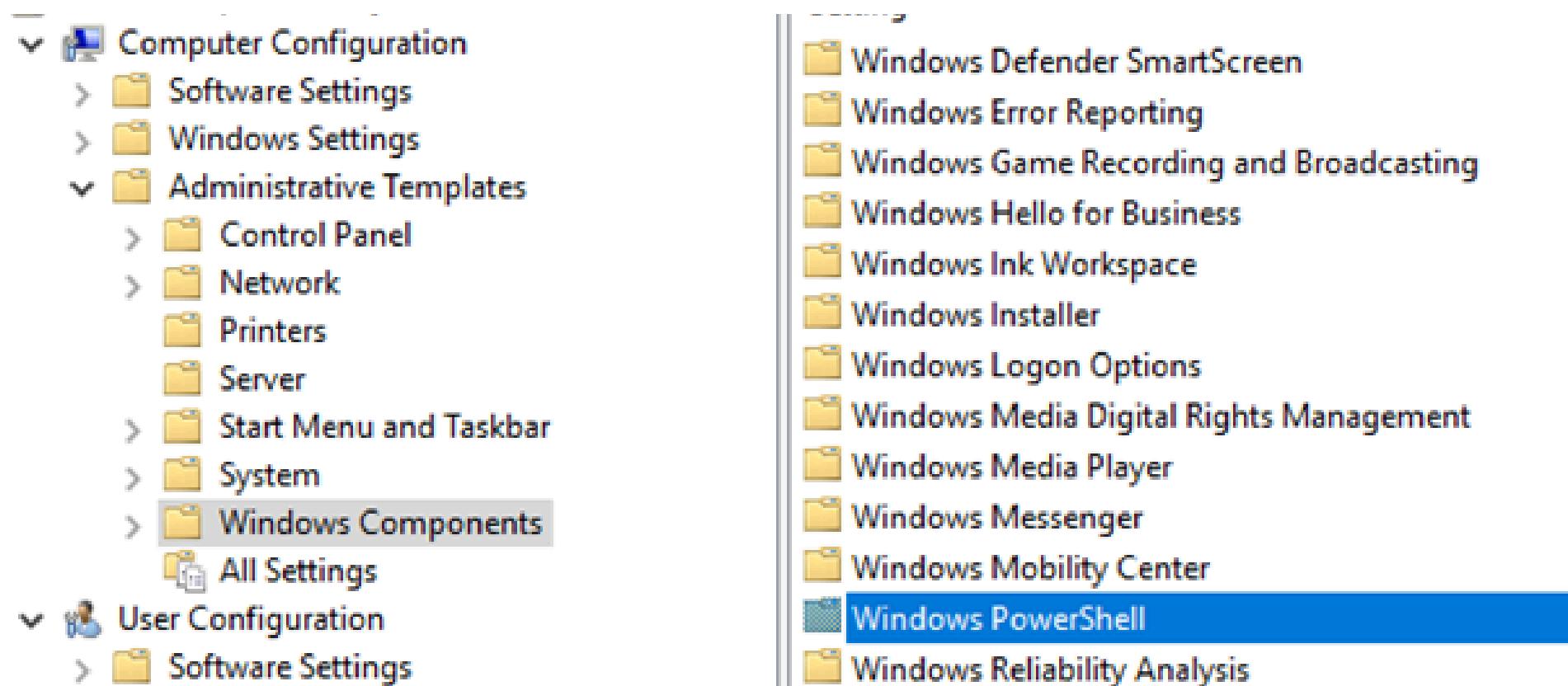


_tasks

(16) Secure System from PowerShell Exploits

1. Inside of Local Group Policy Editor, go to Account Lockout Policy

Path: Computer Configuration → Administrative Templates → Windows Components → Windows PowerShell



All the settings should be Not configured

Setting	State	Comment
Turn on Module Logging	Not configured	No
Turn on PowerShell Script Block Logging	Not configured	No
Turn on Script Execution	Not configured	No
Turn on PowerShell Transcription	Not configured	No
Set the default source path for Update-Help	Not configured	No

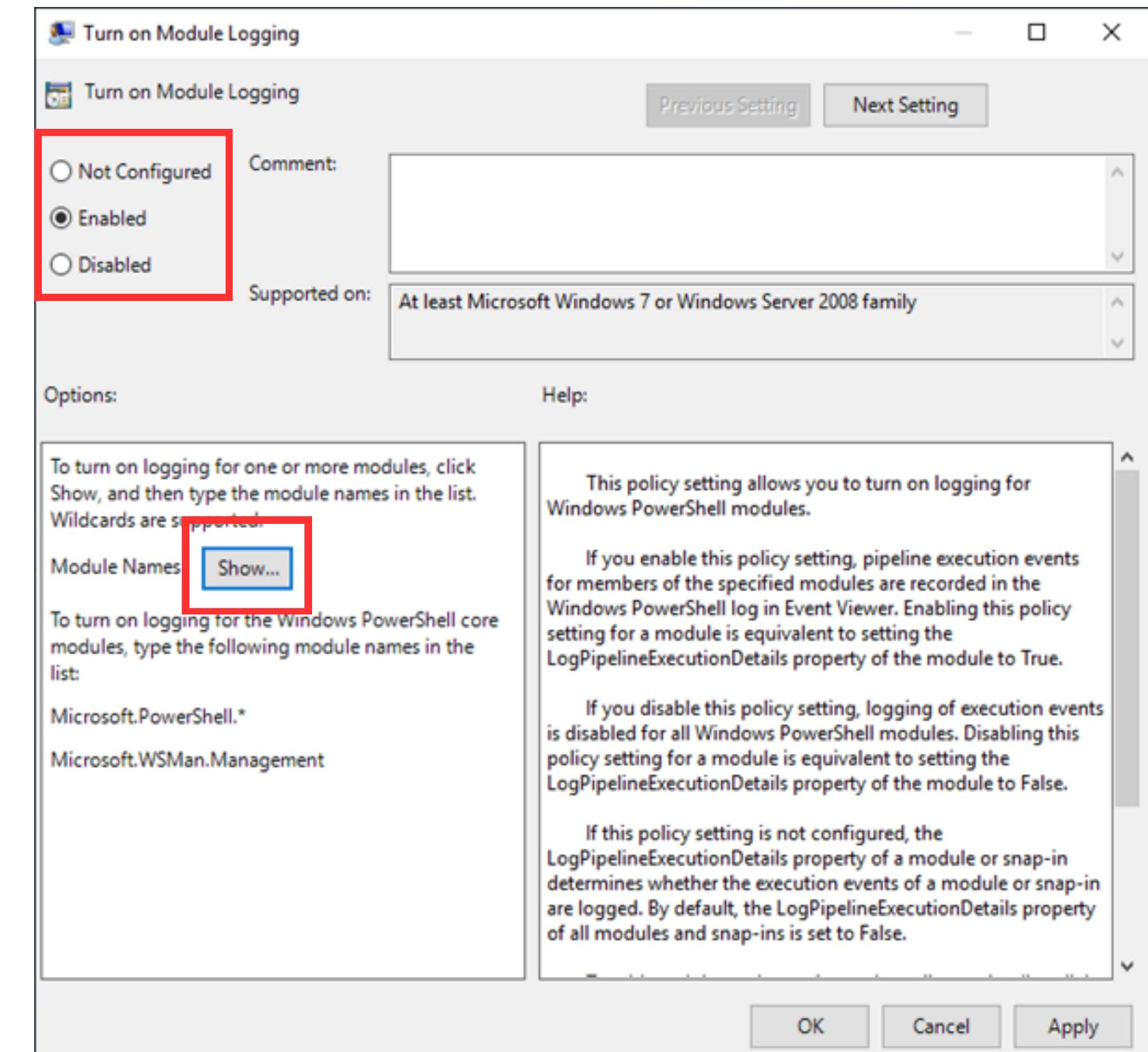
This means PowerShell exploits can run and not be detected

tasks

(16) Secure System from PowerShell Exploits

2. Click "Turn on Module Logging"
 - Inside of this setting, set it to enabled
then click show

Setting	State
Turn on Module Logging	Not configured
Turn on PowerShell Script Block Logging	Not configured
Turn on Script Execution	Not configured
Turn on PowerShell Transcription	Not configured
Set the default source path for Update-Help	Not configured

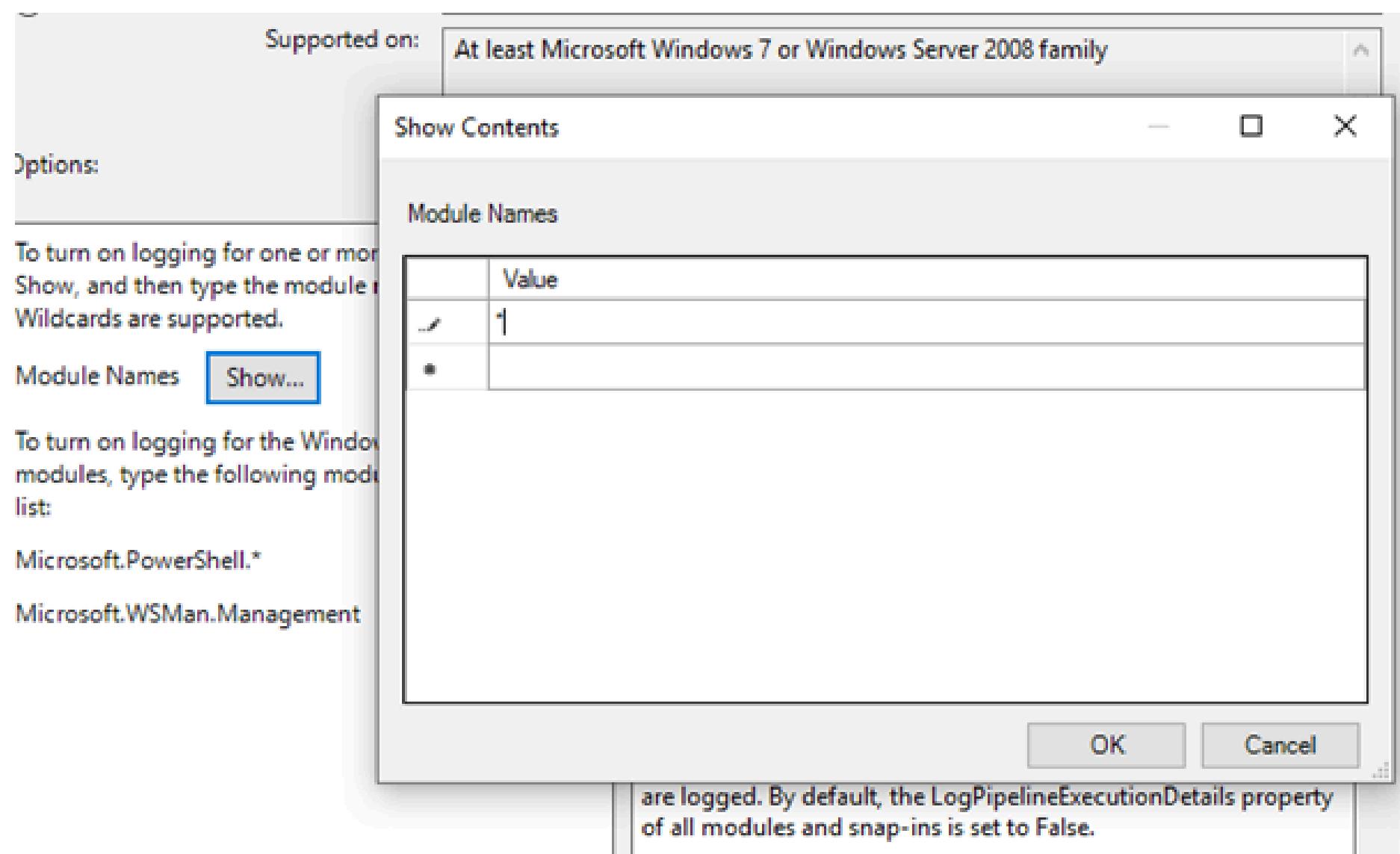


_tasks

(16) Secure System from PowerShell Exploits

After clicking on show, a new window will pop up.
Inside the table, enter "*" as seen in the picture then
click OK then apply

This will cause the computer to log all the scripts that
are run



tasks

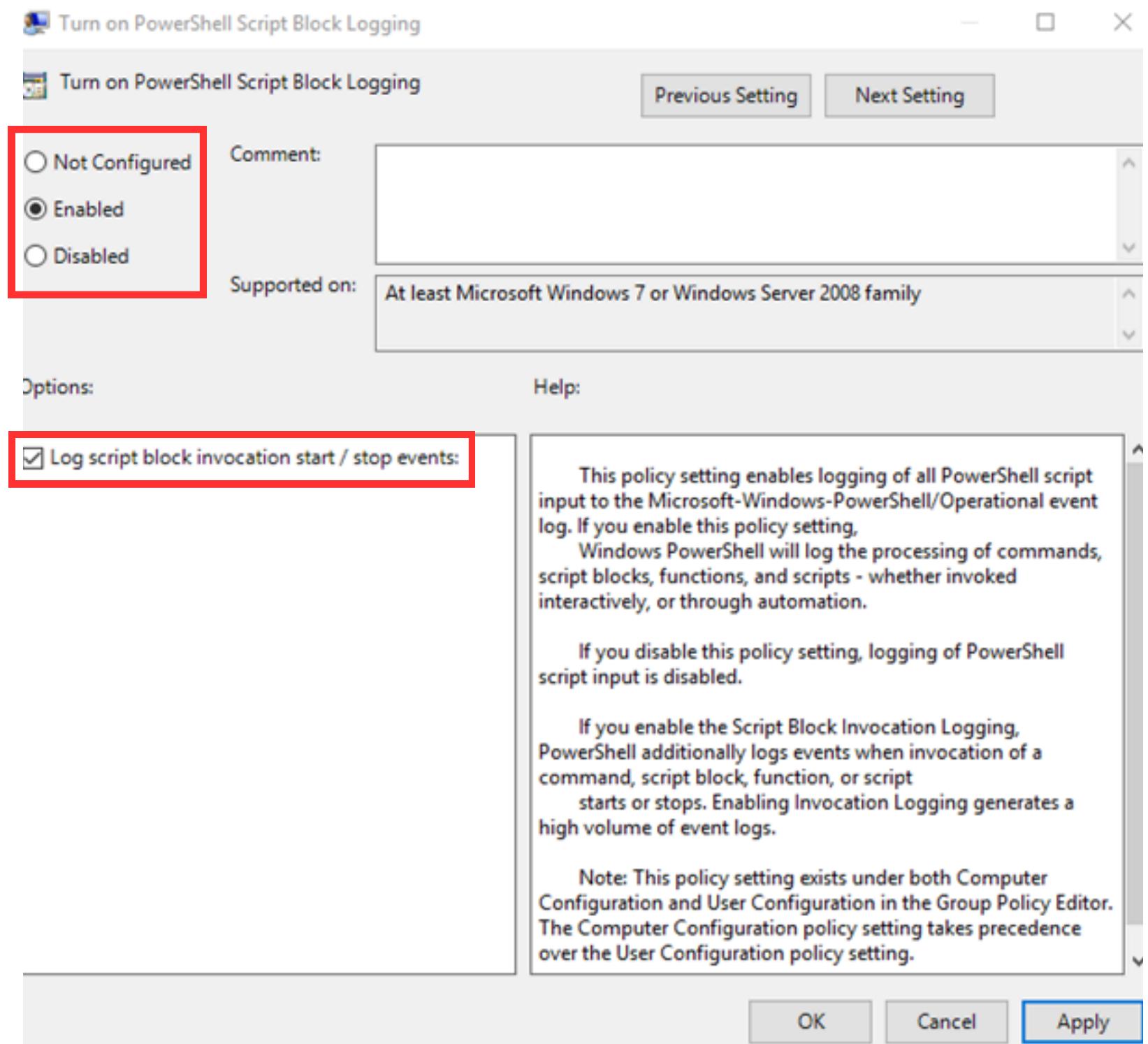
(16) Secure System from PowerShell Exploits

3. Click "Turn on PowerShell Script Block Logging".
 - Inside of this setting, set it to enabled.
 - Check "Log script block invocation start / stop events"
 - Click Apply

Setting	State
Turn on Module Logging	Not configured
Turn on PowerShell Script Block Logging	Not configured
Turn on Script Execution	Not configured
Turn on PowerShell Transcription	Not configured
Set the default source path for Update-Help	Not configured

This will log all blocked scripts when enabled

system security and account management



tasks

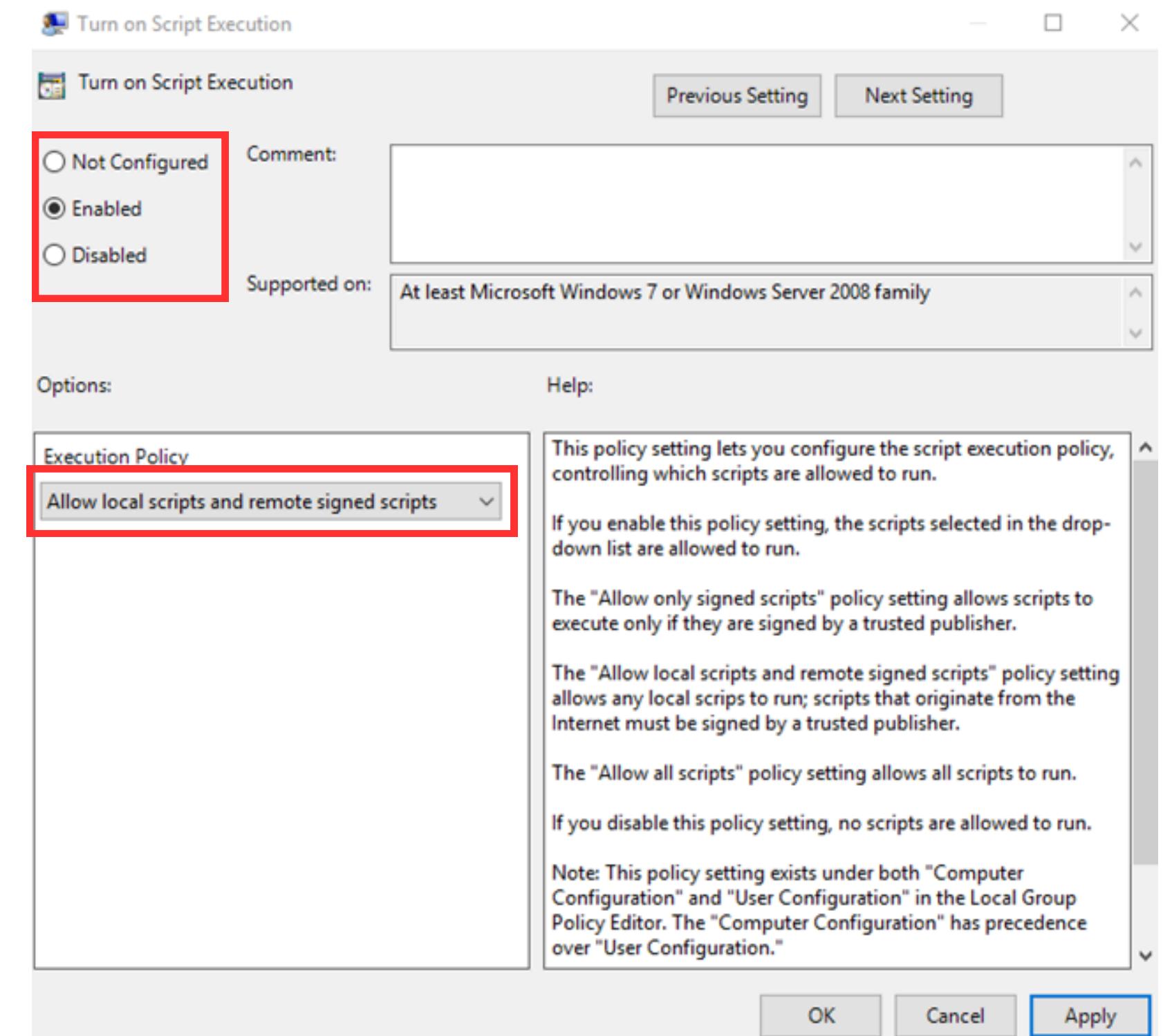
(16) Secure System from PowerShell Exploits

4. Click "Turn on Script Execution"

- Inside of this setting, set it to enabled.
- Set execution policy to only "Allow local scripts and remote signed scripts"
- Click Apply

Setting	State
Turn on Module Logging	Not configured
Turn on PowerShell Script Block Logging	Not configured
Turn on Script Execution	Not configured
Turn on PowerShell Transcription	Not configured
Set the default source path for Update-Help	Not configured

This setting will only allow local scripts and remote signed scripts to run. E.g. Microsoft signed scripts

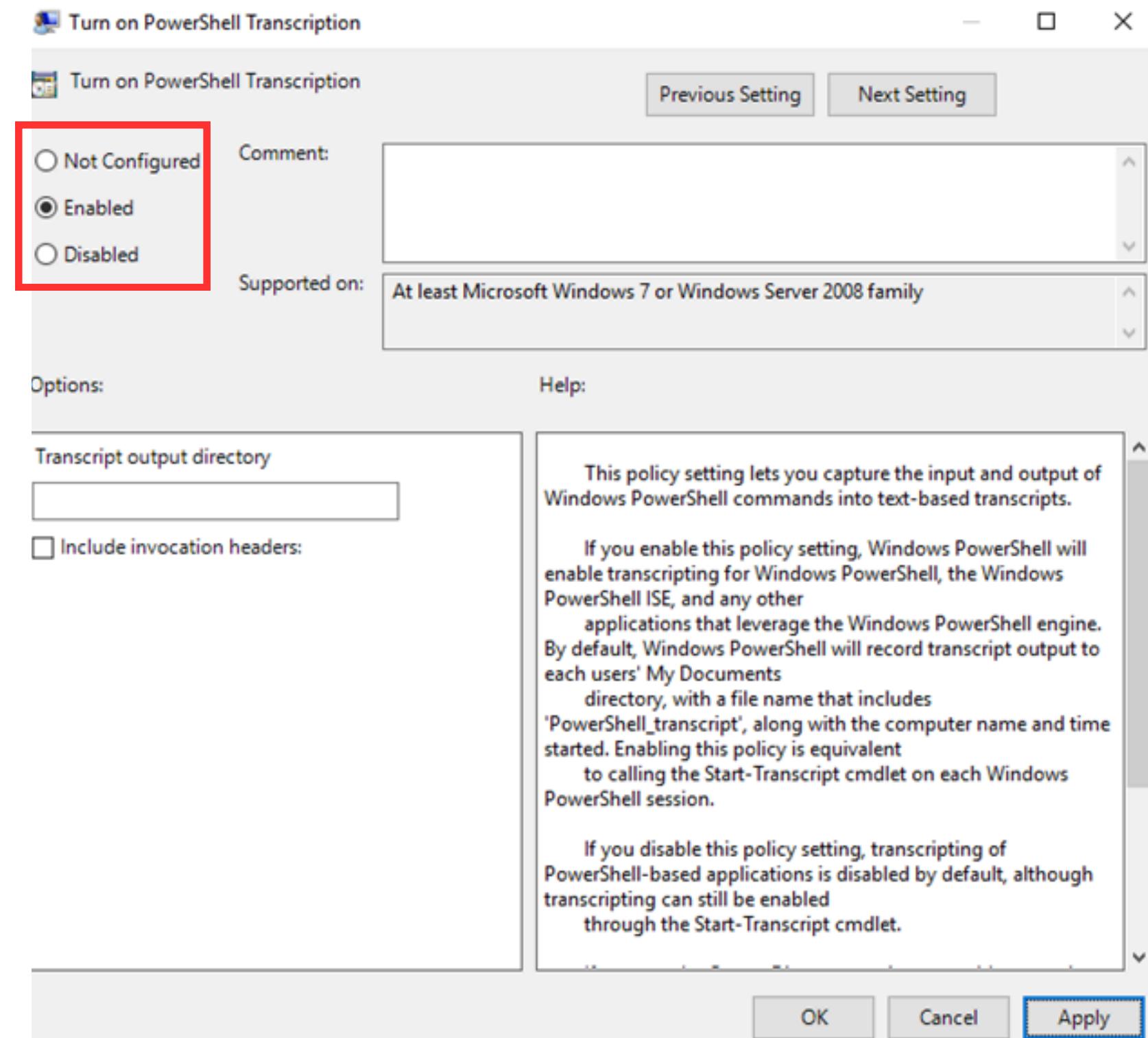


tasks

(16) Secure System from PowerShell Exploits

5. Click “Turn on PowerShell transcription”
 - Inside of this setting, set it to enabled.
 - Click Apply

Setting	State
Turn on Module Logging	Not configured
Turn on PowerShell Script Block Logging	Not configured
Turn on Script Execution	Not configured
Turn on PowerShell Transcription	Not configured
Set the default source path for Update-Help	Not configured



tasks

(30) Create groups for easier account management

1. In the Computer Management dialog box, navigate to "Groups".
2. Click on Action > click on "New group..."

Path: System Tools → Local Users and Groups → Groups

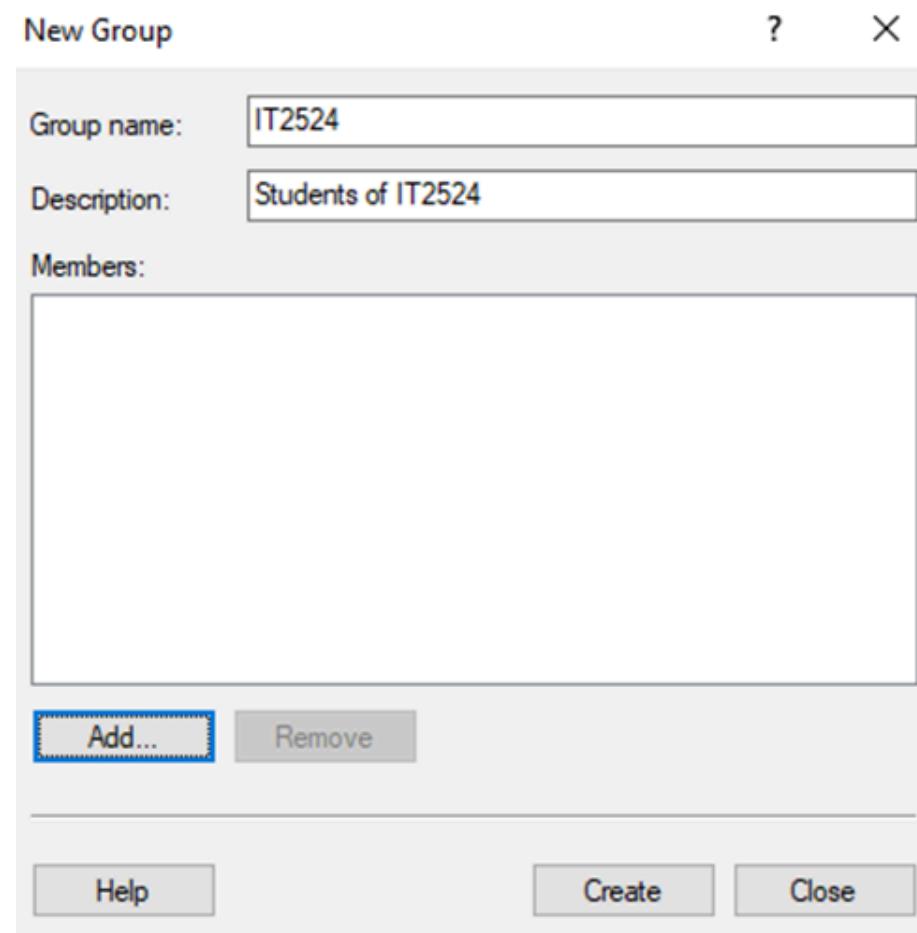


system security and account management

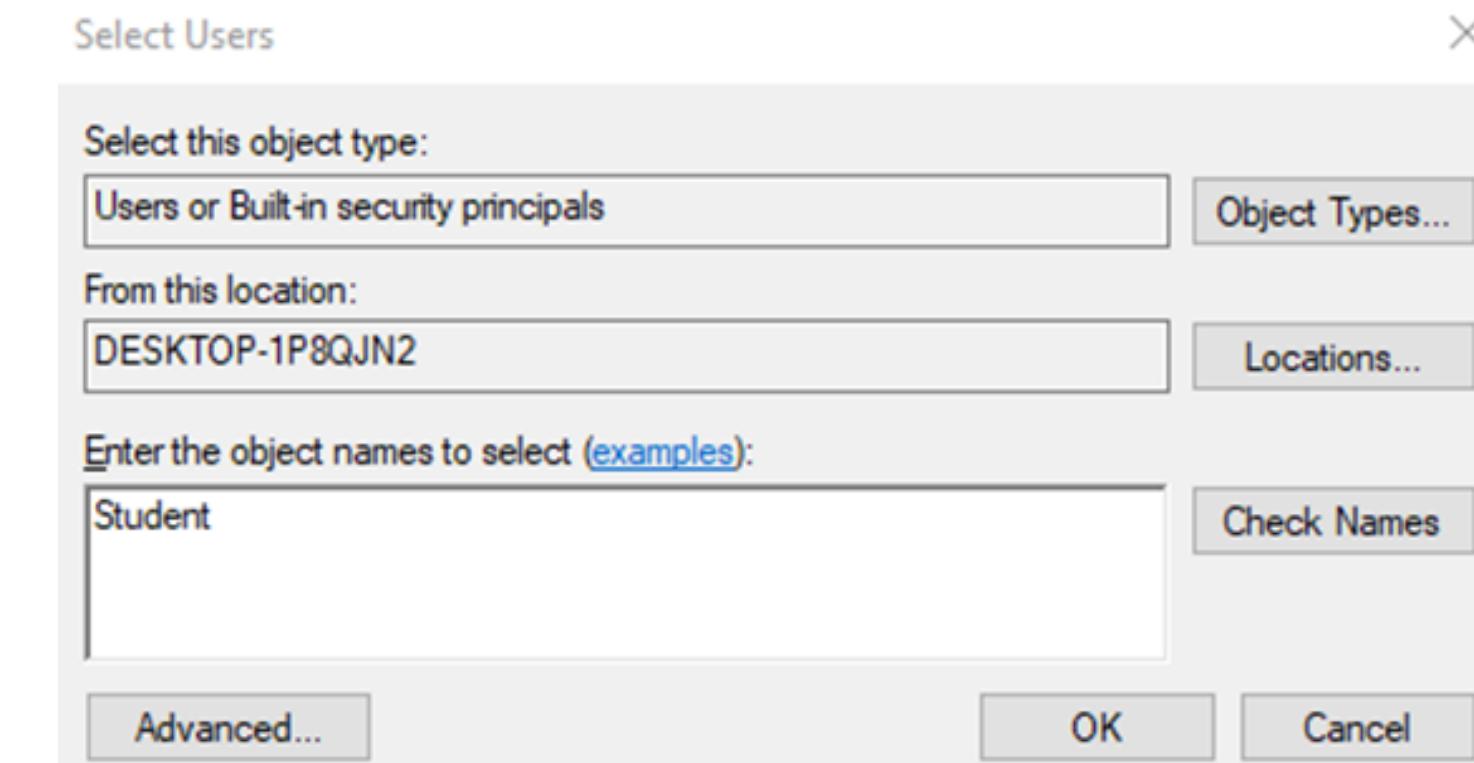
tasks

(30) Create groups for easier account management

3. Enter group name and description > Click “Add”



Enter name of user then click ok



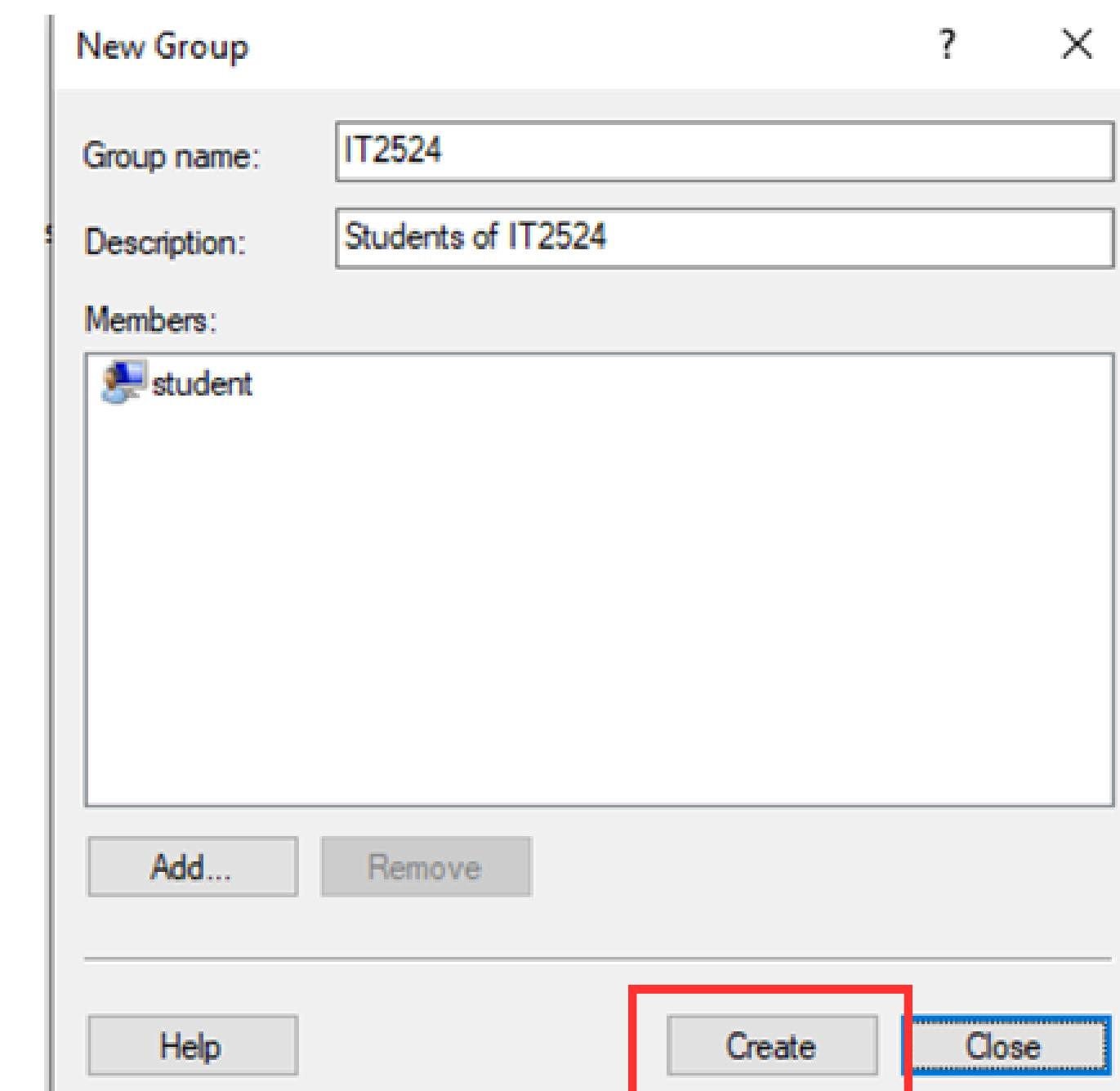
system security and account management

tasks

(30) Create groups for easier account management

3. Click Create

Before creating, you can check if you have all the members inside of the group inside the members section



system security and account management

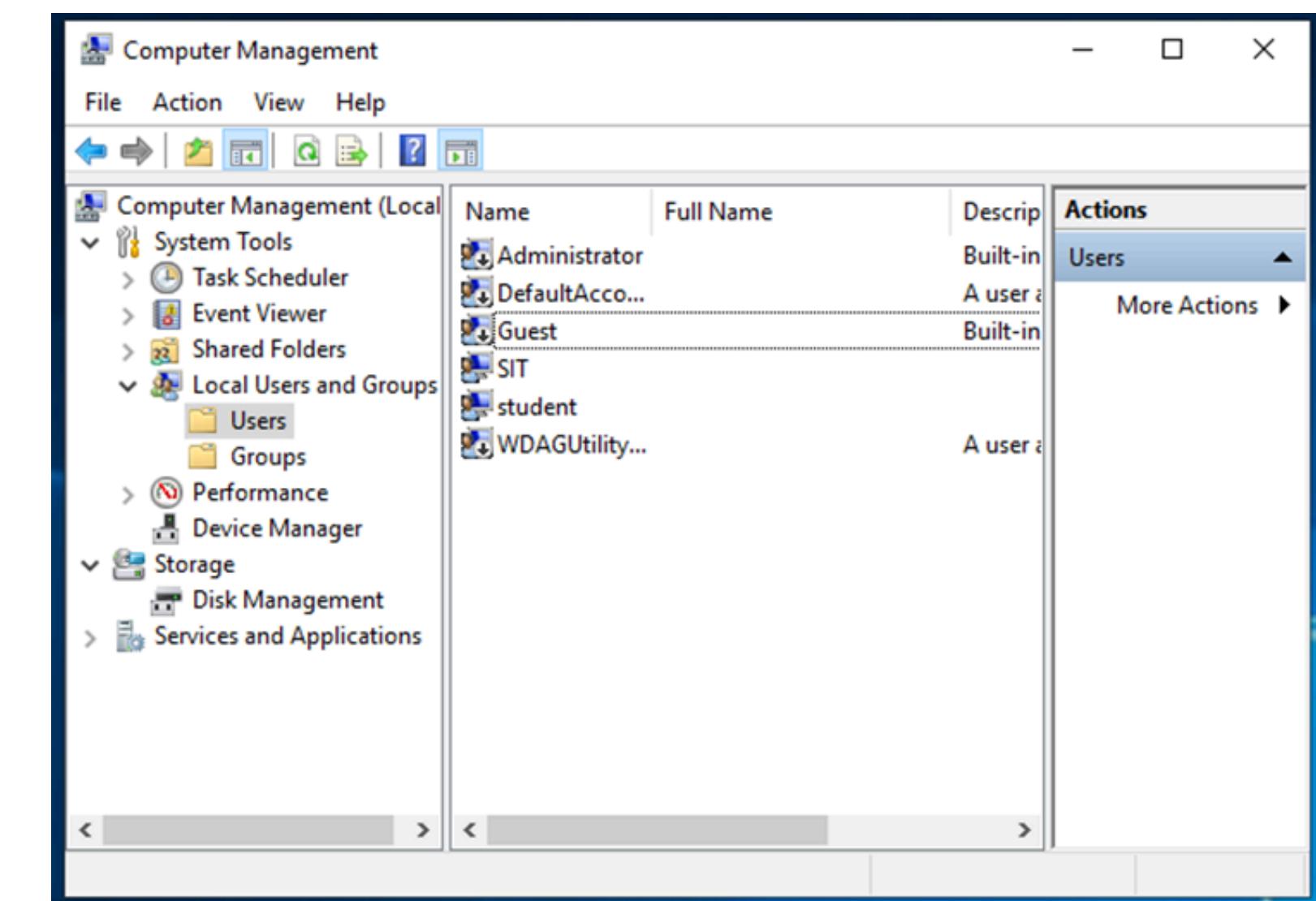
tasks

(30) Create groups for easier account management

Additionally, you can add members to a group from the Users folder

6. In the Computer Management dialog box, navigate to "Users".

Path: System Tools → Local Users and Groups → Users

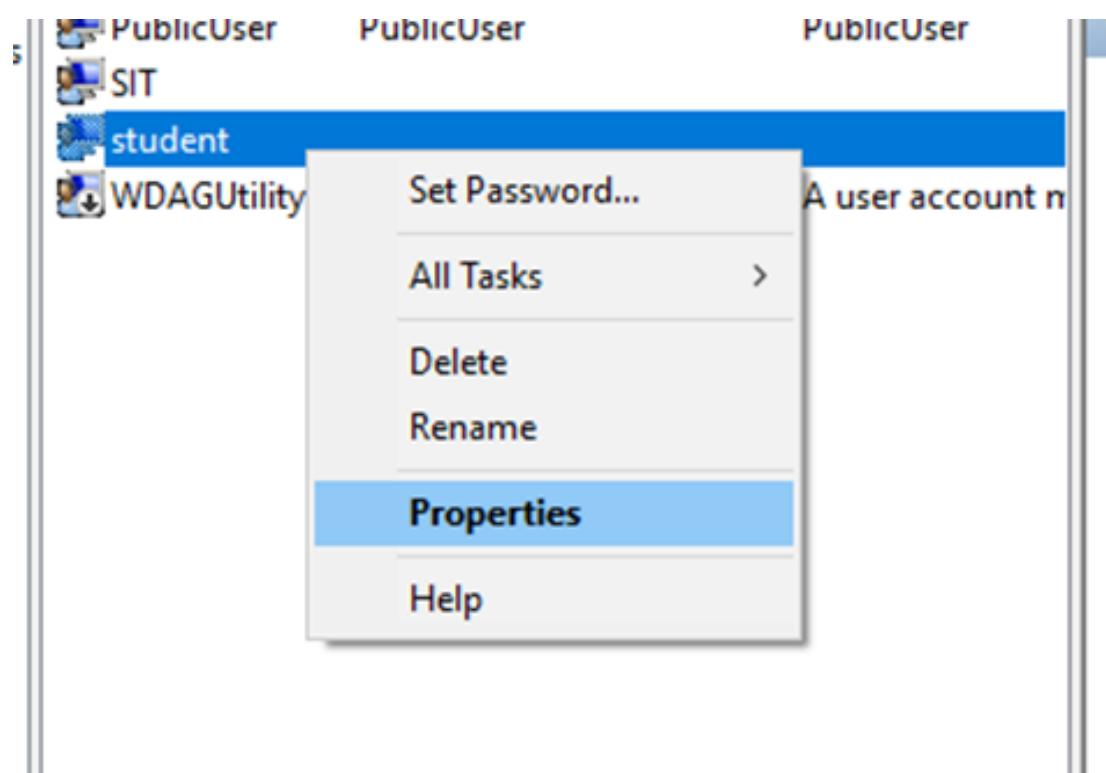


system security and account management

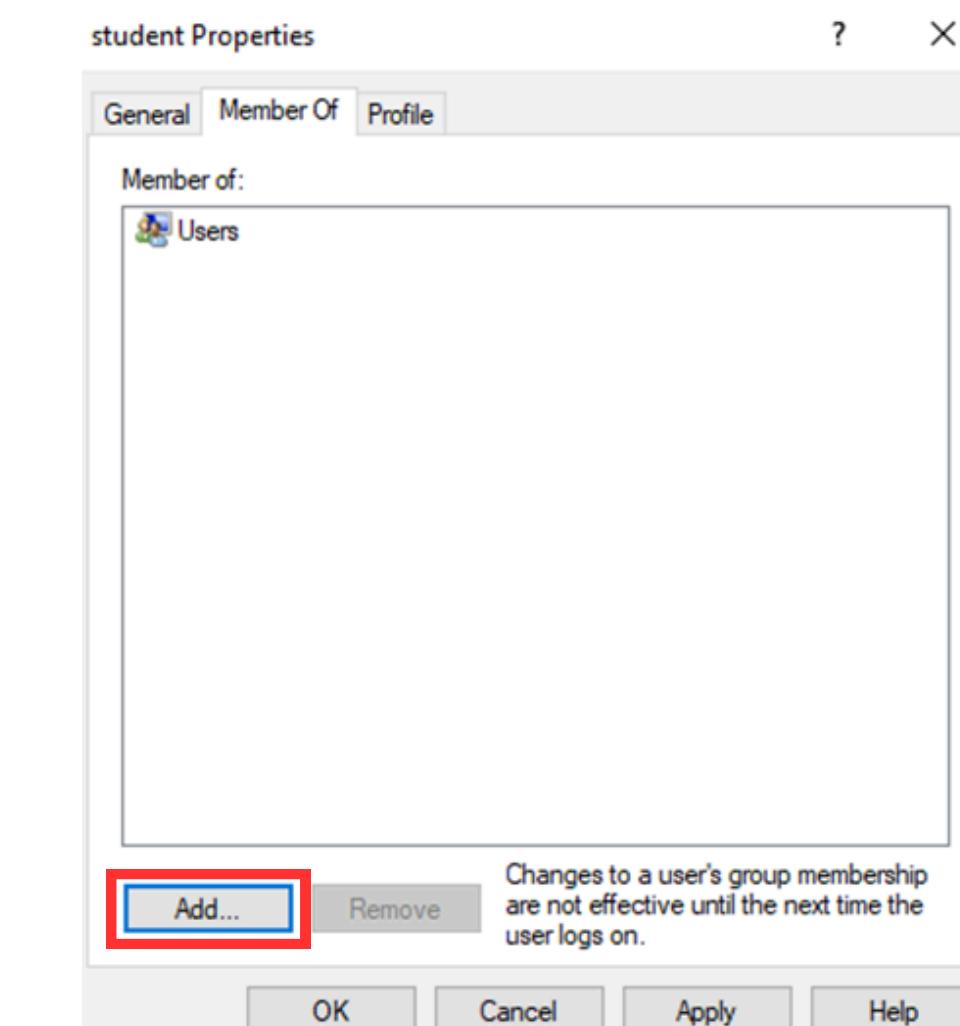
tasks

(30) Create groups for easier account management

7. Right-click on the user you want to add to the group
> click on properties



8. Go to the "Member Of" section and click "Add..."

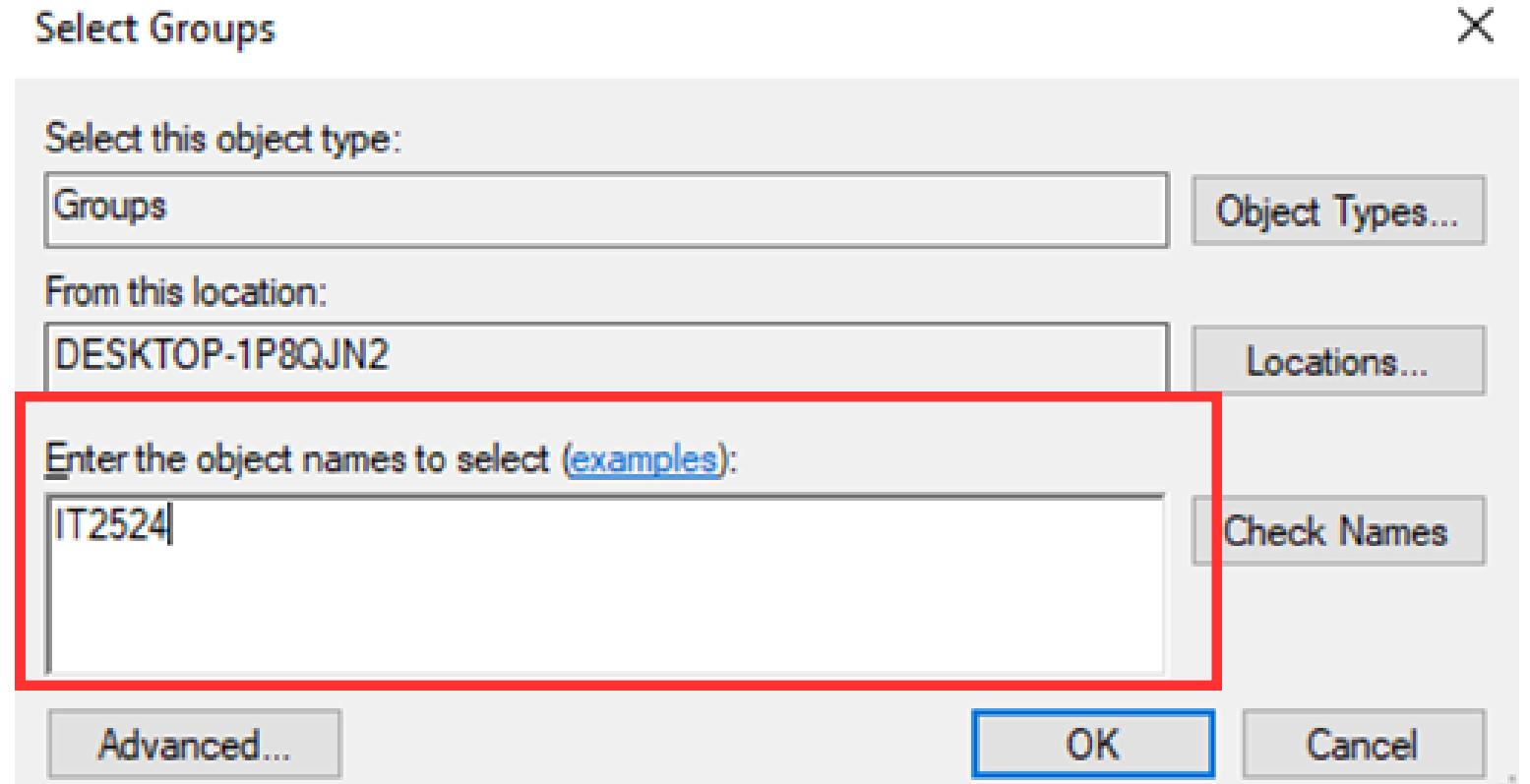


system security and account management

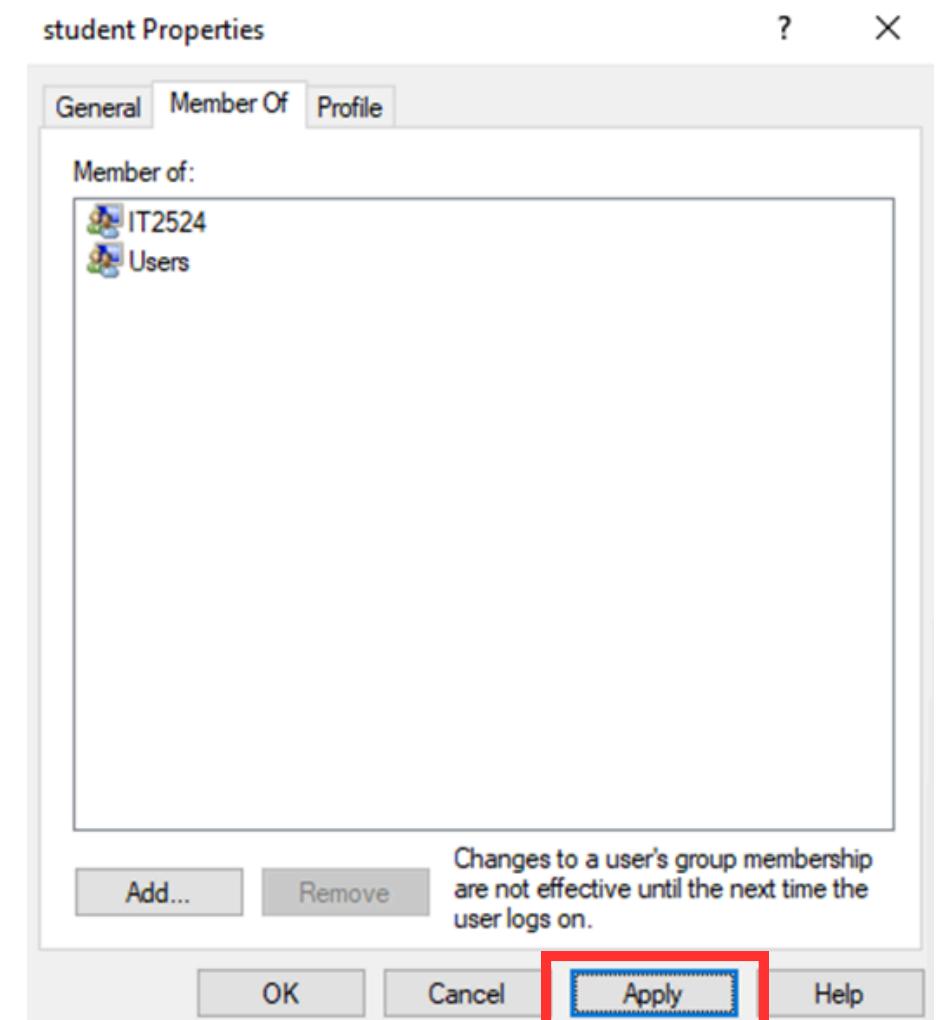
tasks

(30) Create groups for easier account management

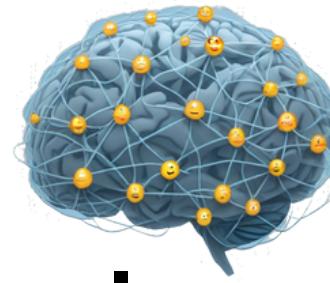
9. Enter the group name and click ok



Click apply



system security and account management



network stuff and access control

by Dhiraj

tasks

done by Dhiraj

- (7) Disable Internet Connection Sharing
- (8) Protect file sharing and shared folders
- (9) Enable Internet Connection Firewall
- (10) Use software restriction policies
- (11) Disable Unnecessary Services
- (15) Disable Remote Access
- (28) Install Host-Based Intrusion Prevention System



base tasks

- (36) Configure Audit Policies for Sensitive Data Access on Win 10



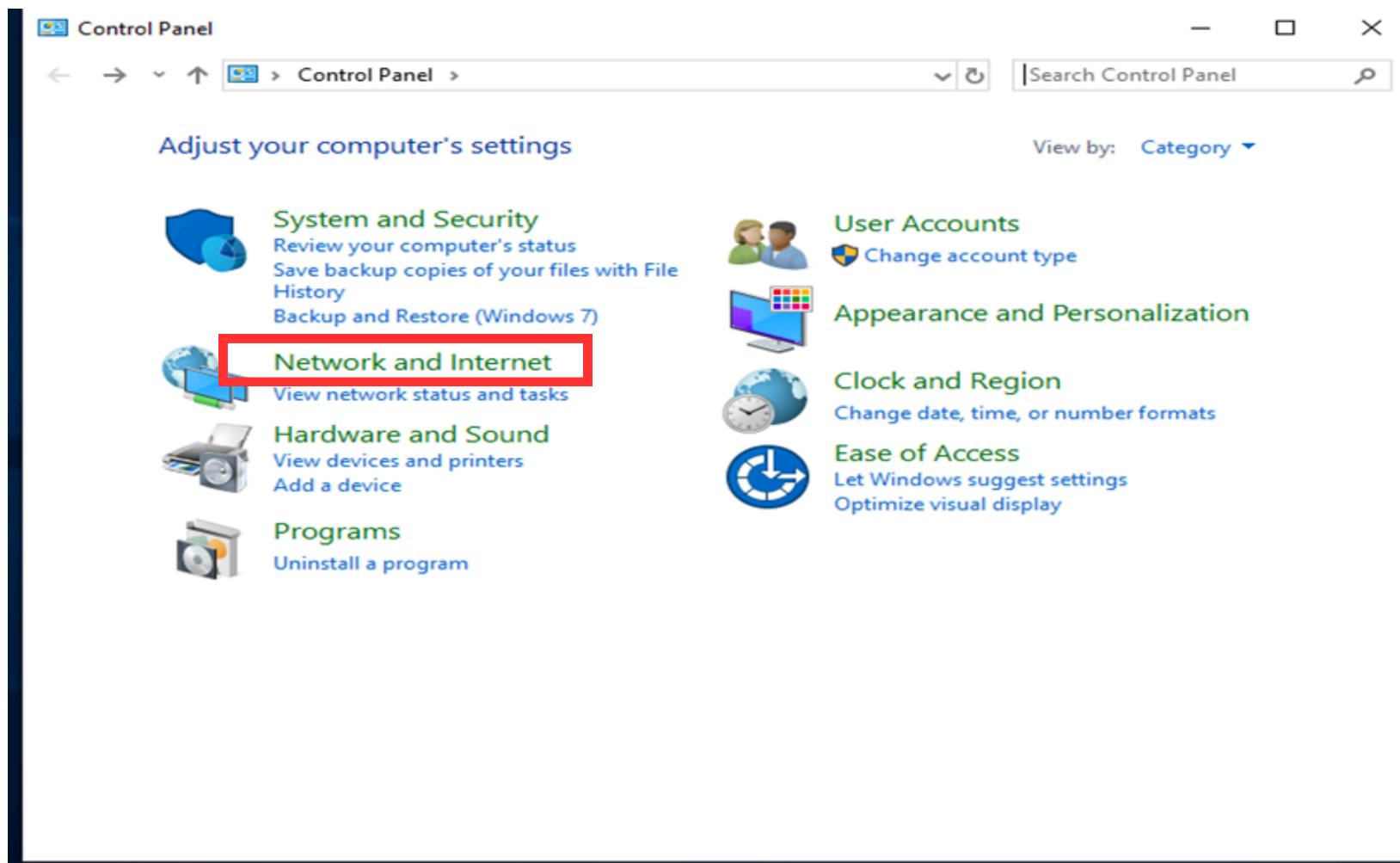
additional tasks

network stuff and access control

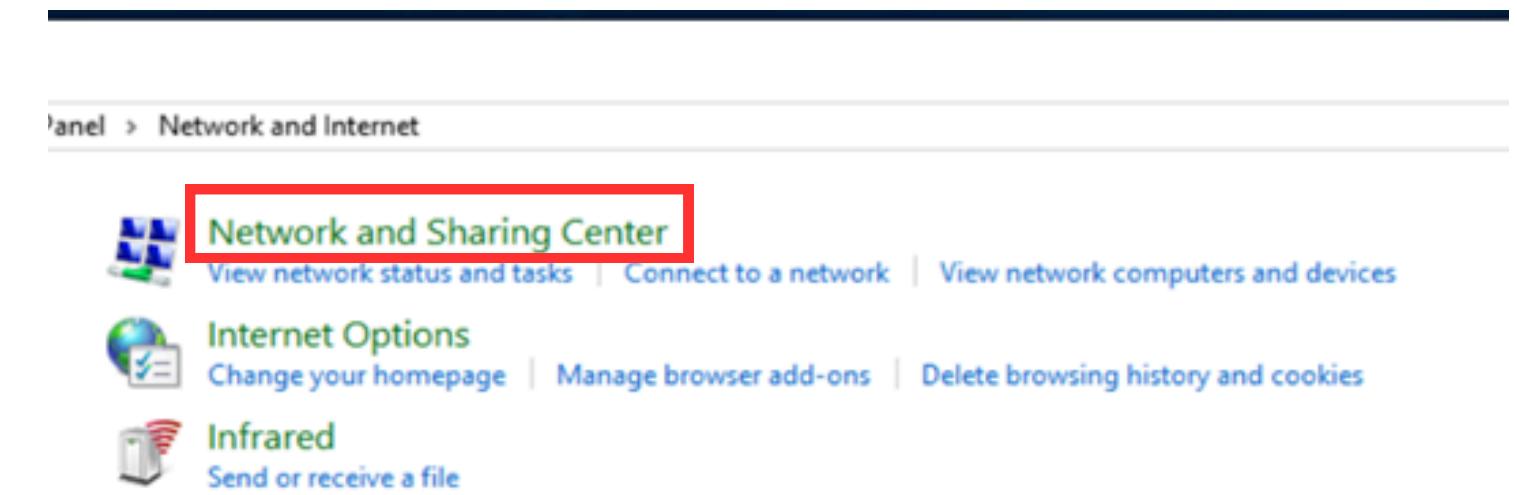
tasks

(8) Protect Files And Shared Folders

1. Open 'Control Panel' and click on 'Network and Internet'



2. Click on 'Network and Sharing Centre'.

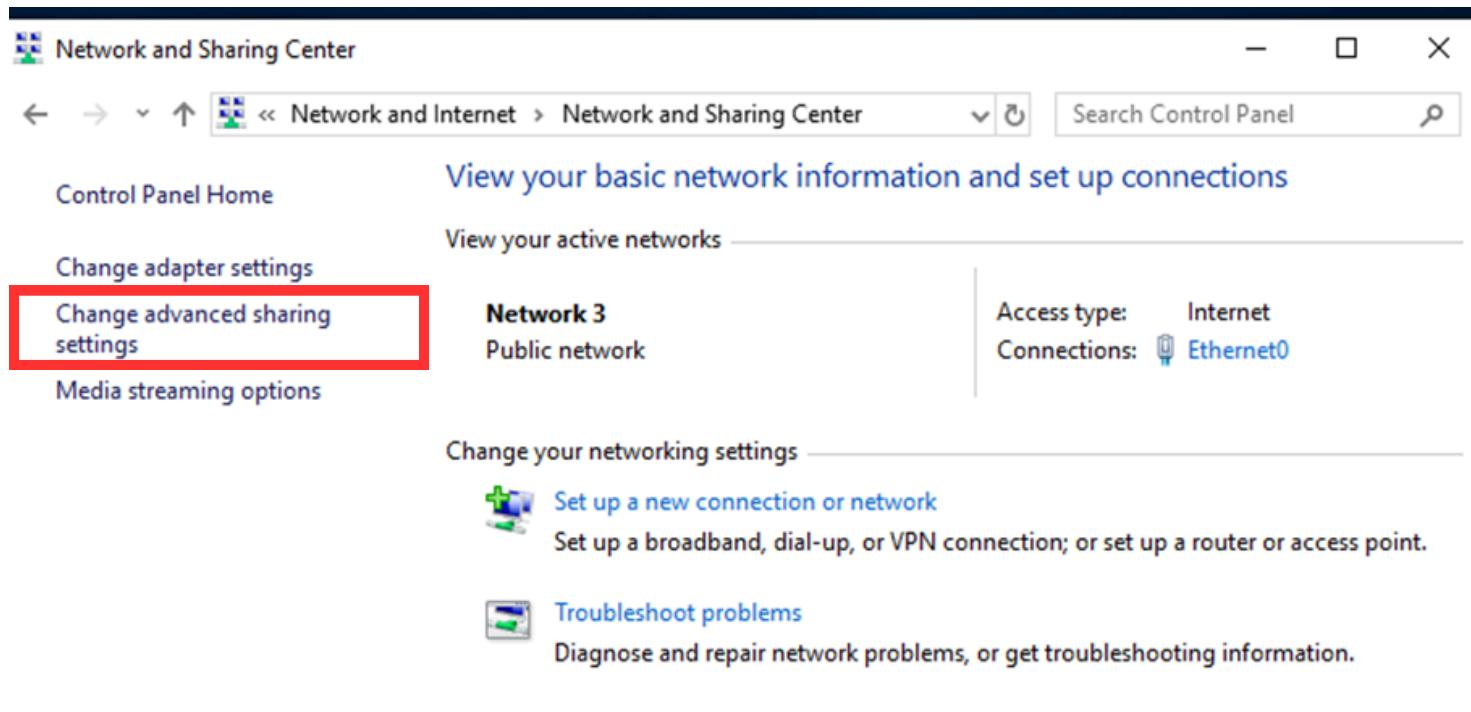


network stuff and access control

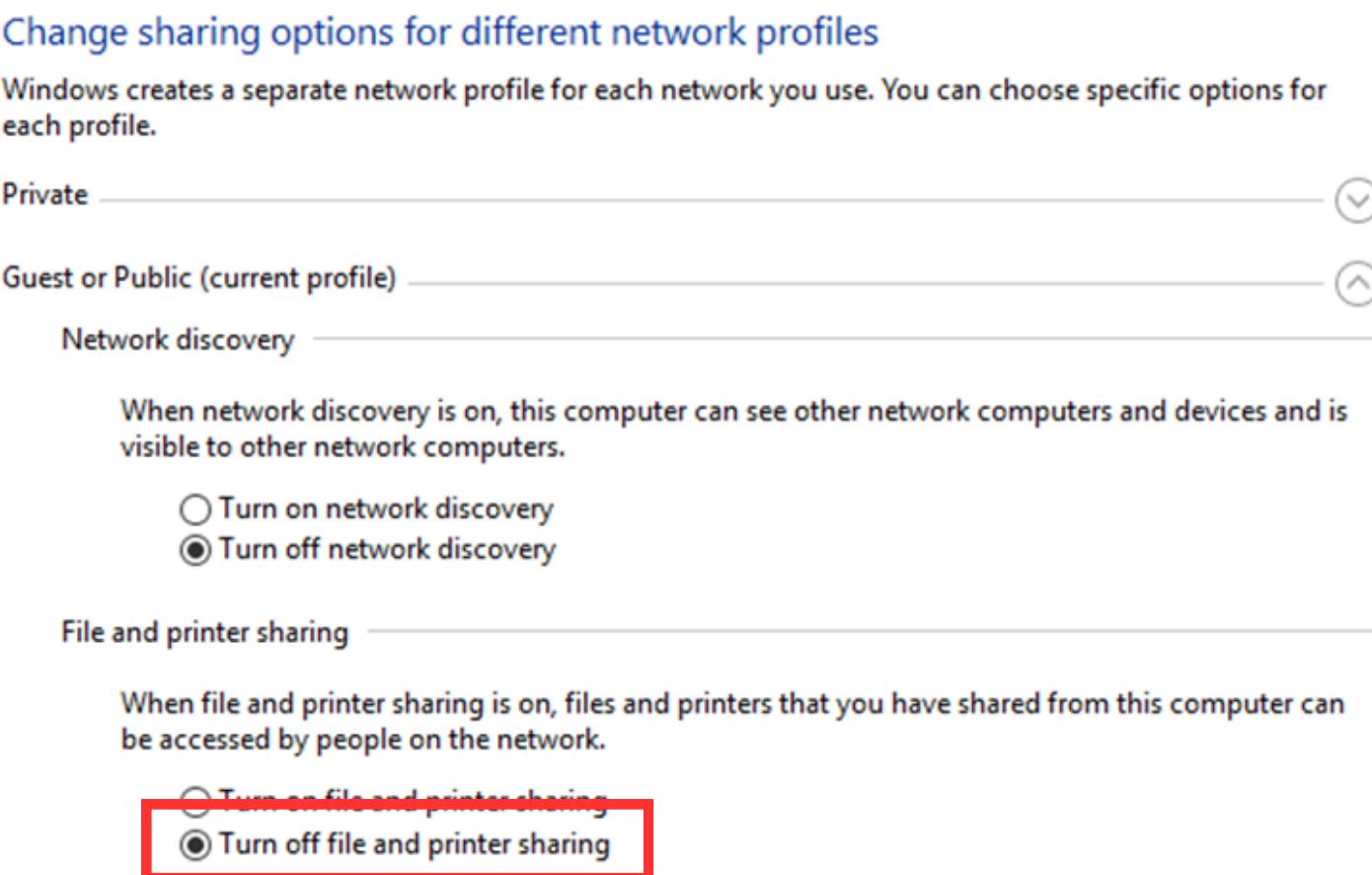
__tasks

(8) Protect Files And Shared Folders

3. Click on 'Change advanced sharing settings'



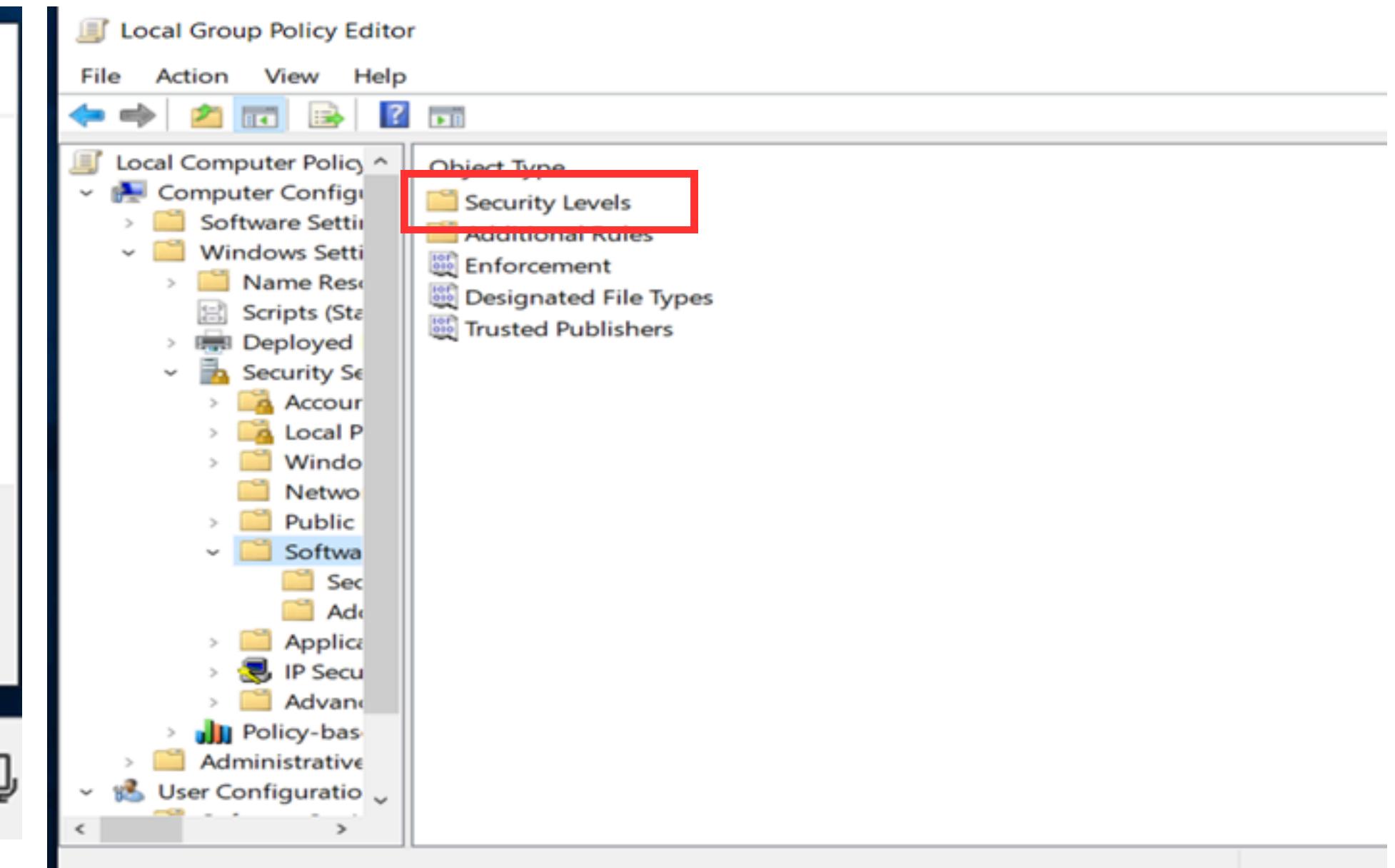
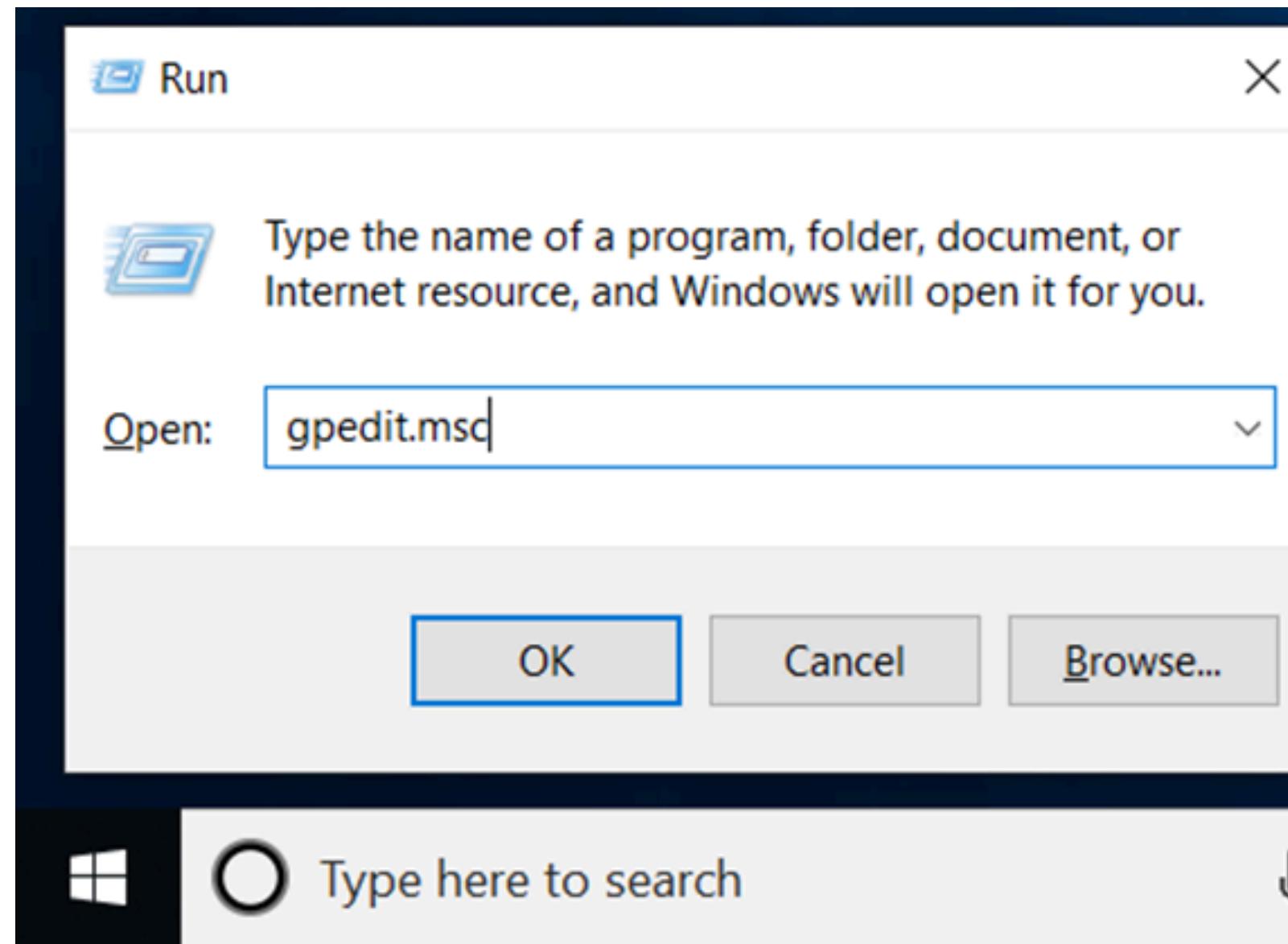
4. Turn off File And Printer sharing for your network profile (private, guest, or public). Click on Save changes.



tasks

(10) Use software restriction policies

1.Press Win + R and type, 'gpedit.msc' to open the Group Policy Editor. 2. Click on Computer Configuration > Windows Settings > Security Settings > Software Restriction Policies > Security Levels



tasks

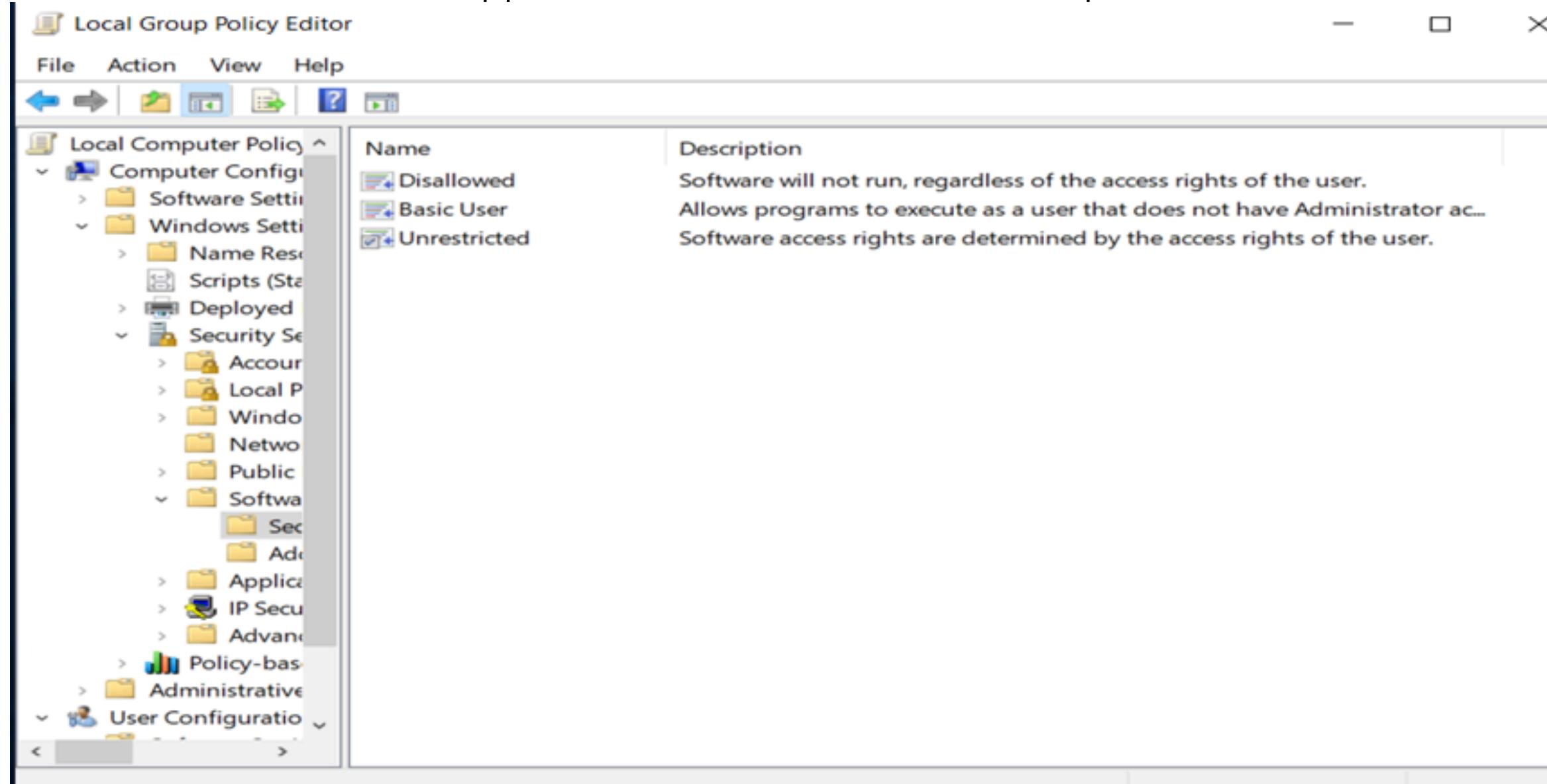
(10) Use software restriction policies

3. Choose one of the following:

Disallowed: Blocks all applications unless explicitly allowed (recommended for a secure setup).

Basic User: Allows applications to run but without administrator privileges.

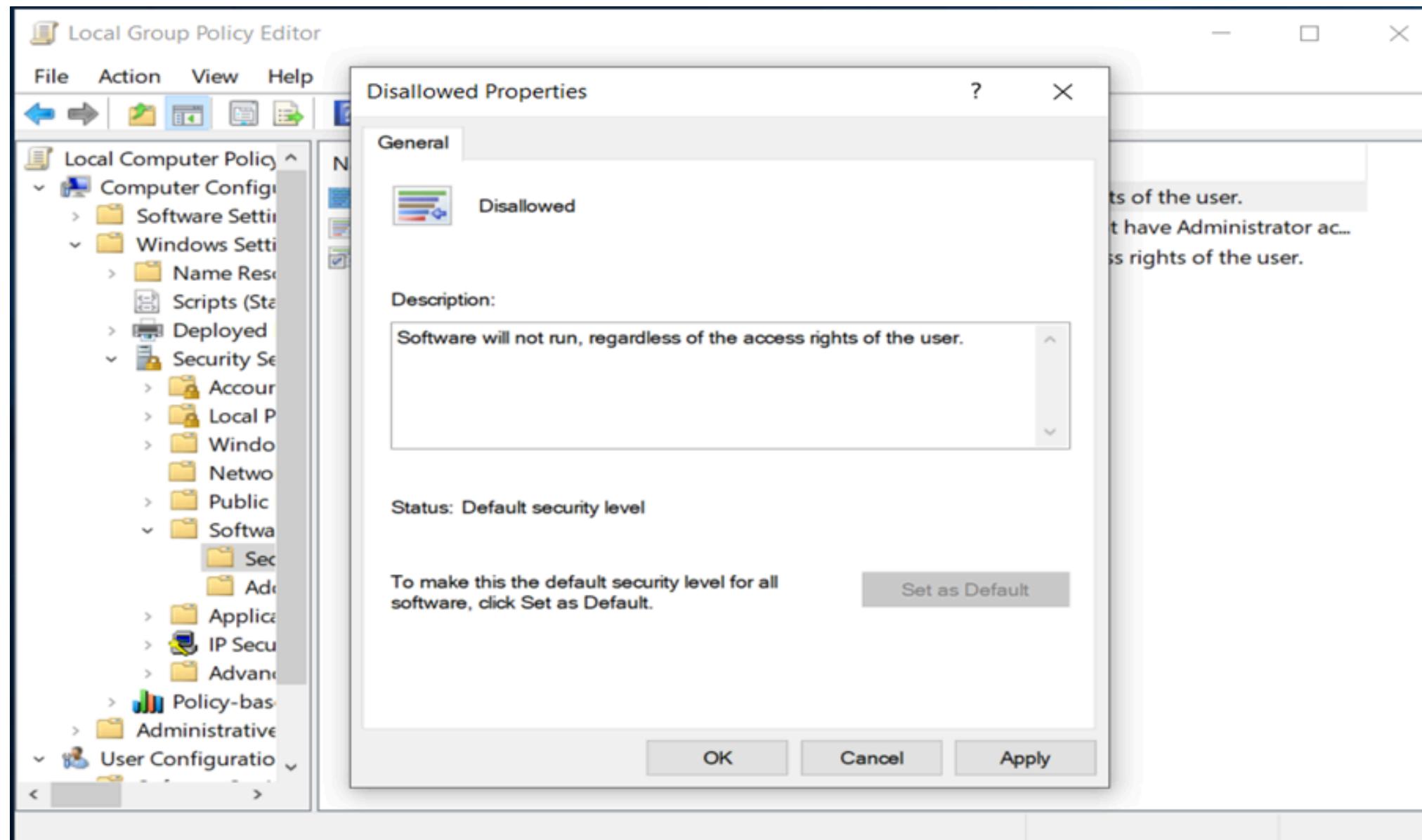
Unrestricted: Allows all applications to run unless there's a specific restriction rule.



tasks

(10) Use software restriction policies

4. Choose your preferred level of security then Apply > OK.

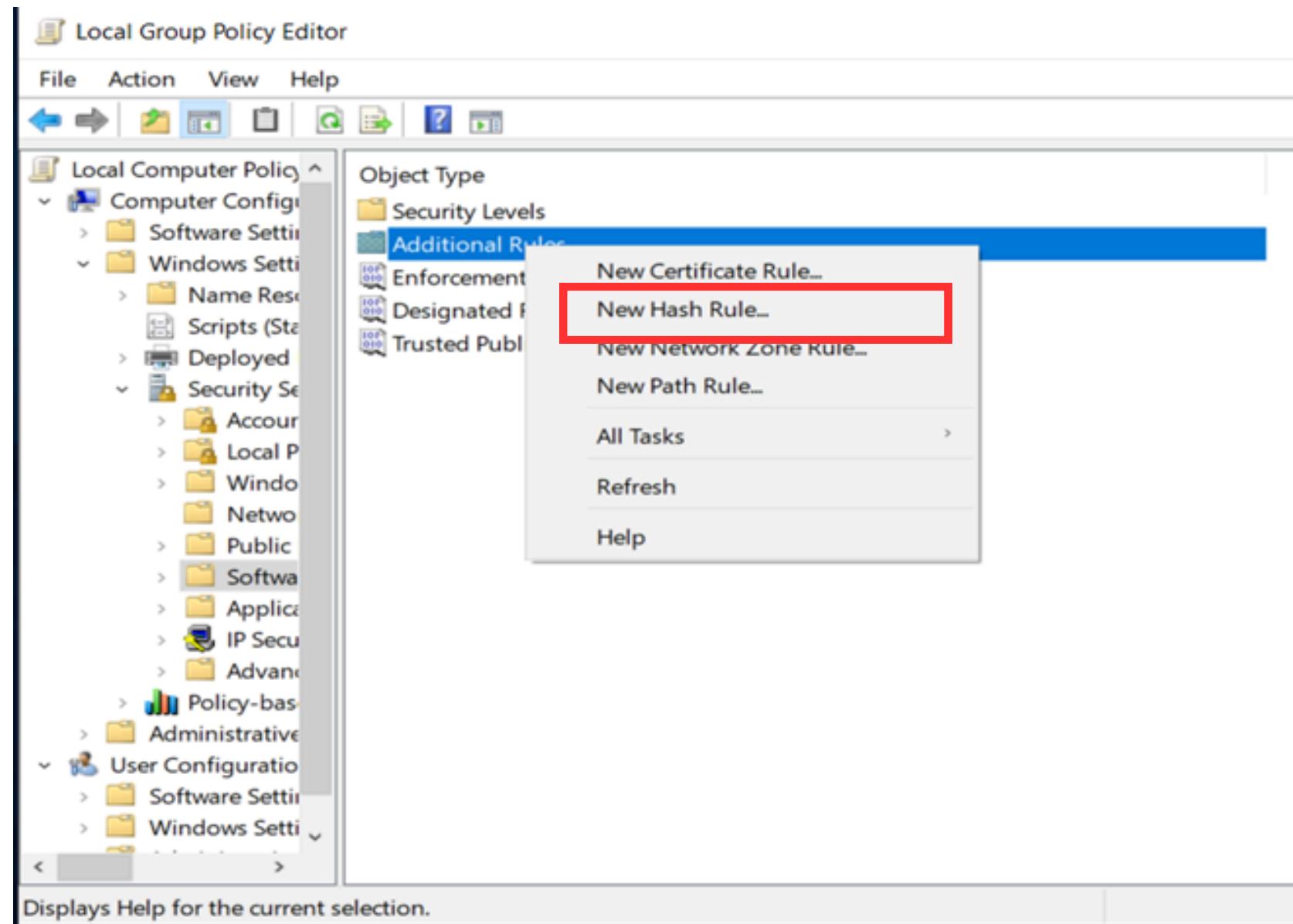


tasks

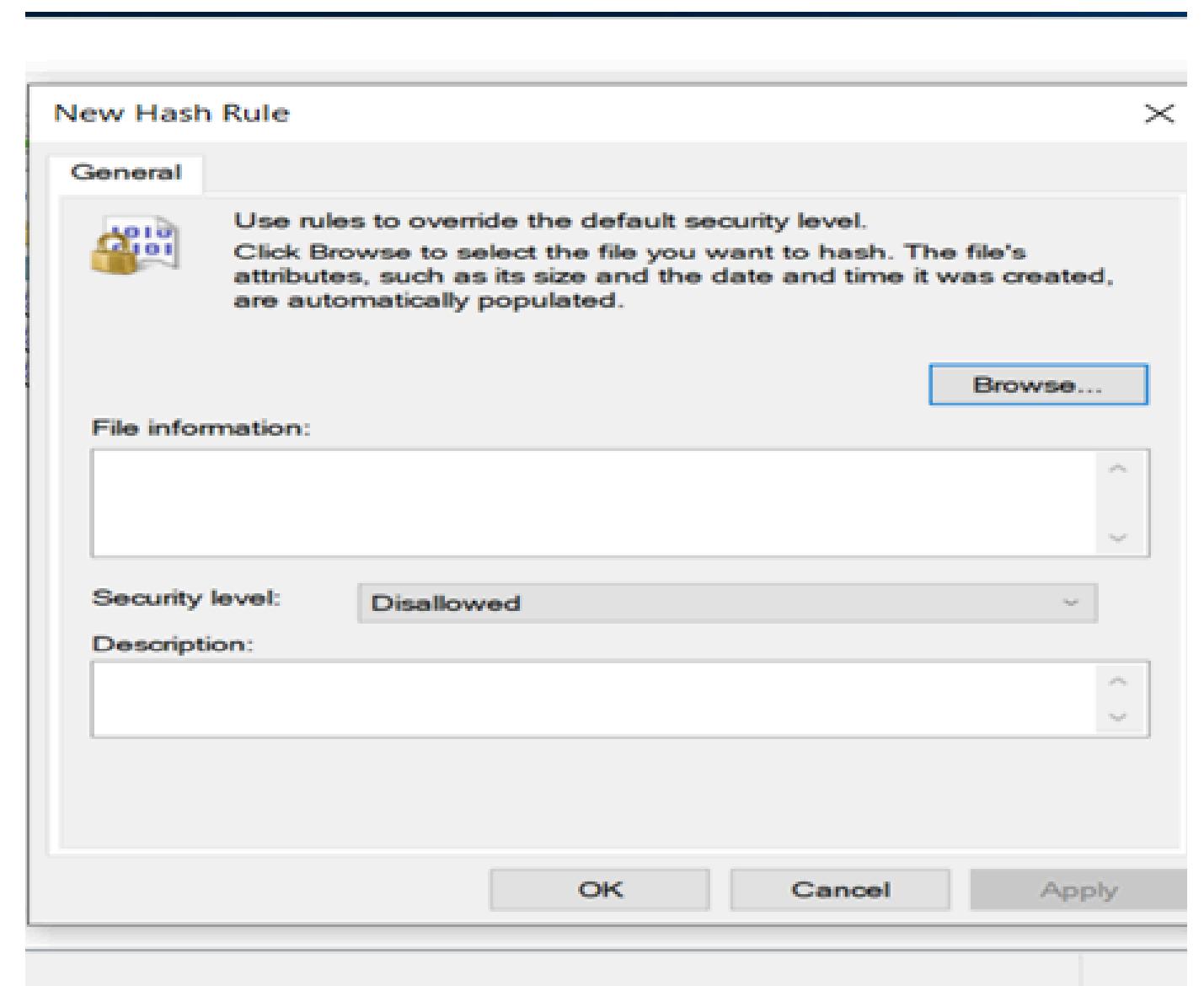
(10) Use software restriction policies

Additional way to use software policy

1. Right Click on additional rules and click on New Hash Rules



2. Browse for the file to for the hash rule to be executed on

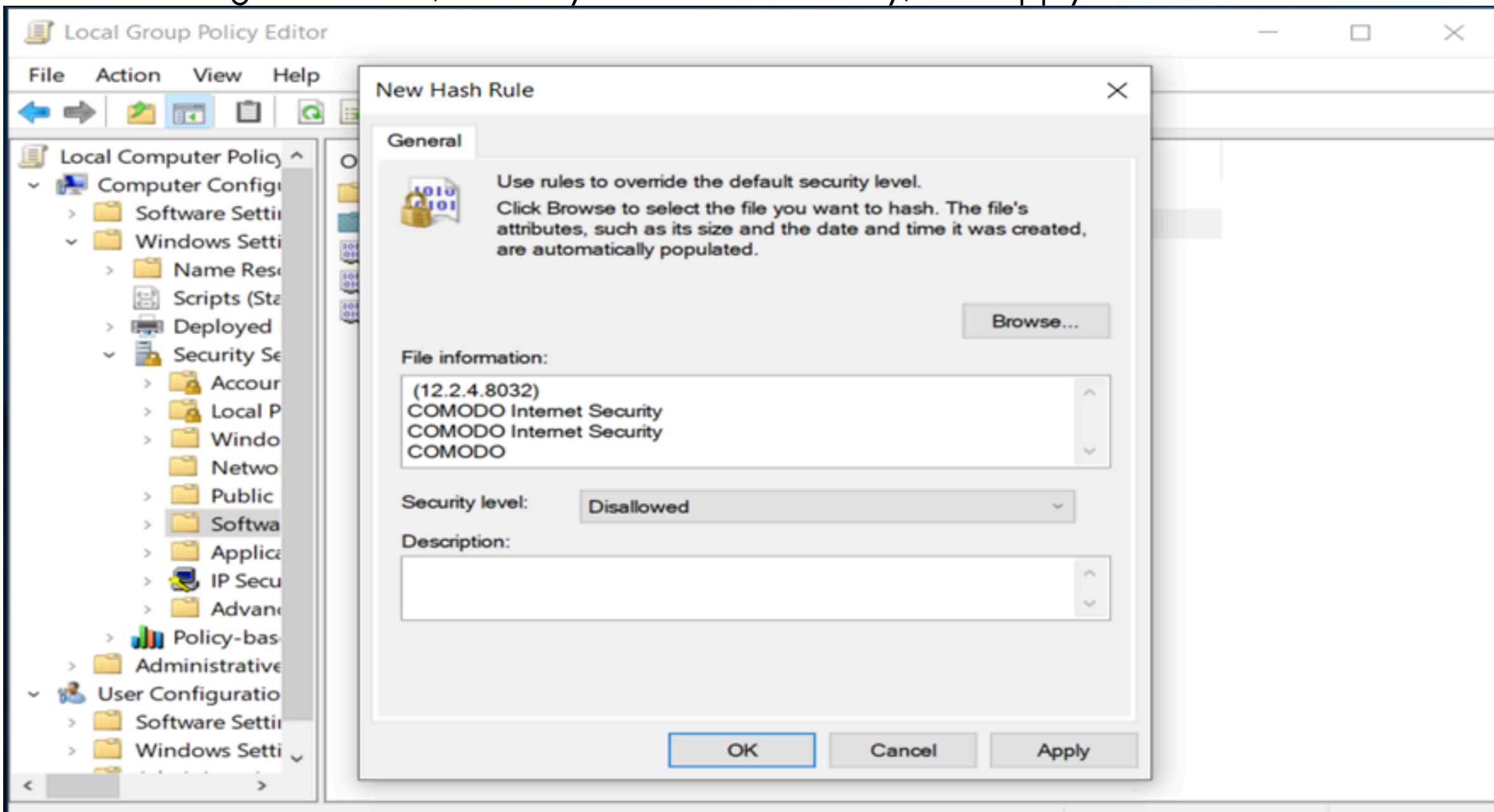


tasks

(10) Use software restriction policies

Additional way to use software policy

3.after searching for the file,choose your level of security,click apply and ok

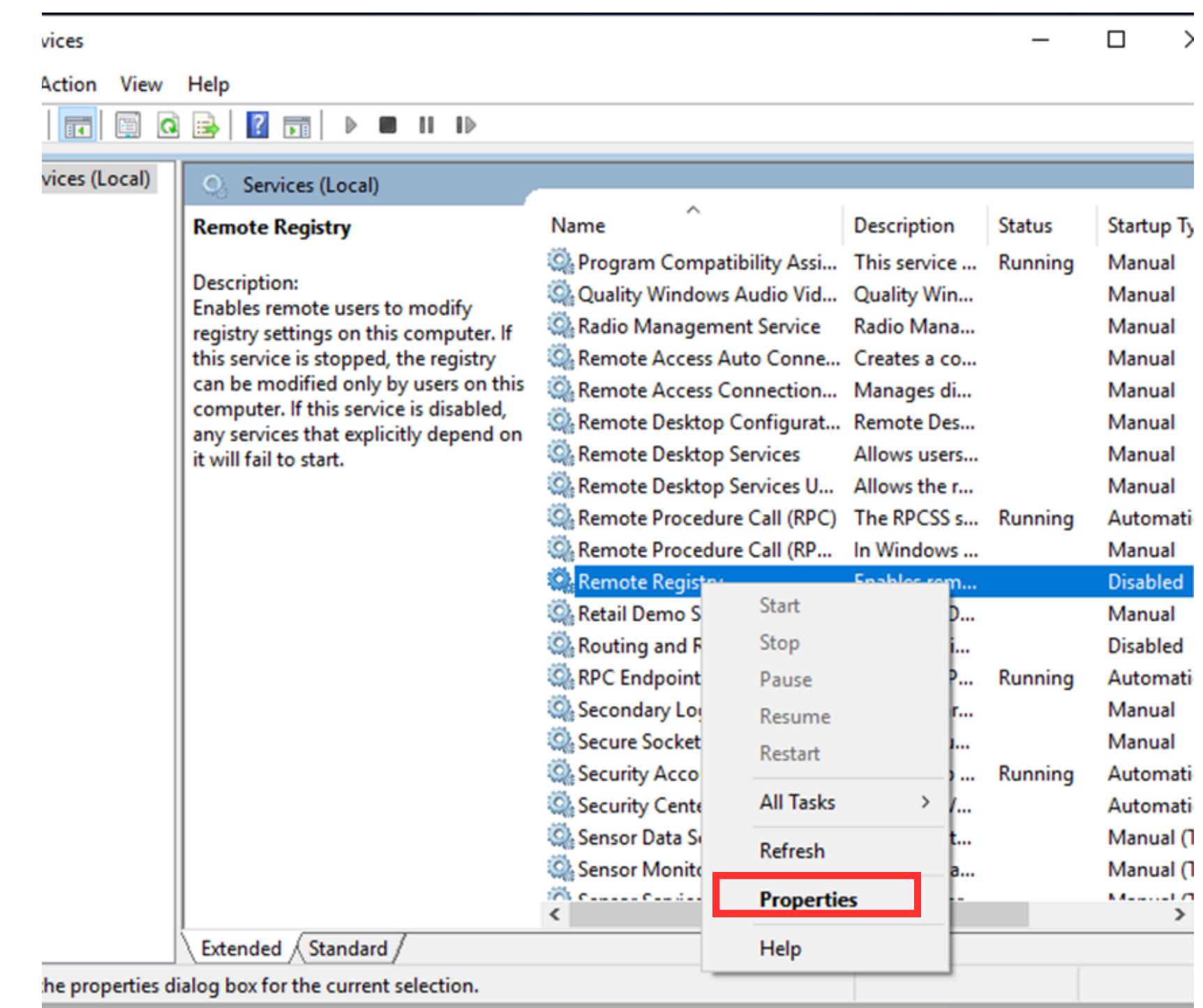
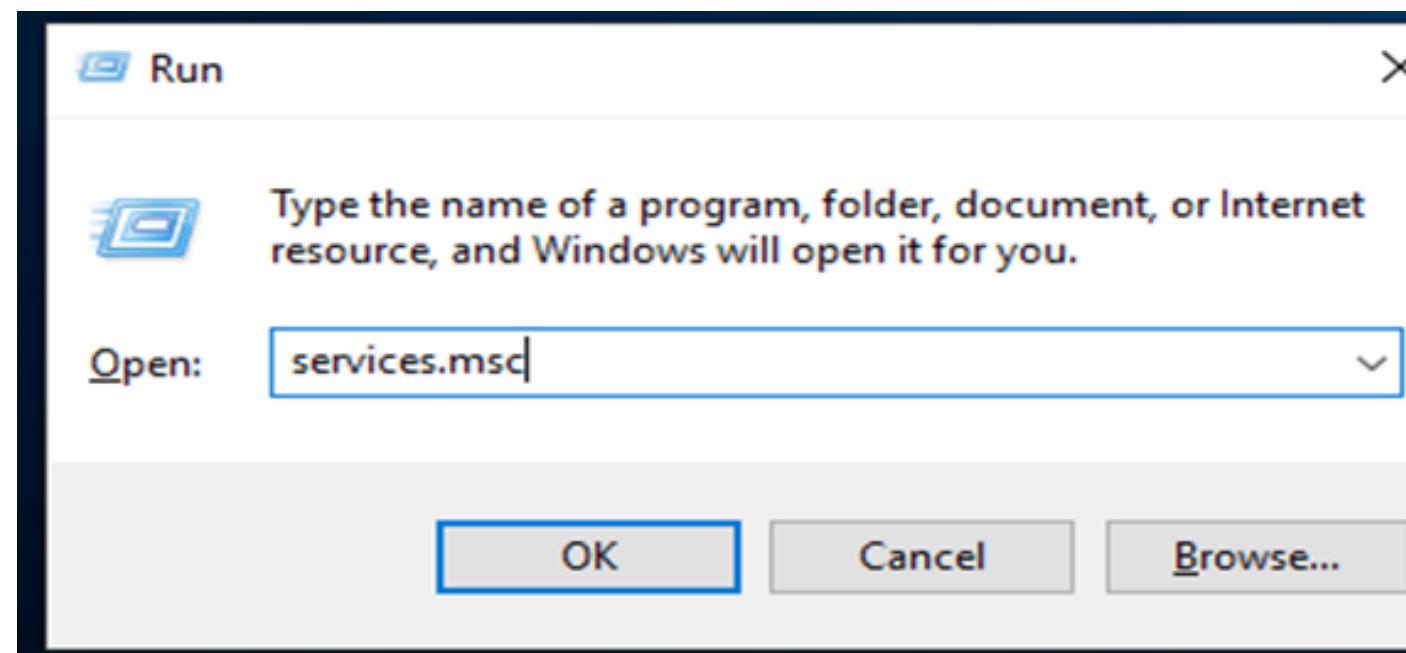


__tasks

2. Review the list and identify services that aren't required (like Windows Error Reporting Service, Remote Registry, Telnet, etc.). Right-click on one and select properties

(11) Disable unnecessary services

1. Press Win + R, and type services.msc > press OK

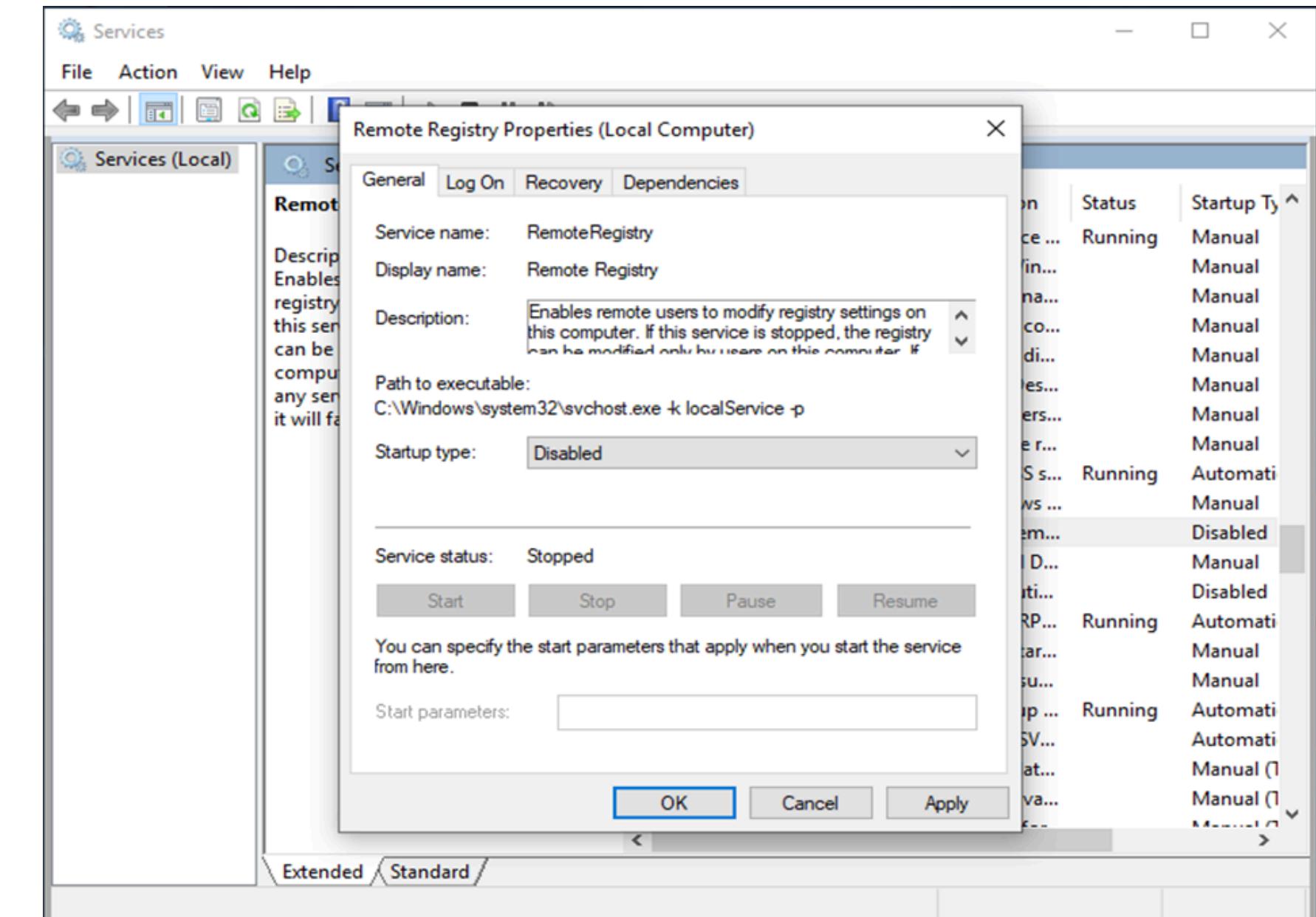
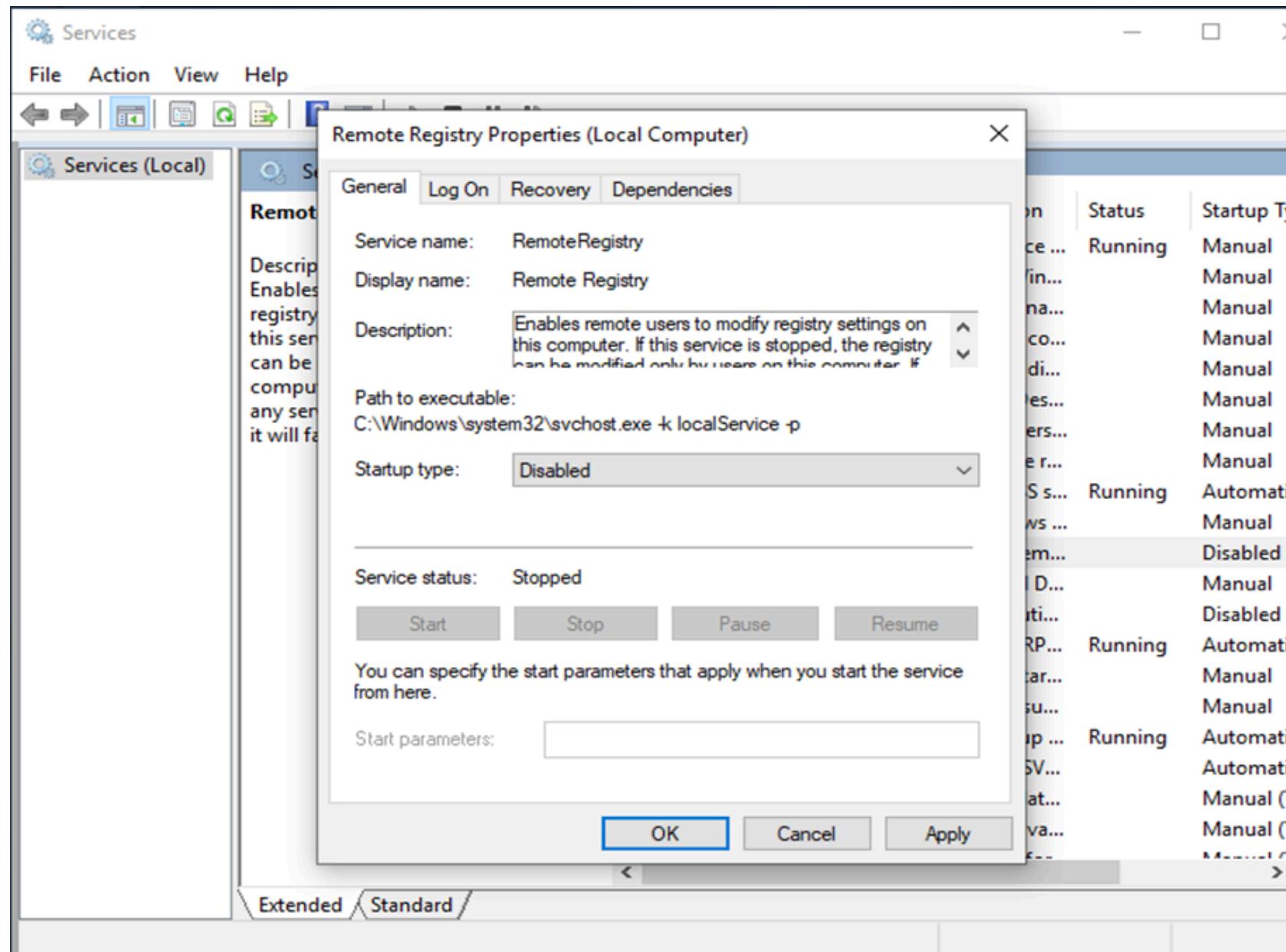


tasks

(11) Disable unnecessary services

4. Change the startup type from 'manual' to disable on your unnecessary service. Click apply and ok

E.gDisable FAX



__tasks

(28) Install Host-Based Intrusion Prevention System

1. Install Comodo Internet Security Download -
12.2.2.8012

The screenshot shows a web browser window with the following details:

- Title Bar:** TechSpot
- URL:** https://www.techspot.com/downloads/4758-comodo... ↗
- Page Content:**
 - Section Title:** Comodo Internet Security Download Free - 12.2.2.8012 - TechSpot
 - Date:** Sep 21, 2023
 - Description:** Comodo Internet Security, Comodo's award-winning free security suite, offers prevention-based, Default Deny Protection (DDP) technology to prevent malware in your PC.
 - Rating:** 4.6/5 (82)
 - Operating System:** Windows
 - Software Version:** 12.2.2.8012
 - Size:** 218 MB
- Search Suggestions:** comodo internet security windows 10, free antivirus comodo internet security, comodo internet security latest version, free comodo cybersecurity, comodo antivirus free download 2020, comodo dragon internet security free
- Bottom Bar:** Type here to search, with various icons for file operations like copy, paste, cut, and save.

2. Scroll down and click on 'Download Now'

The screenshot shows the product page for Comodo Internet Security on TechSpot:

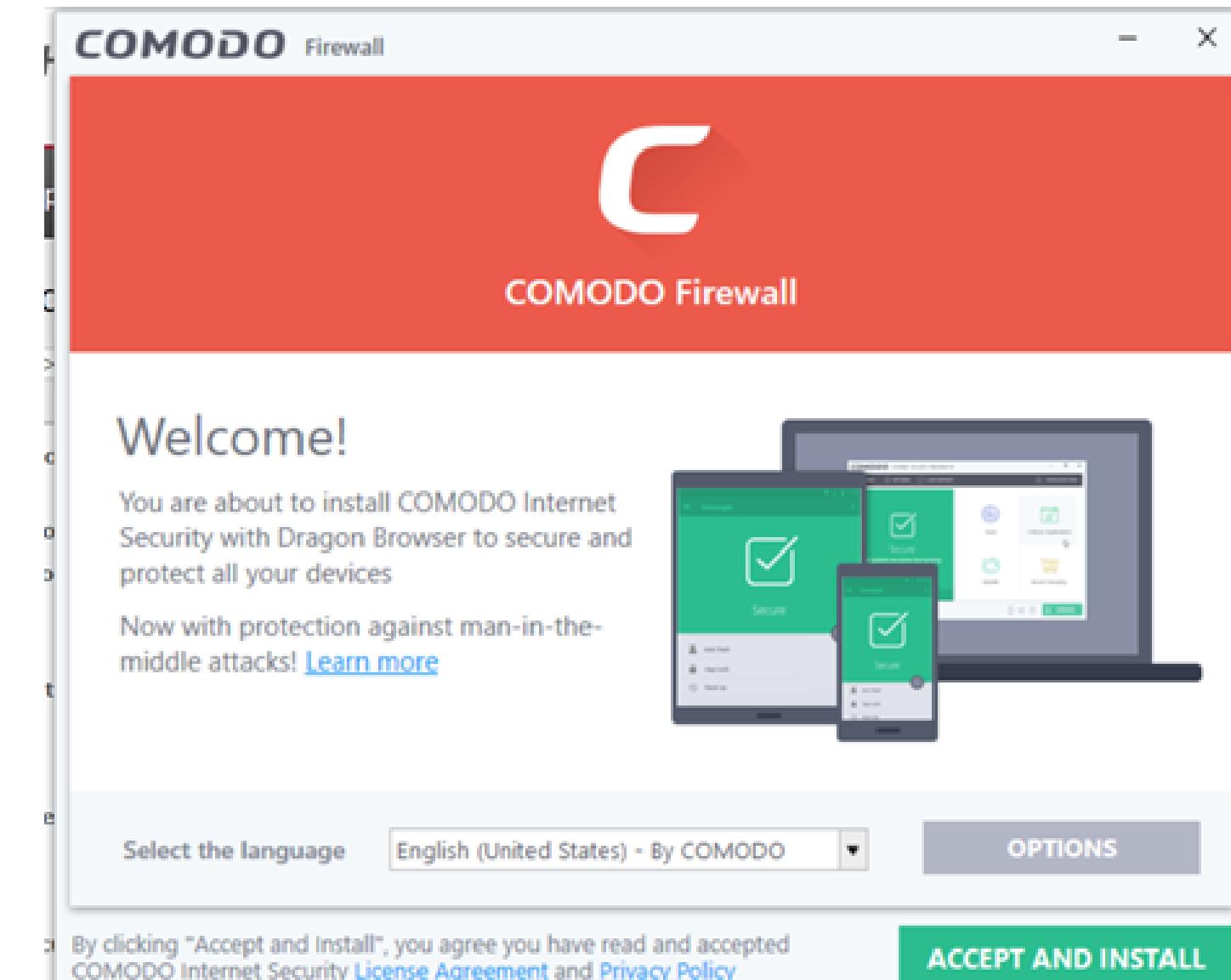
- Header:** Comodo Internet Security plus Antivirus protection for PCs.
- Navigation:** OVERVIEW, CERTIFIED (checkmark), SIMILARS (7)
- Product Description:** Comodo Internet Security, Comodo's award-winning free security suite, offers prevention-based, Default Deny Protection (DDP) technology to prevent malware in your PC. Conventional security suites ignore prevention, focusing only on the eventual detection of viruses. Basically, this means that it will allow all applications to access your PC resources by default as long as the application is not on your security software's blacklist of already known malware.
- Call-to-Action:** Download Now (button highlighted with a red border)
- Side Panel:** Fast servers and clean downloads. Serving tech enthusiasts for over 25 years. Tested on TechSpot Labs.
- Advertisement:** Make professional videos with ease. Download Filmora now. DOWNLOAD >
- Certification:** Certified 100% clean. Tested on TechSpot labs. Safe to download and install.
- TECHSPOT:** TECHSPOT logo with a blue hexagon icon.

tasks

3. When this pop up shows, click yes

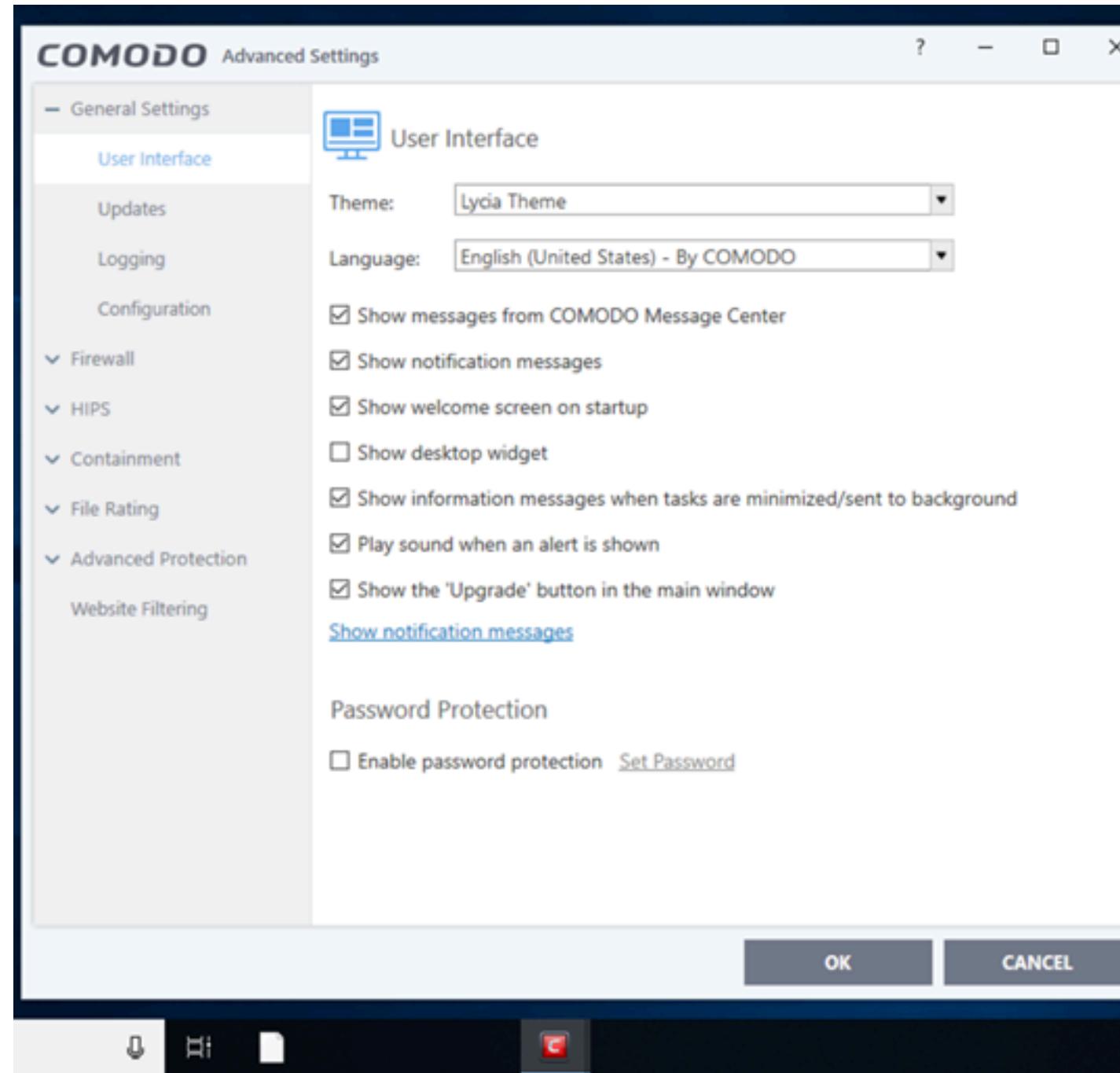


4. Choose your preferred language and click accept and install, after downloading click restart

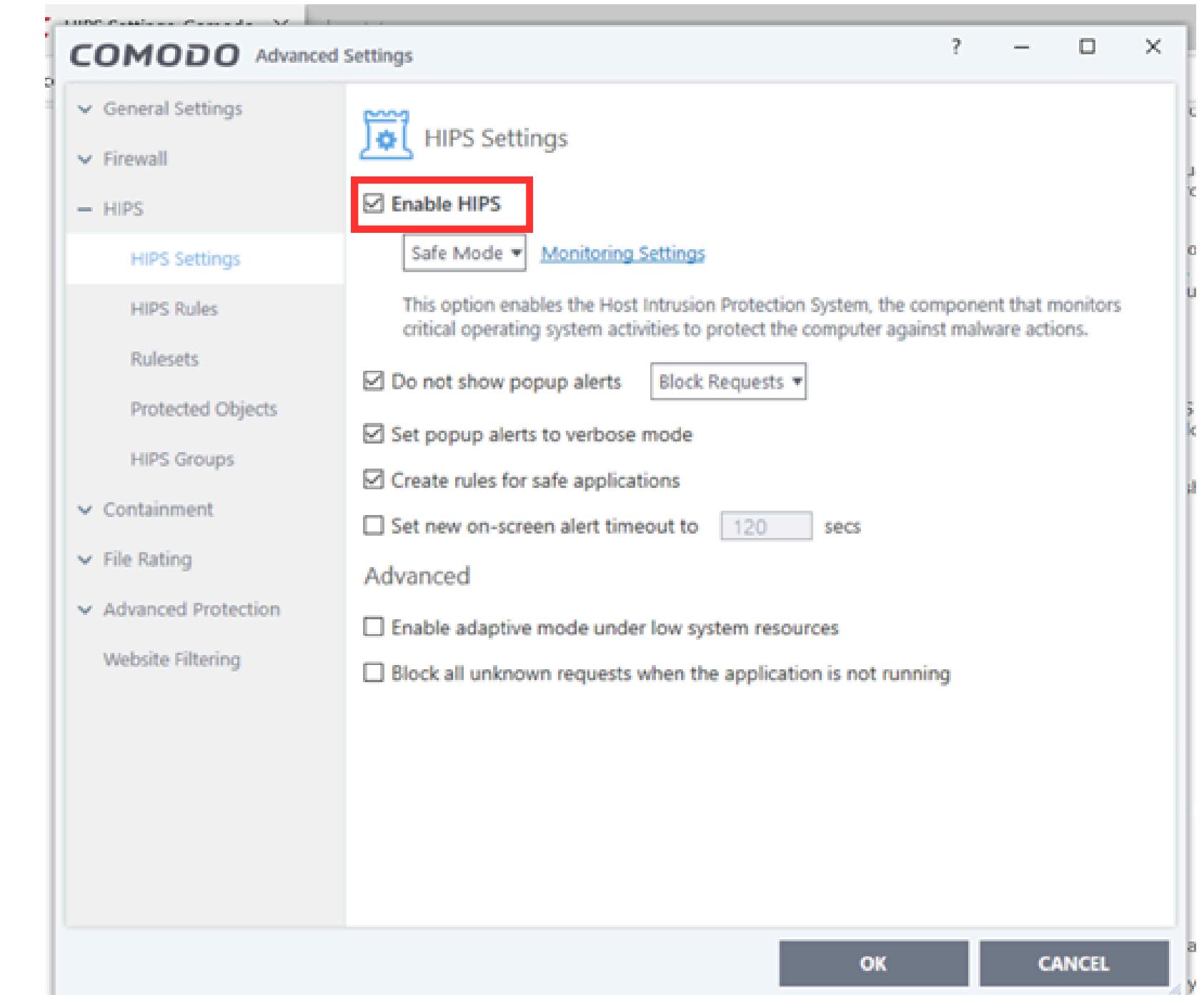


tasks

5.After Restarting,Open up the Comodo Firewall

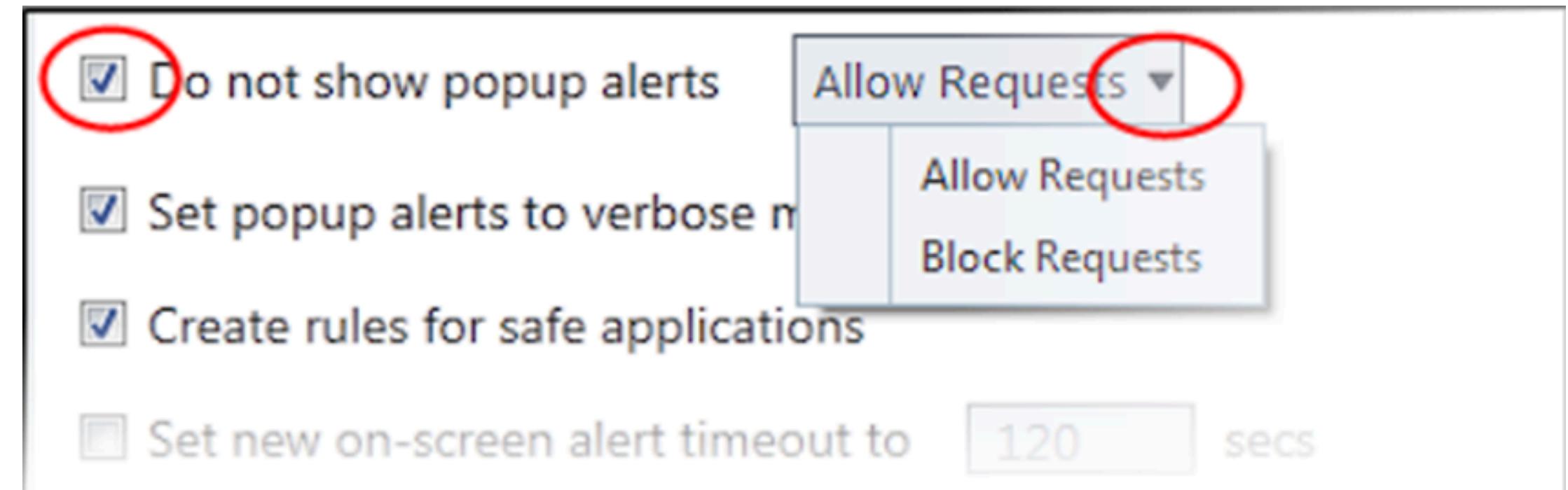
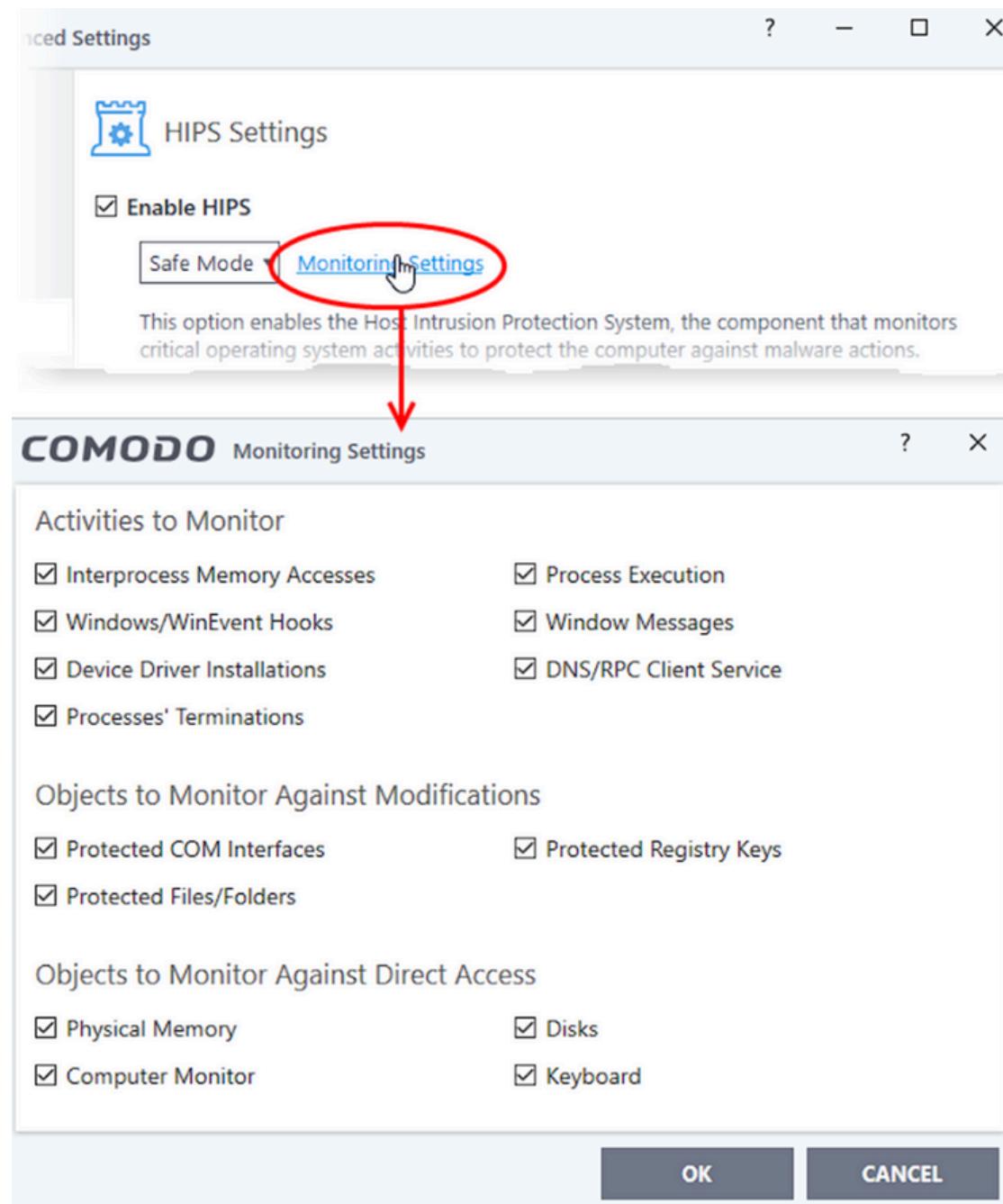


6.Scroll to HIPS settings and click on 'Enable HIPS' and click on 'Safe Mod'



tasks

7.Click on Monitoring settings to choose the devices you want it to be monitored

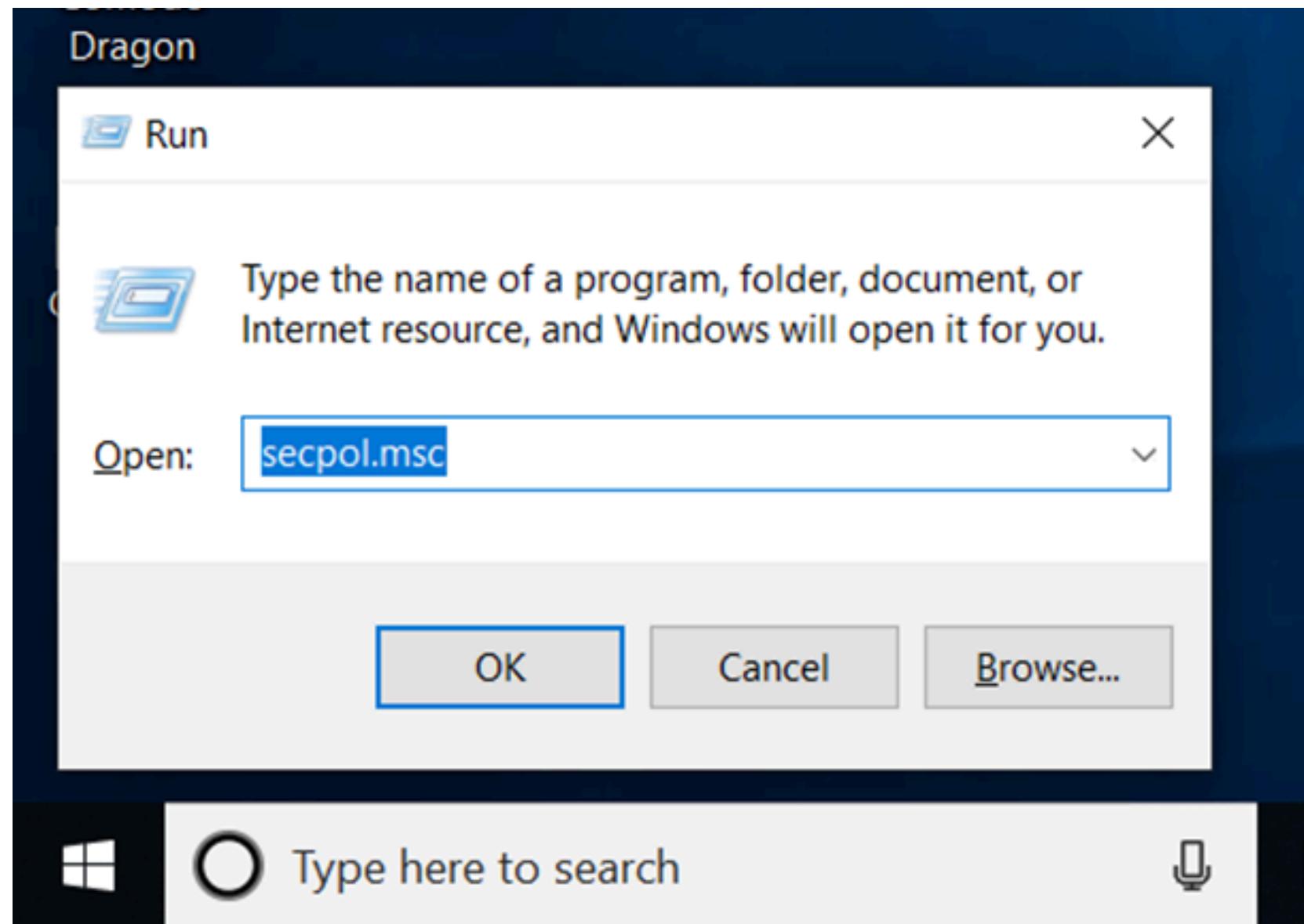


8.Click on the selected boxes,e.g. Block request from pop-up alerts

tasks

(36) Configure Audit Policies for Sensitive Data Access on Windows 10

1.Press win+r, type 'secpol.msc', this will open Local Security Policy

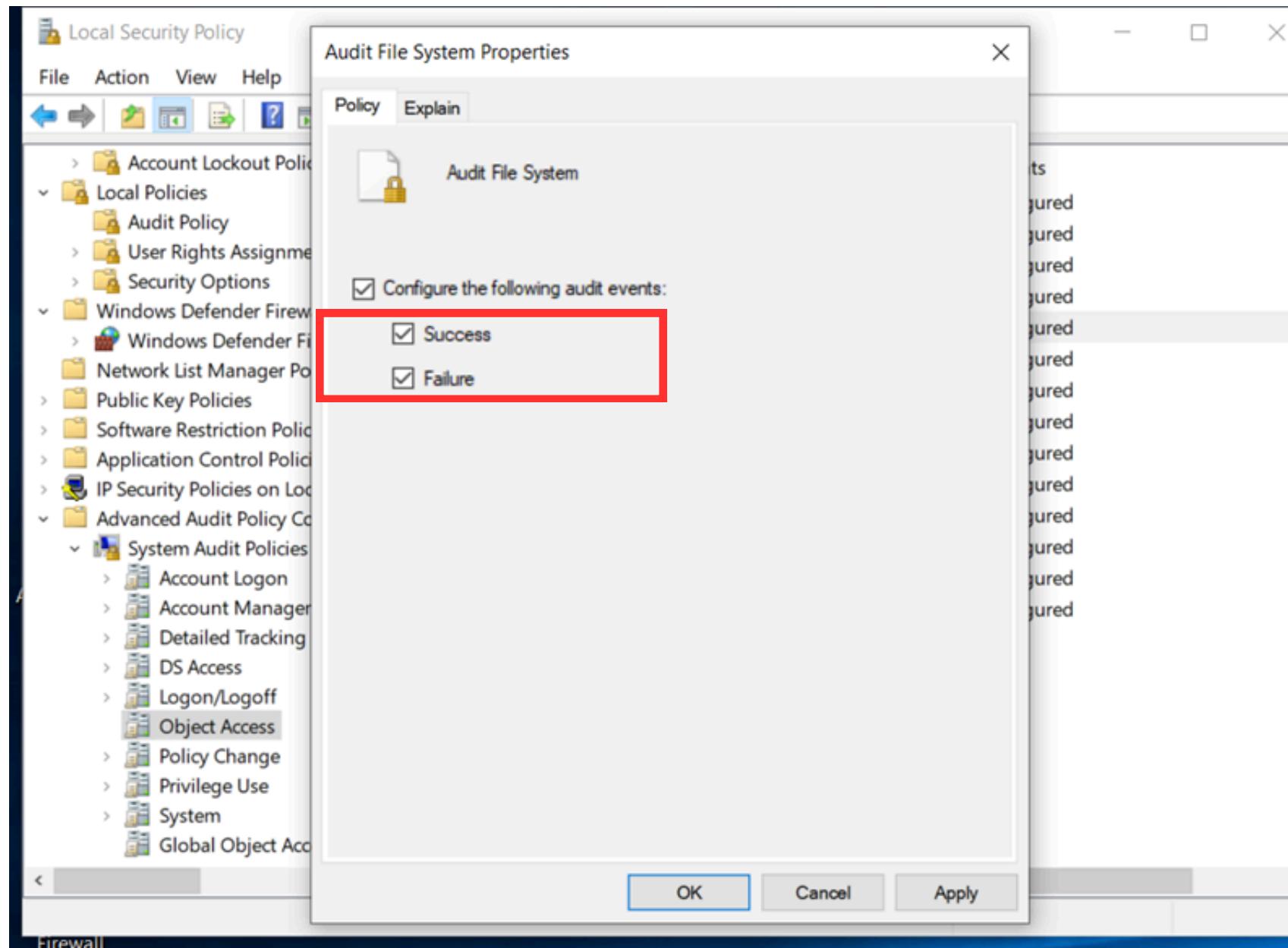


2.Go to Advanced Audit Policy Config > System Audit Policies > Object Access and click on Audit File System

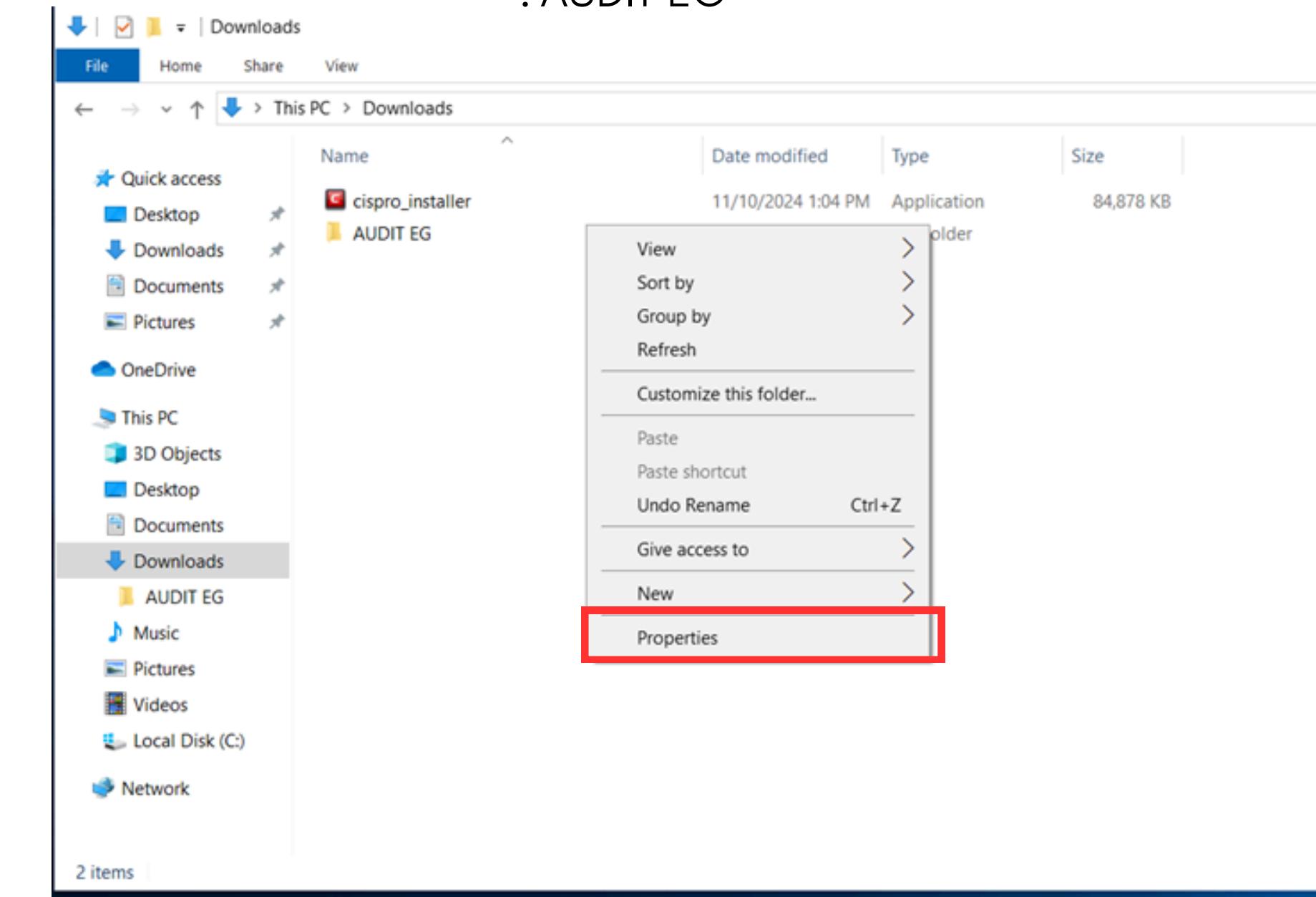
A screenshot of the 'Local Security Policy' snap-in window. The title bar says 'Local Security Policy'. The left pane shows a tree view of security policies: Account Lockout Policy, Local Policies (with Audit Policy selected), User Rights Assignment, Security Options, Windows Defender Firewall with Advanced Security (with Windows Defender Firewall with Advanced Security selected), Network List Manager Policies, Public Key Policies, Software Restriction Policies, Application Control Policies, IP Security Policies on Local Computer, and Advanced Audit Policy Configuration (with System Audit Policies - Local Group selected). The right pane is divided into three sections: 'Subcategory' (listing various audit events like Audit Application Generated, Audit Detailed File Share, Audit File Share, and Audit File System, with Audit File System highlighted by a red box), 'Audit Events' (listing the status for each event: Not Configured for most, except Audit File Share which is Not Configured), and 'Audit Options' (which is mostly empty).

tasks

3.Click on the Success and Failure box,click apply and ok

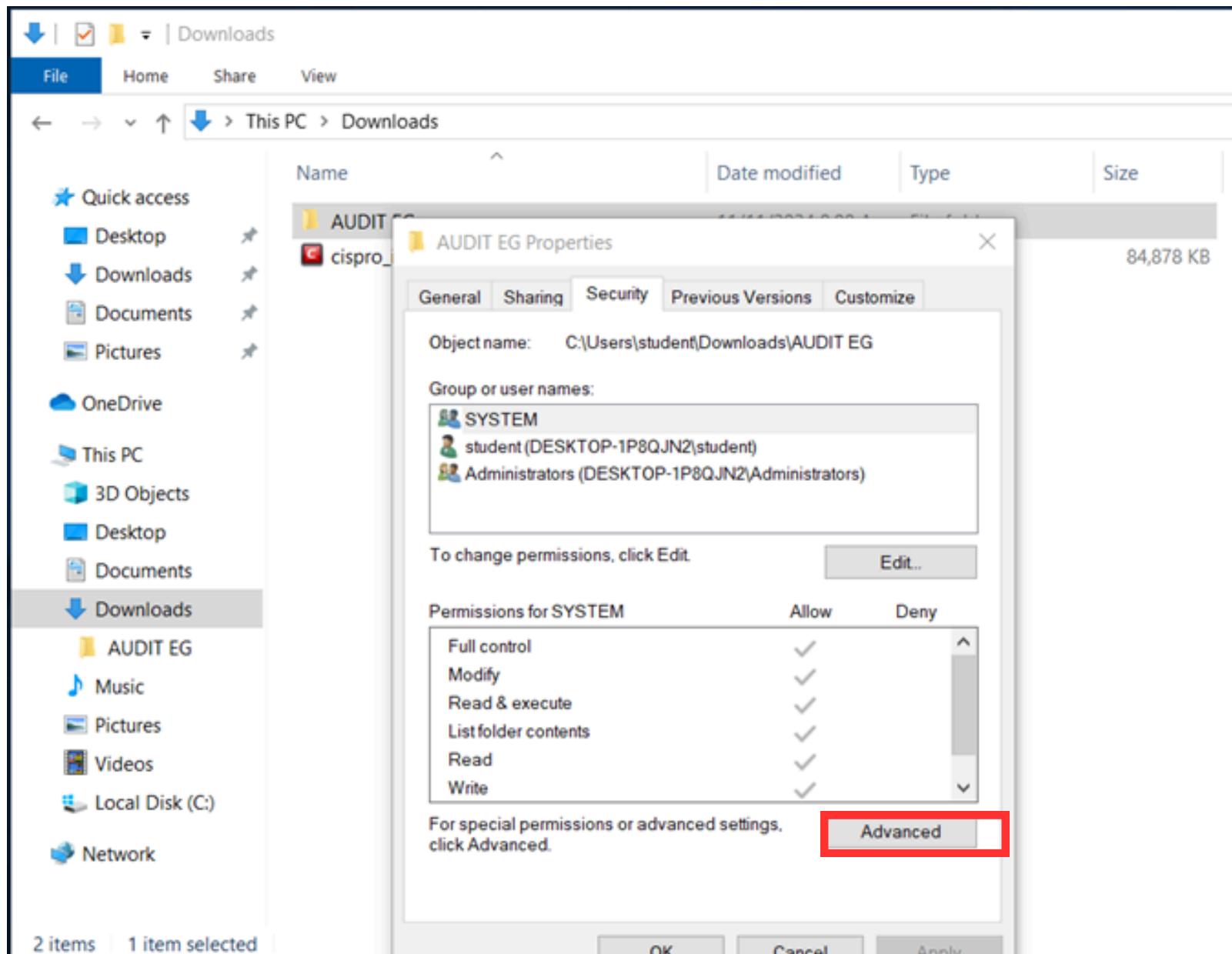


4.On the file you want to audit,right click and select 'Properties' e.g : 'AUDIT EG'

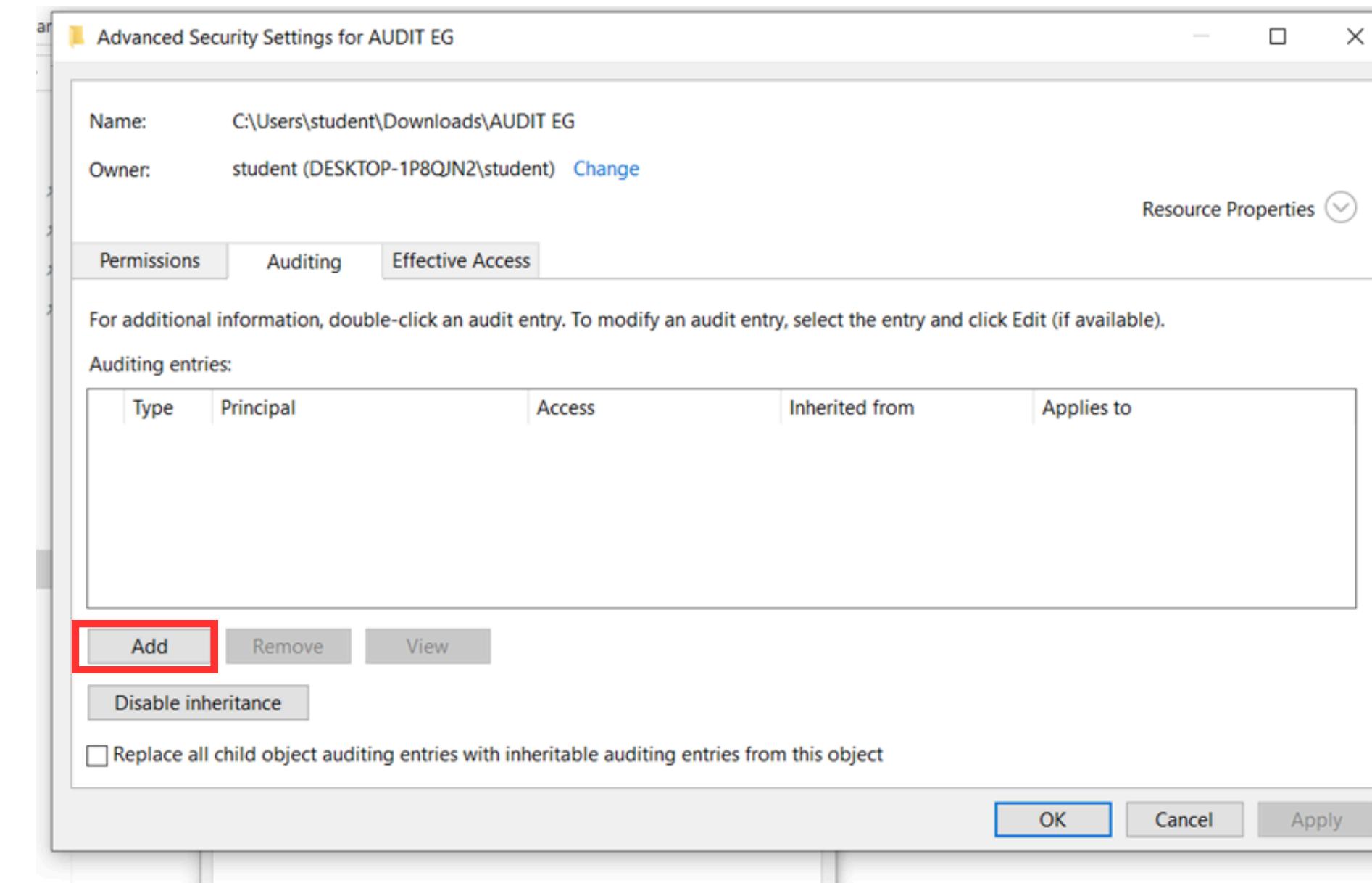


tasks

5.Go to the Security tab and click 'Advanced'



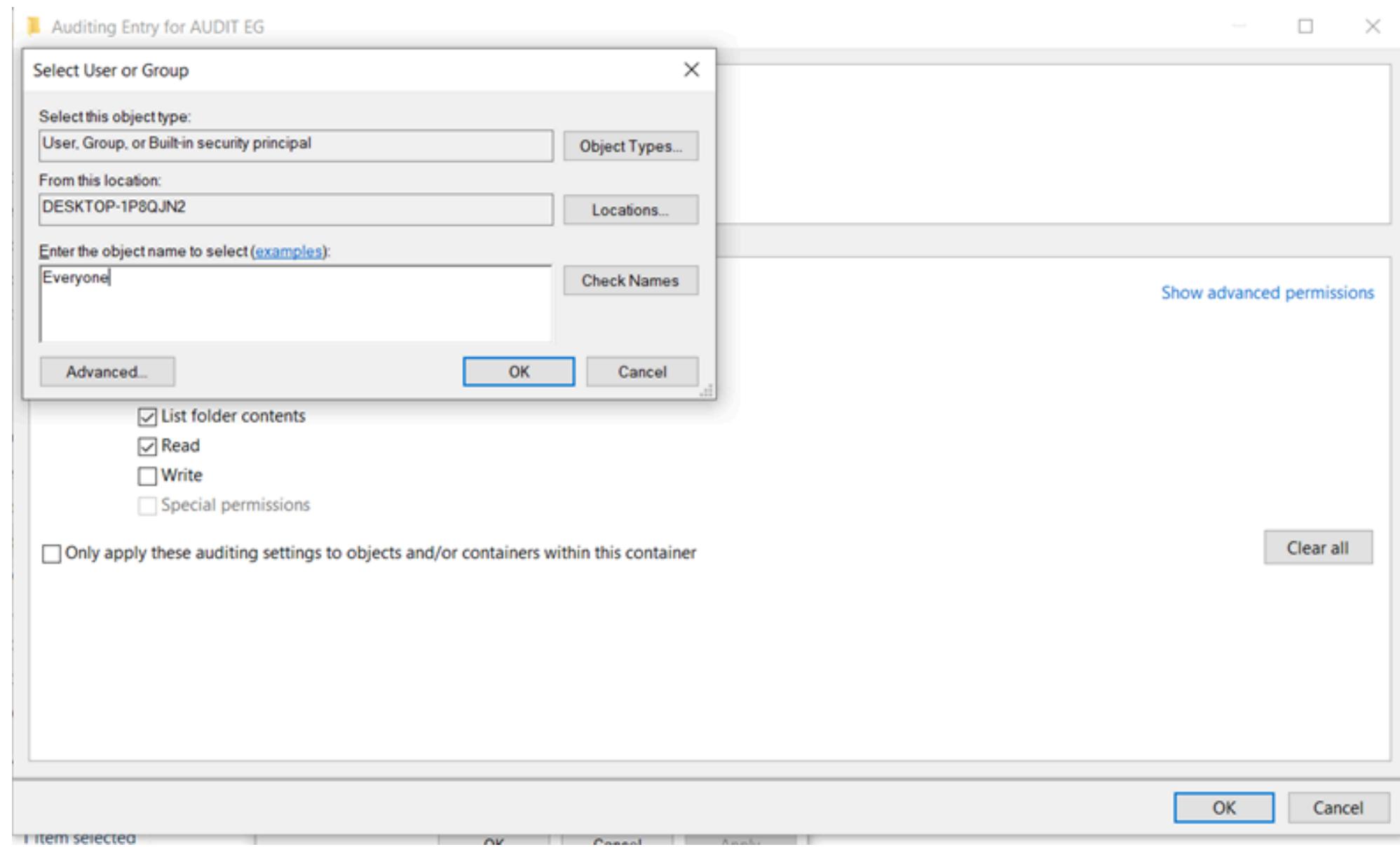
6.Click on Add





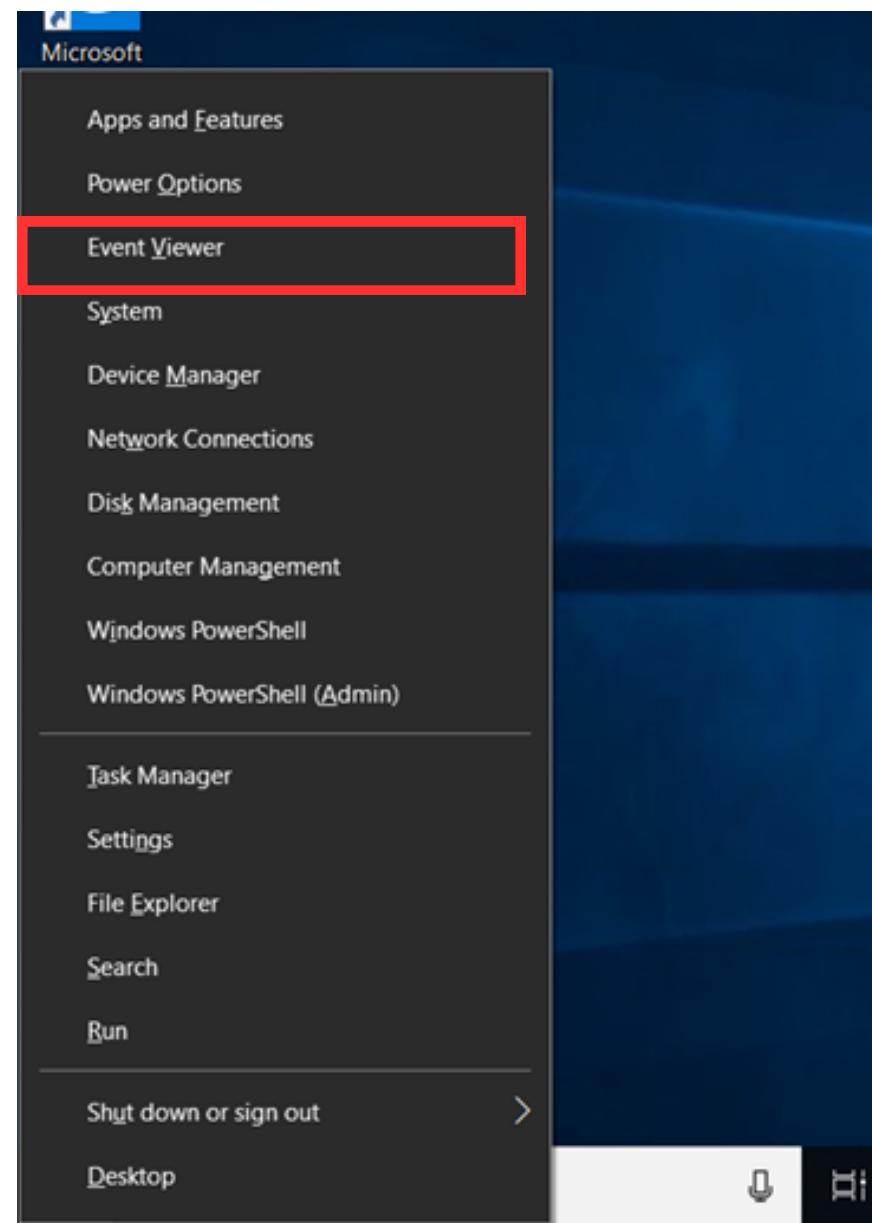
_tasks

7.Click on 'Particular groups',then enter the object as 'everyone', click check names, and ok. Tick the boxes you want to audit.E.g-Read, Write and Modify, and Click ok



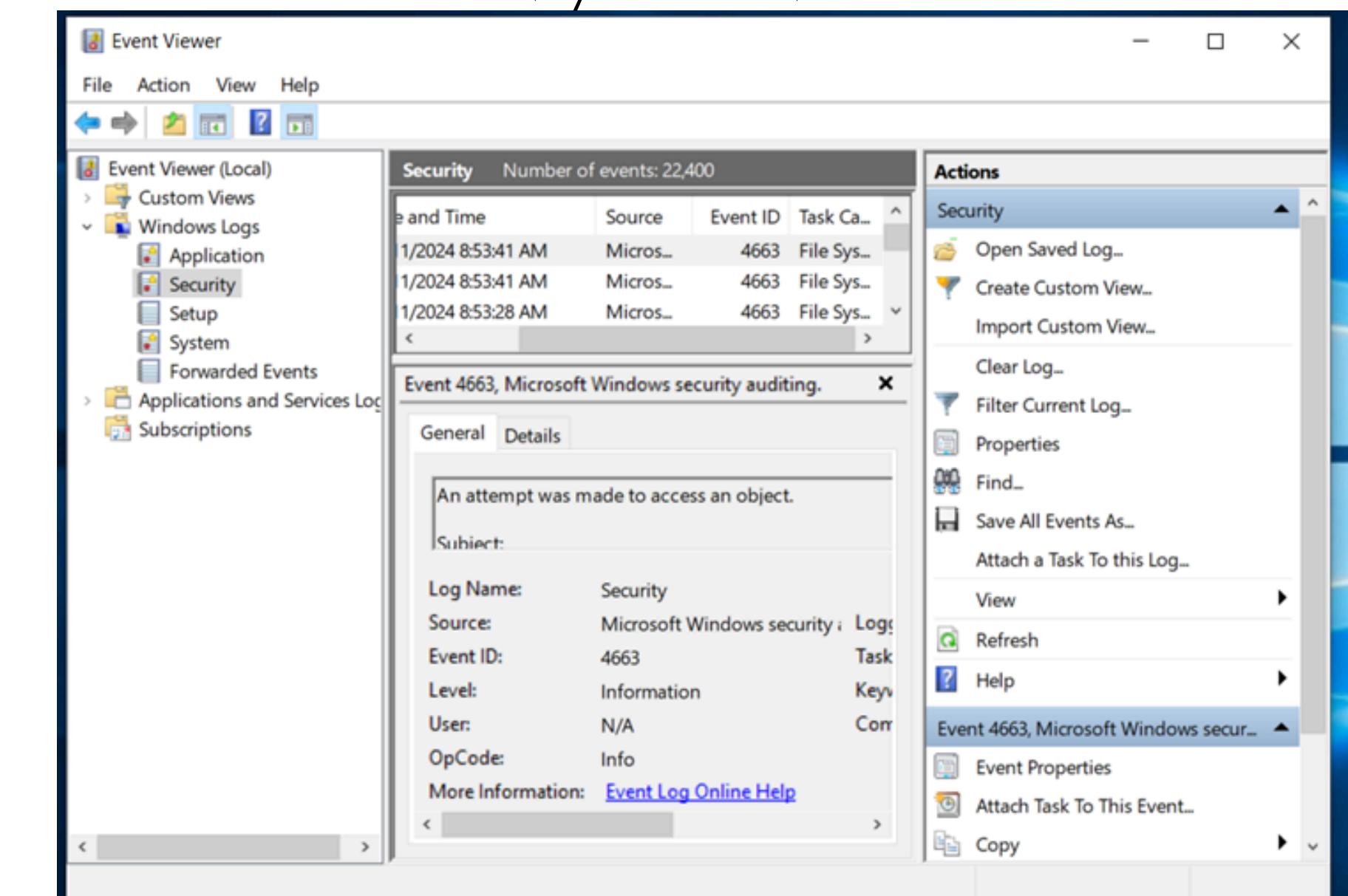
tasks

1.Press Win + X and select Event Viewer



CHECK FOR AUDIT

2.In Event Viewer,navigate to:Windows Logs > Security.Look for event id 4663(which is logged for file access attempts).You can filter the logs to only show relevant events, such as file access and modifications, to quickly track activity on sensitive data.



device protection and malware stuff

by Jun Lin

tasks

done by Jun Lin

(12) Disable USB, or Disable Autorun and Boot from USB (preferred)

(13) Install antivirus software and updates

(20) Maximize or Enhance Windows Defender Features

 (a) Antivirus

 (b) Exploit Guard

 (c) Device Guard

 (d) Application Guard (Not completed)

 (e) Credential Guard

(14) Keep up-to-date on the latest security updates

(17) Enable Auto Updates

(21) Enable Microsoft SmartScreen

} base tasks

device protection and malware stuff

tasks

done by Jun Lin

- (34) Network Level Authentication (NLA) for RDP
- (37) Enabling Memory Integrity
- (38) Disabling Auto login



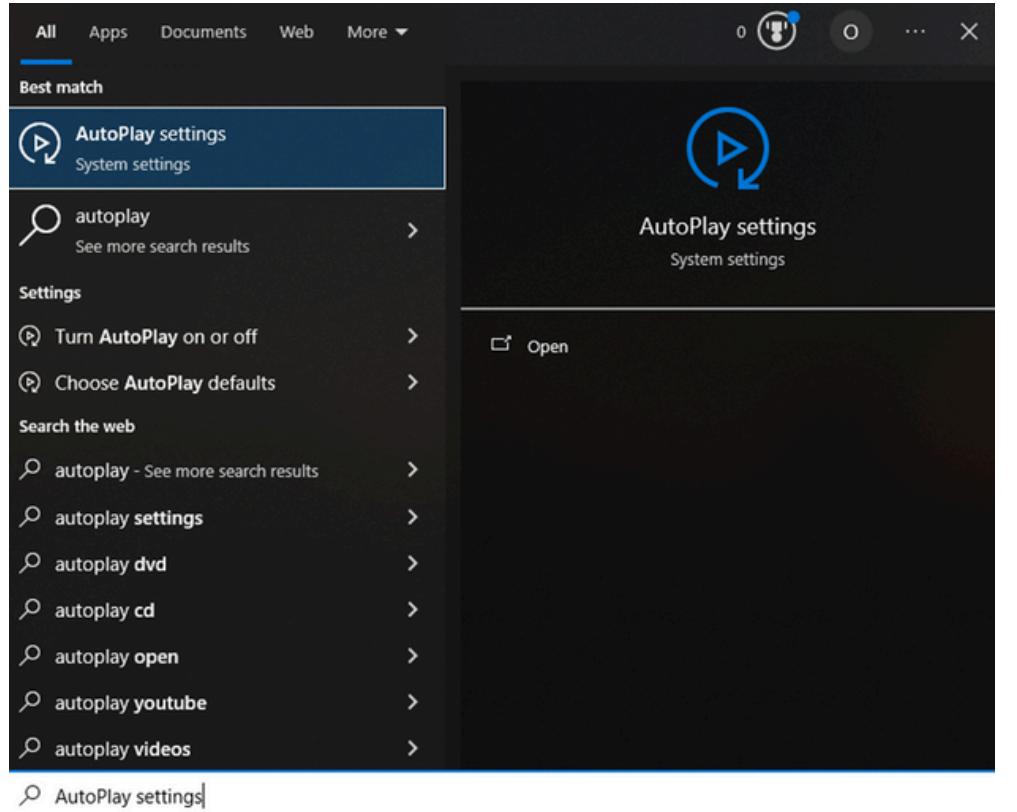
additional tasks

device protection and malware stuff

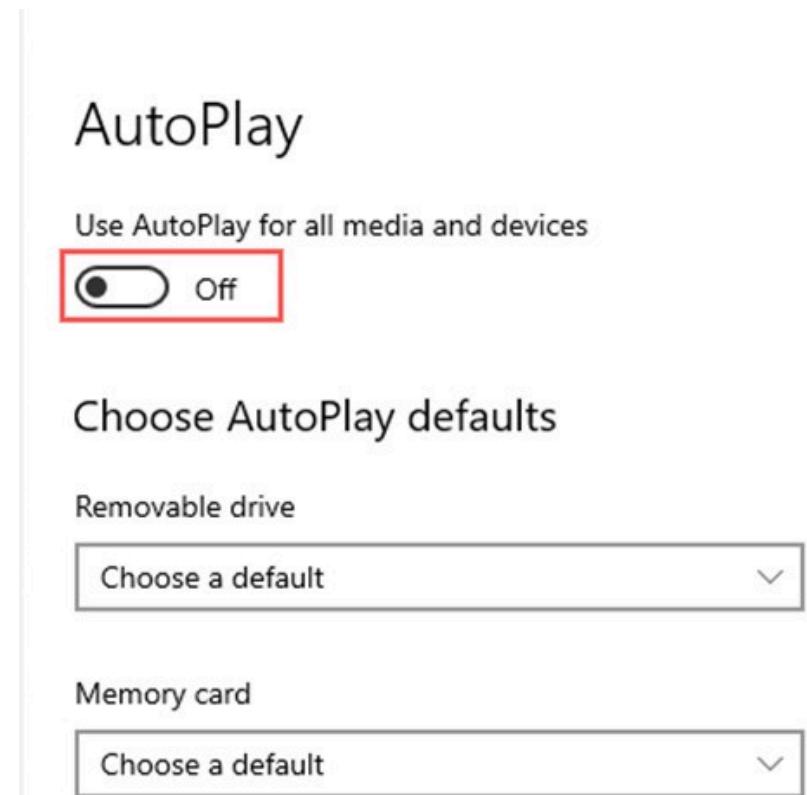
_tasks

(12) Disable Autorun and Boot from USB

1. Search for AutoPlay Settings and press Enter



2. Toggle Off AutoPlay



device protection and malware stuff

tasks

(12) Disable Autorun and Boot from USB

3. Select 'Take No Action' in the drop-down menu below 'Removable drive' and below 'Memory card'

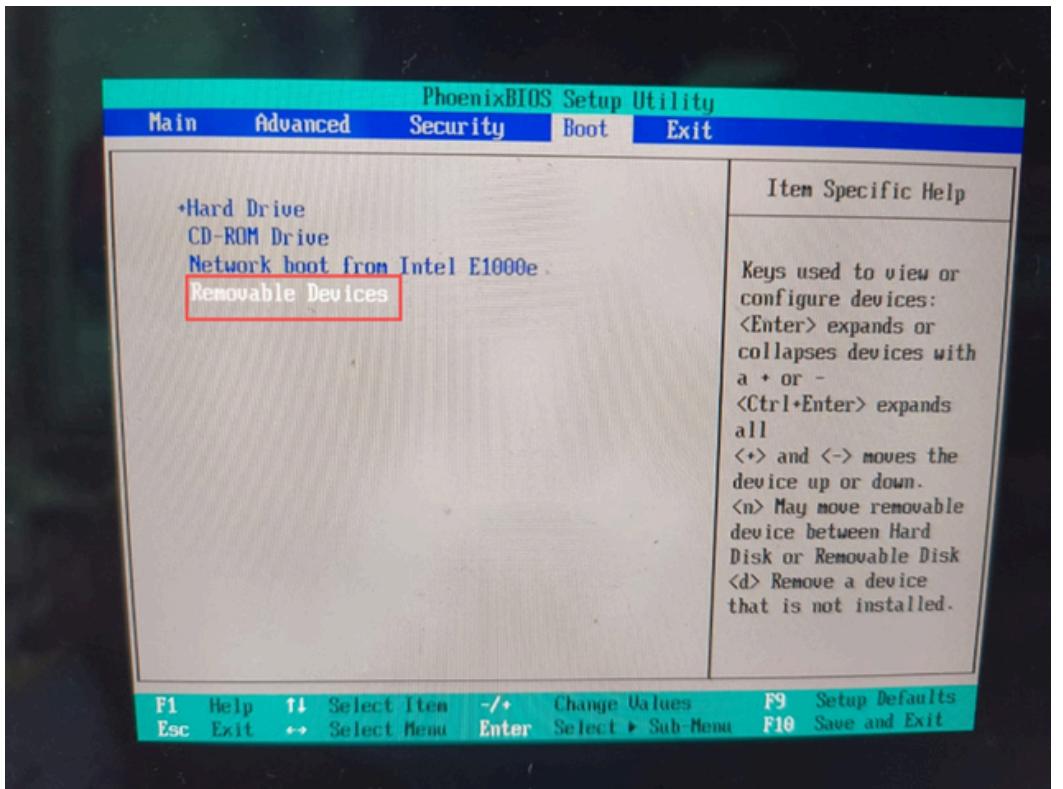


device protection and malware stuff

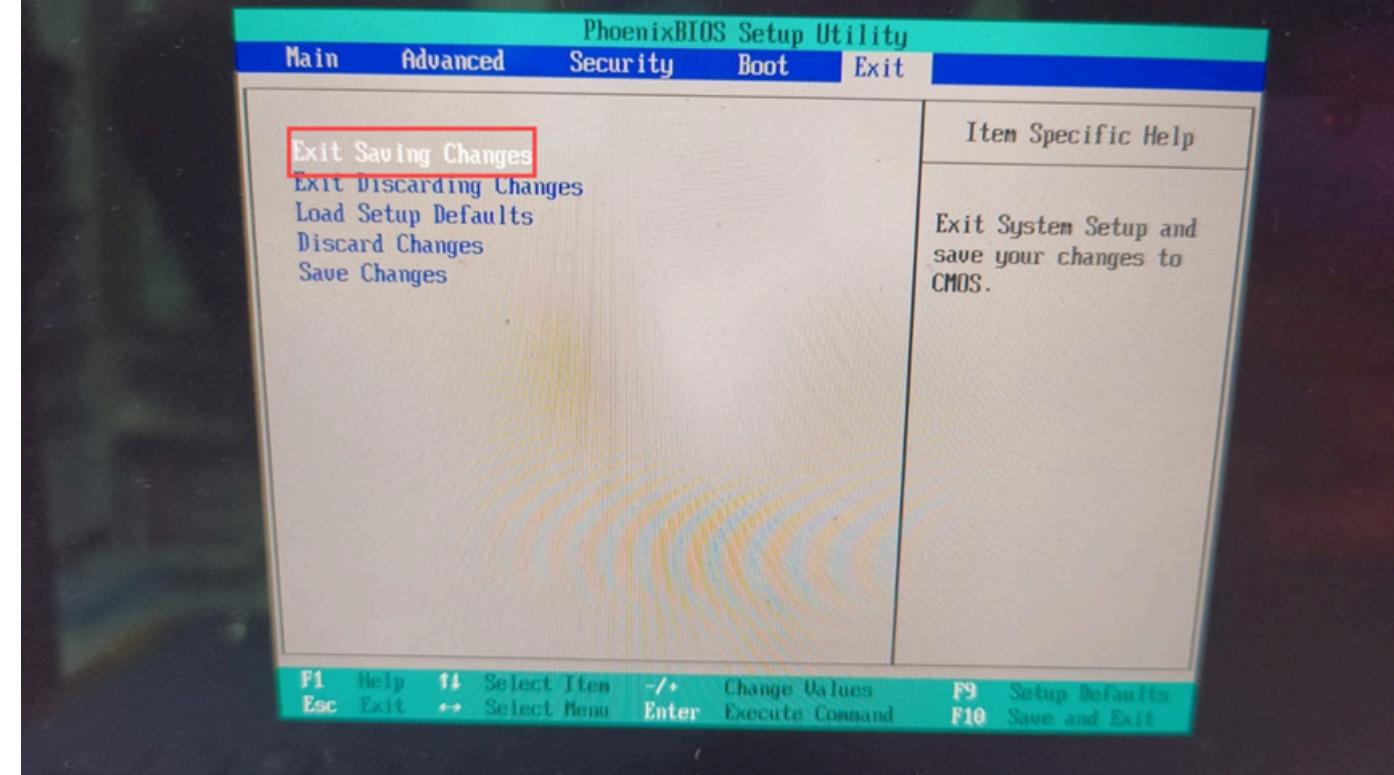
tasks

(12) Disable Autorun and Boot from USB

4. Go to BIOS > Boot Tab and move 'Removable Devices' to the bottom by pressing the “ - ” key



5. Proceed to the Exit tab and Exit Saving Changes



device protection and malware stuff

— tasks

(13) Install antivirus software and updates

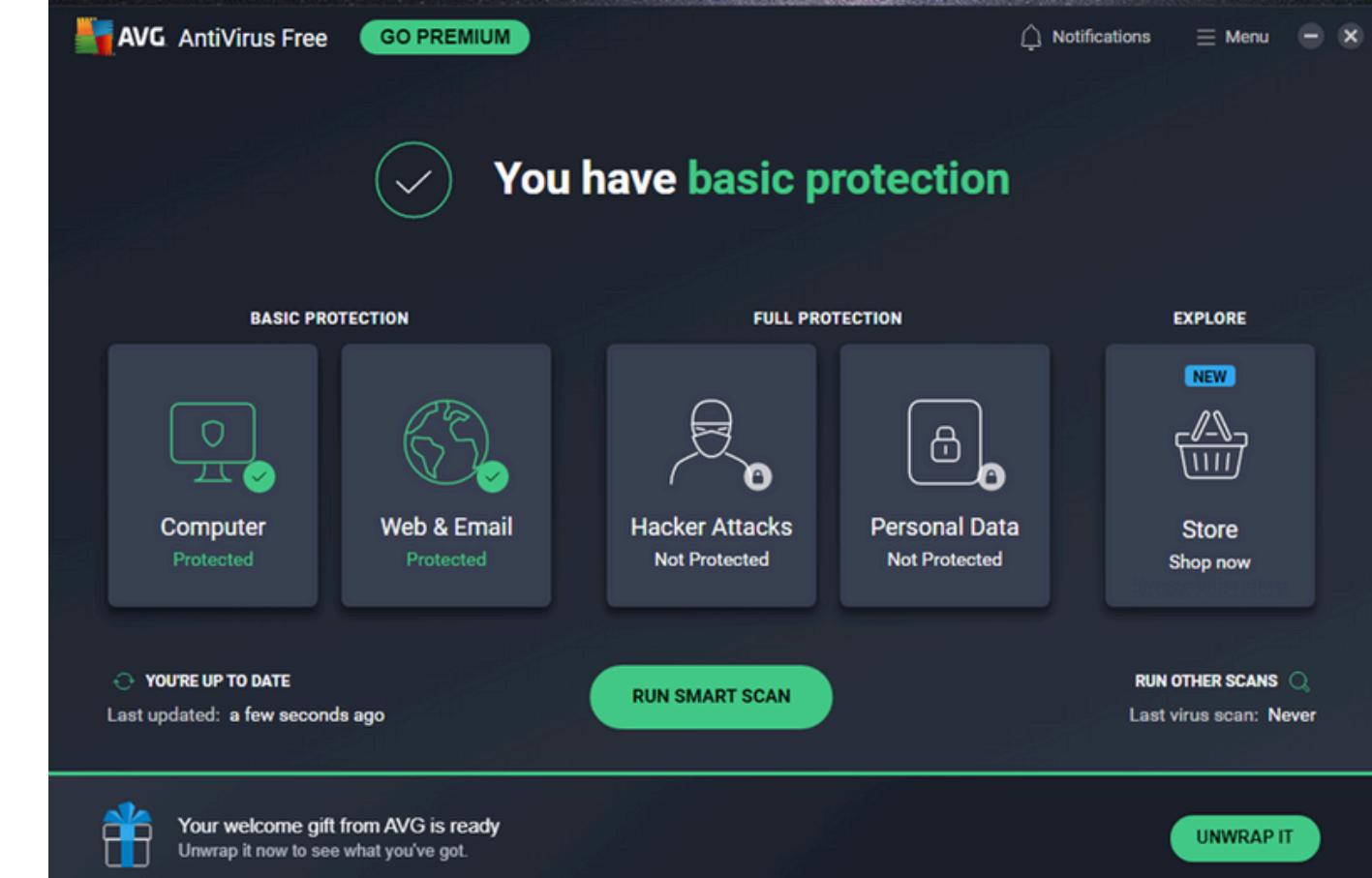


1. Visit the Microsoft Store > search for AVG AntiVirus Free > Install



device protection and malware stuff

2. Launch AVG > follow through with the initial setup
> Run a Smart Scan

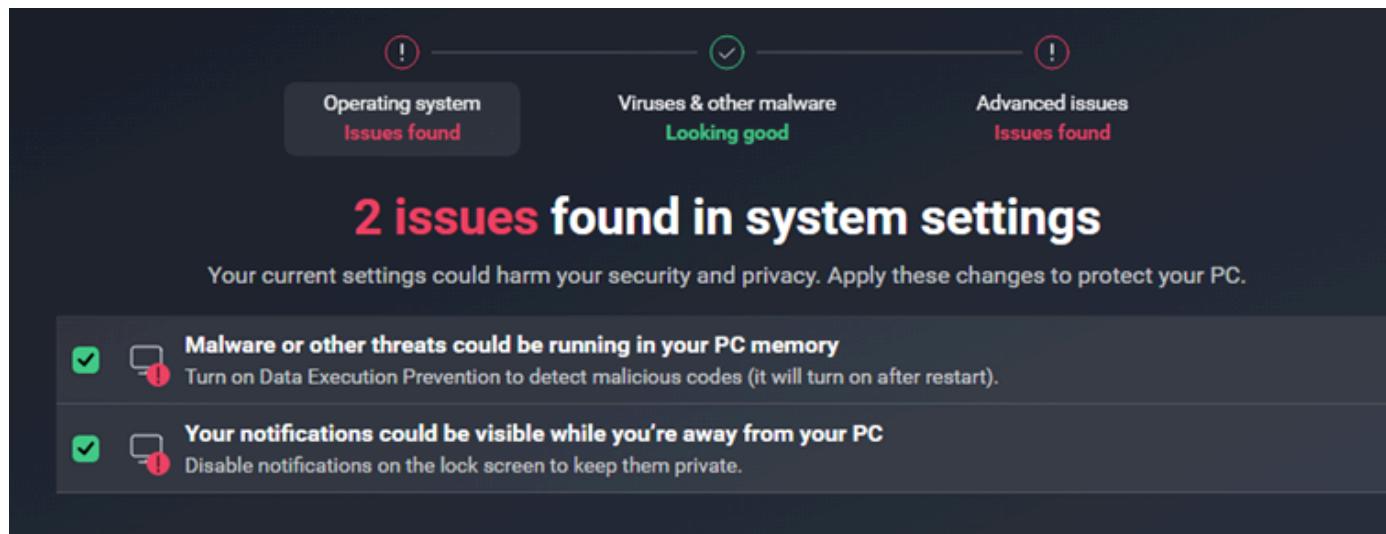


— tasks

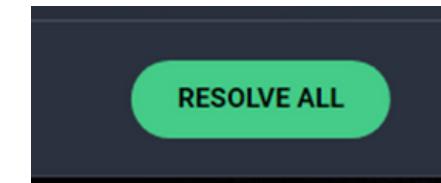
(13) Install antivirus software and updates



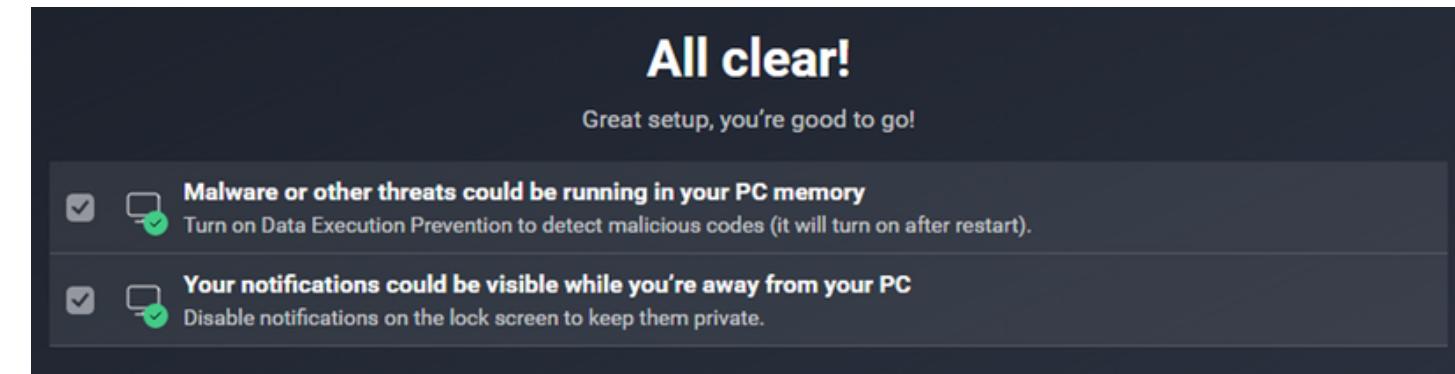
3. If there are issues found with your system
> Review them to check if needed



Click Resolve All to fix the detected issues



Once okay, you will see the following message:



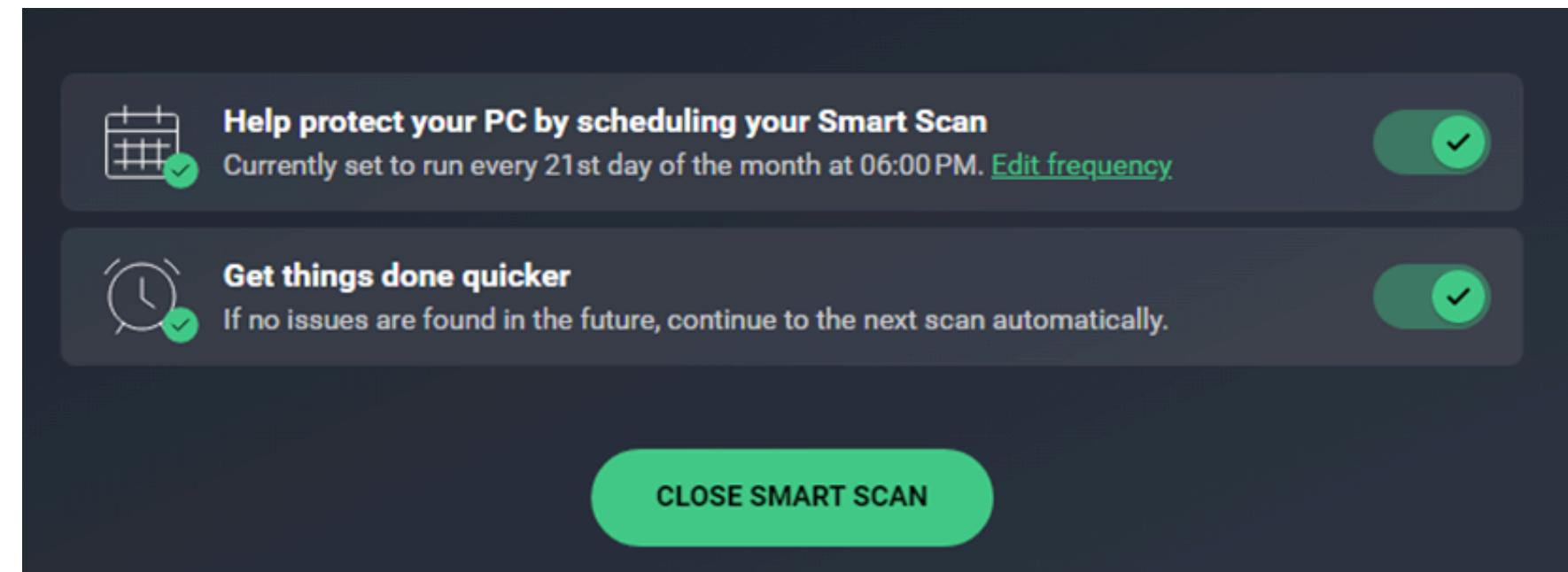
device protection and malware stuff

_tasks

(13) Install antivirus software and updates



Here are some additional settings to enable if automation is preferred



device protection and malware stuff

tasks

(13) Install antivirus software and updates

4. Go to Windows Security > Virus & threat protection and turn on Periodic scanning for automation



🛡 Virus & threat protection

Protection for your device against threats.

AVG Antivirus

AVG Antivirus is turned on.

Current threats

✓ No actions needed.

Protection settings

✓ No actions needed.

Protection updates

✓ No actions needed.

[Open app](#)

Microsoft Defender Antivirus options

You can keep using your current provider, and have Microsoft Defender Antivirus periodically check for threats.

Periodic scanning

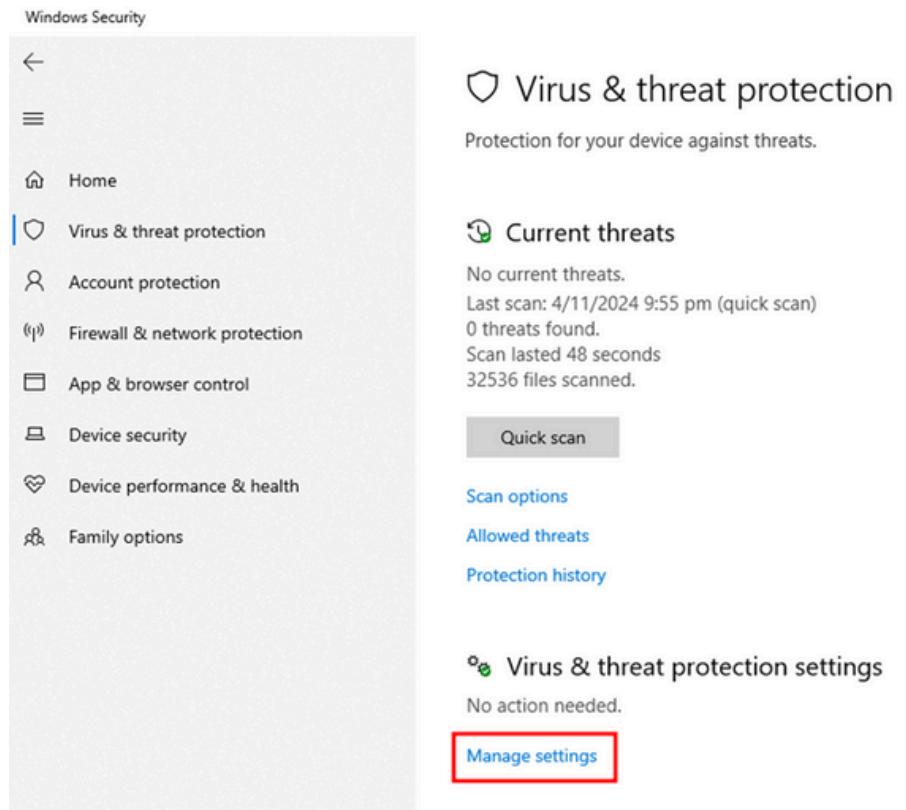
On

device protection and malware stuff

tasks

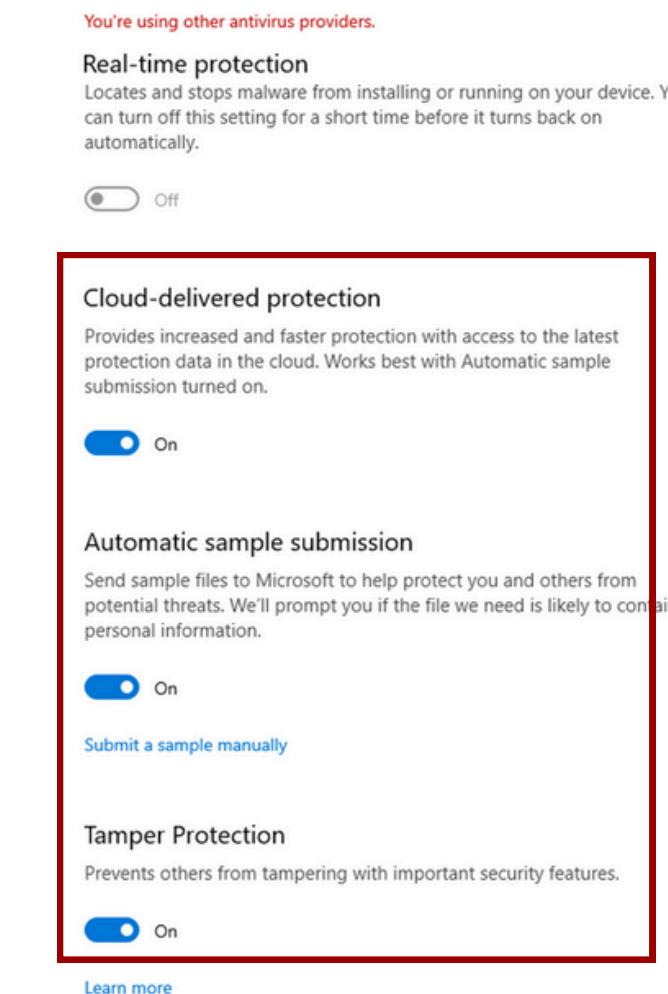
(20) Maximize or Enhance Windows Defender Features (Antivirus)

1. Launch Windows Security > “Virus & threat protection” > “Manage settings”



device protection and malware stuff

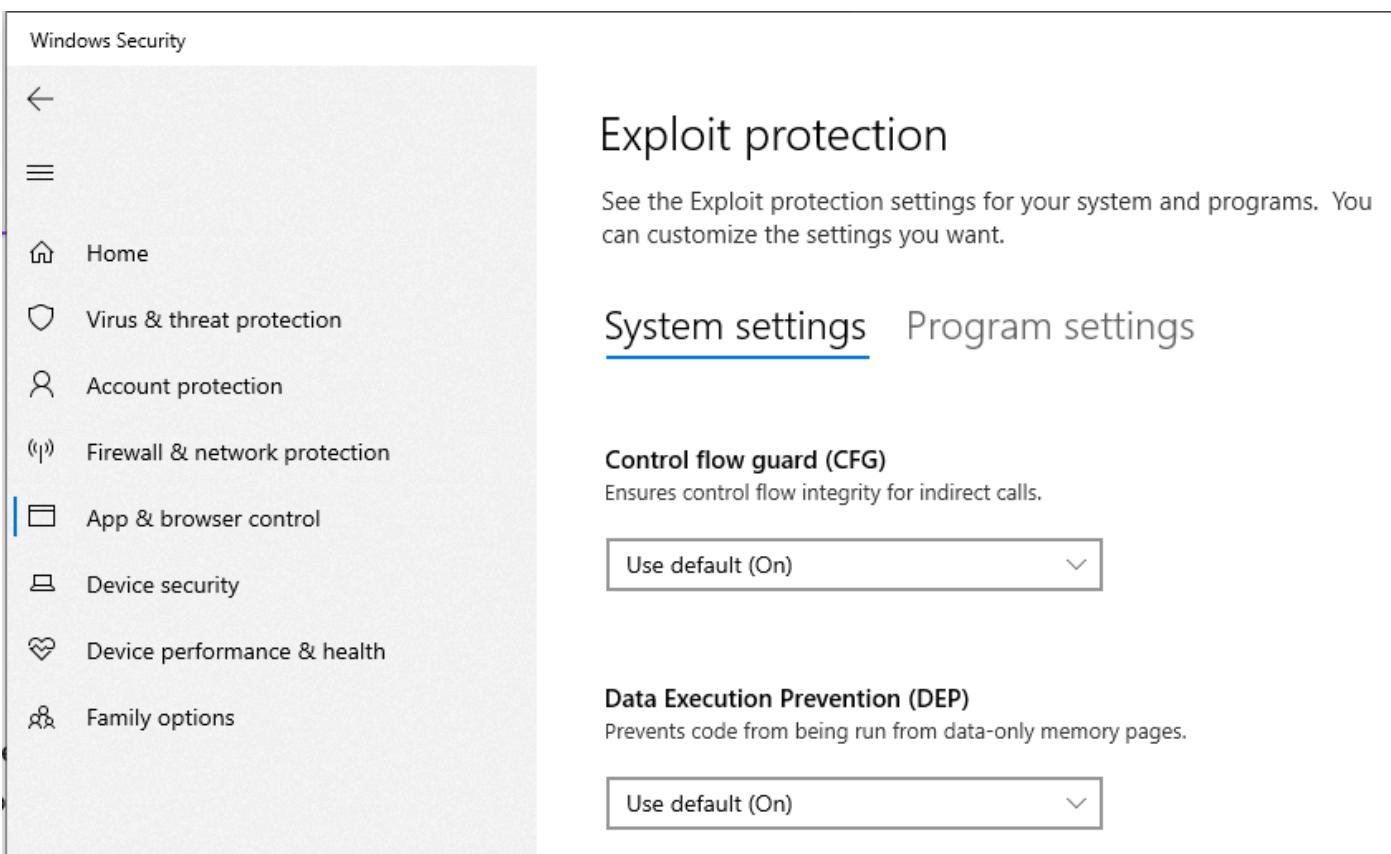
2. Turn on “Cloud-delivered protection”, “Automatic sample submission”, and “Tamper



tasks

(20) Maximize or Enhance Windows Defender Features (Exploit Guard)

1. Open “Windows Security” > App & browser control > Exploit protection setting



device protection and malware stuff

tasks

(20) Maximize or Enhance Windows Defender Features (Exploit Guard)

2. Turn on these settings:

- Control Flow Guard (CFG)
- Data Execution Prevention (DEP)
- Randomize memory allocations (ASLR)
- Validate heap integrity

Control flow guard (CFG)

Ensures control flow integrity for indirect calls.

On by default

This change requires you to restart your device.

Data Execution Prevention (DEP)

Prevents code from being run from data-only memory pages.

On by default

This change requires you to restart your device.

Randomize memory allocations (Bottom-up ASLR)

Randomize locations for virtual memory allocations.

On by default

This change requires you to restart your device.

Validate heap integrity

Terminates a process when heap corruption is detected.

On by default

Export settings

tasks

(20) Maximize or Enhance Windows Defender
Features (Exploit Guard)

3. Go to Windows Security > Virus and threat protection > Manage ransomware protection

 Ransomware protection

No action needed.

[Manage ransomware protection](#)

device protection and malware stuff

4. Turn on 'Controlled folder access

 Ransomware protection

Protect your files against threats like ransomware, and see how to restore files in case of an attack.

Controlled folder access

Protect files, folders, and memory areas on your device from unauthorized changes by unfriendly applications.



[Block history](#)

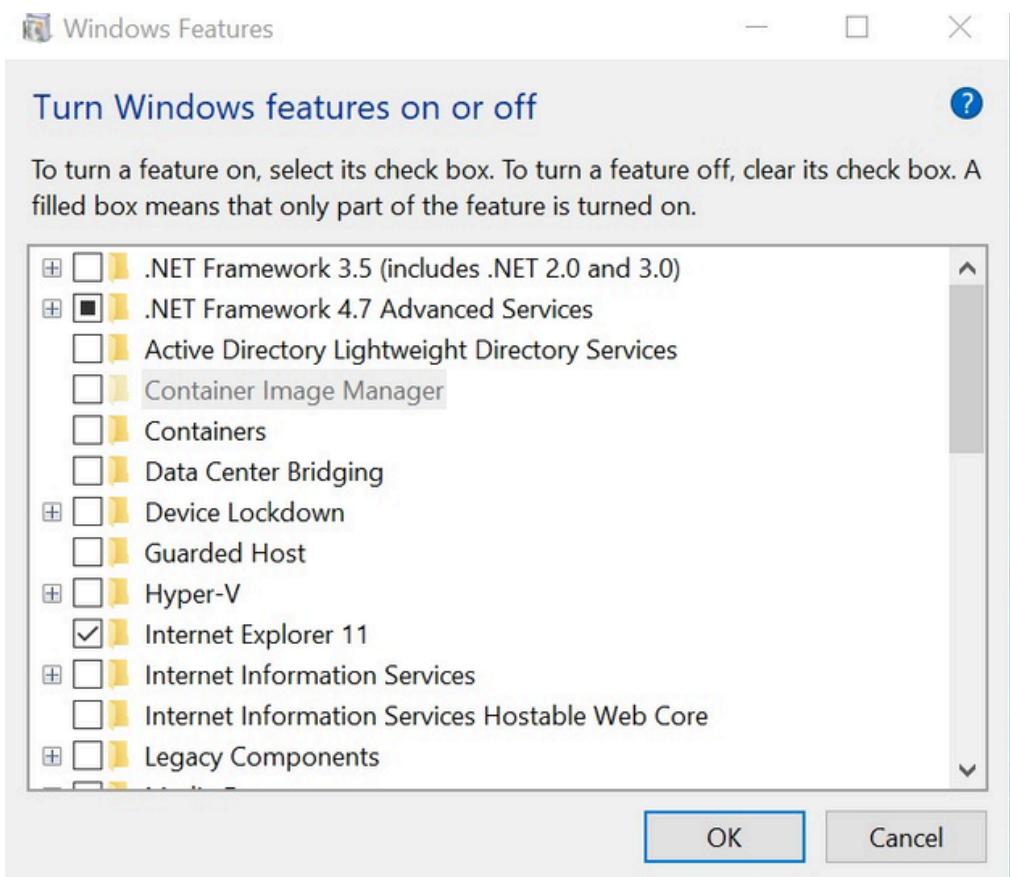
[Protected folders](#)

[Allow an app through Controlled folder access](#)

_tasks

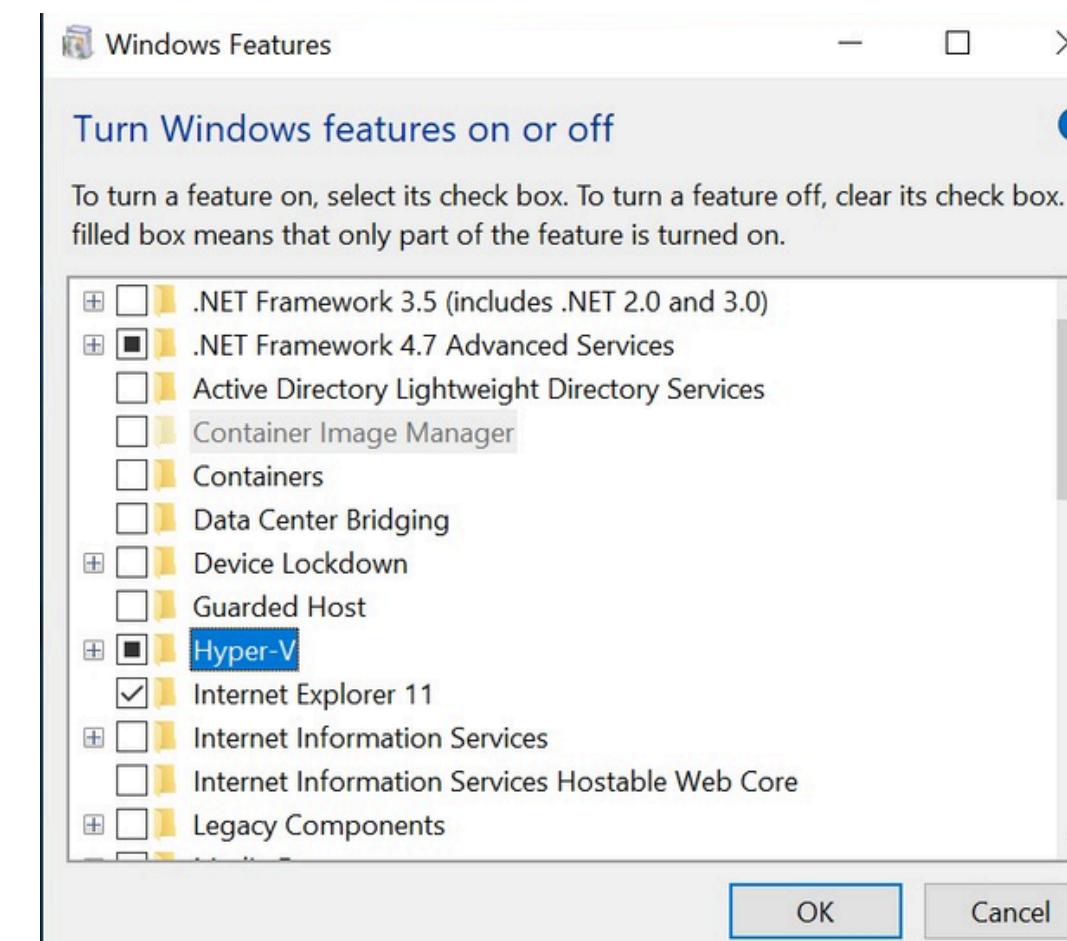
(20) Maximize or Enhance Windows Defender Features (Exploit Guard)

1. Search 'Turn Windows features on or off' and press Enter



device protection and malware stuff

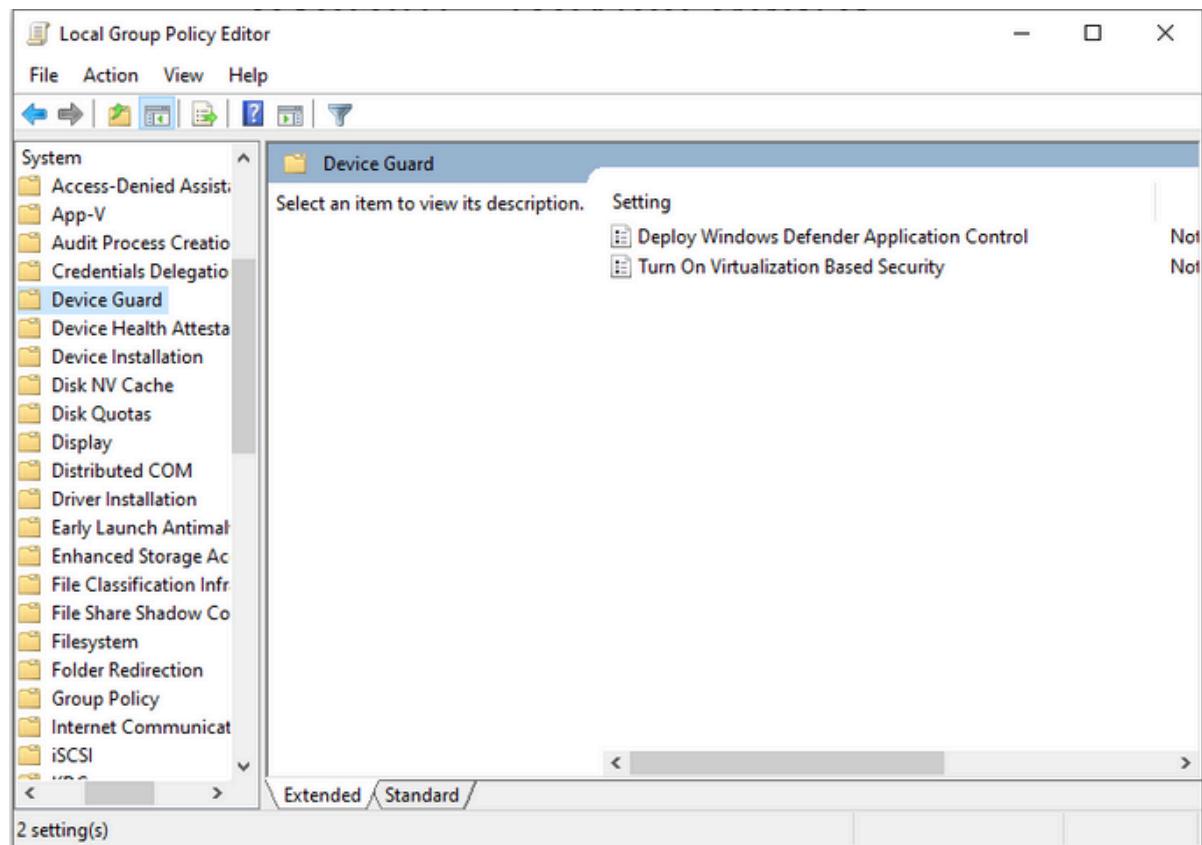
2. Tick the checkbox next to Hyper-V



tasks

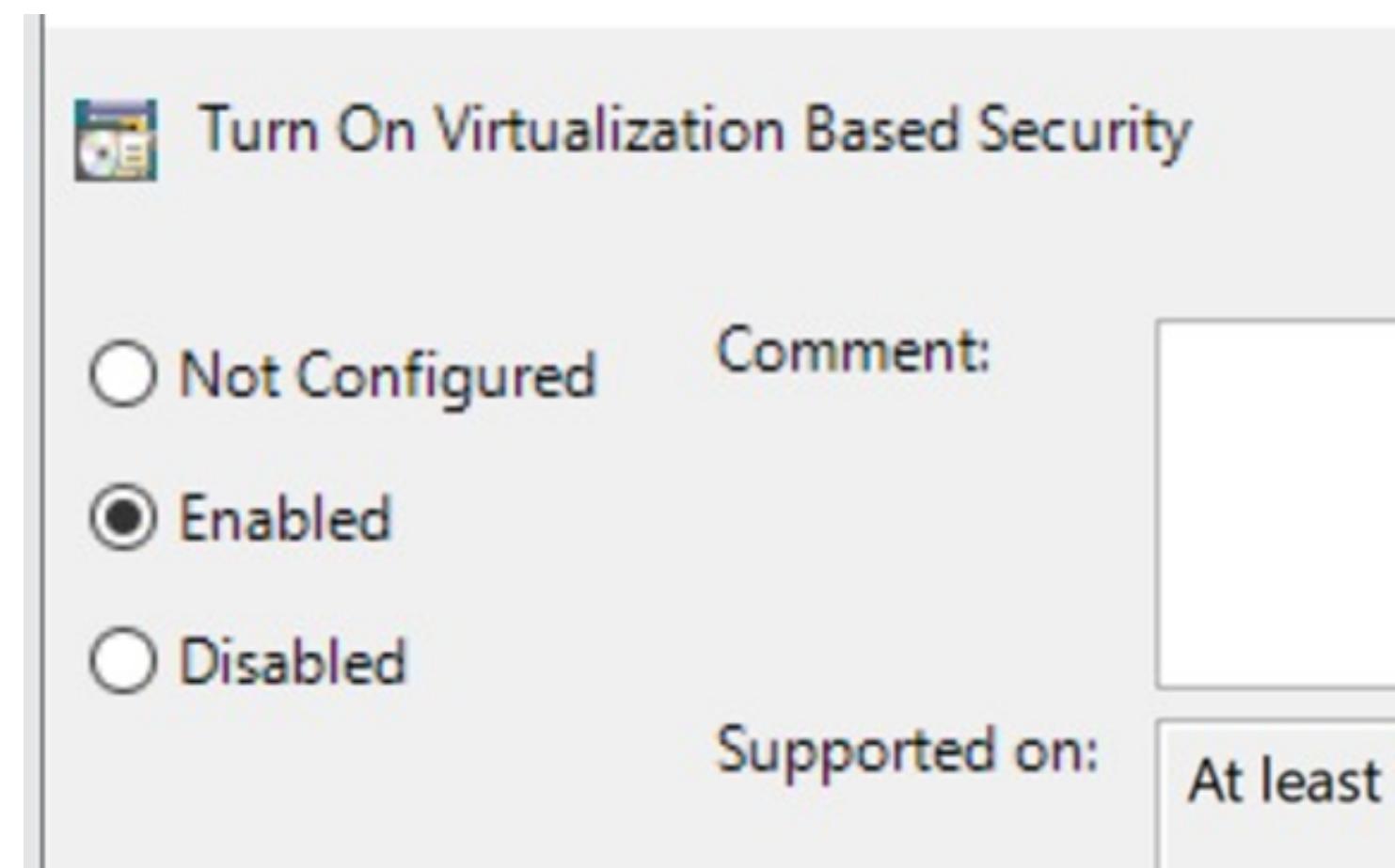
(20) Maximize or Enhance Windows Defender Features (Credential Guard)

1. Open Group Policy Editor > Computer Configuration > Administrative Templates > System > Device Guard



device protection and malware stuff

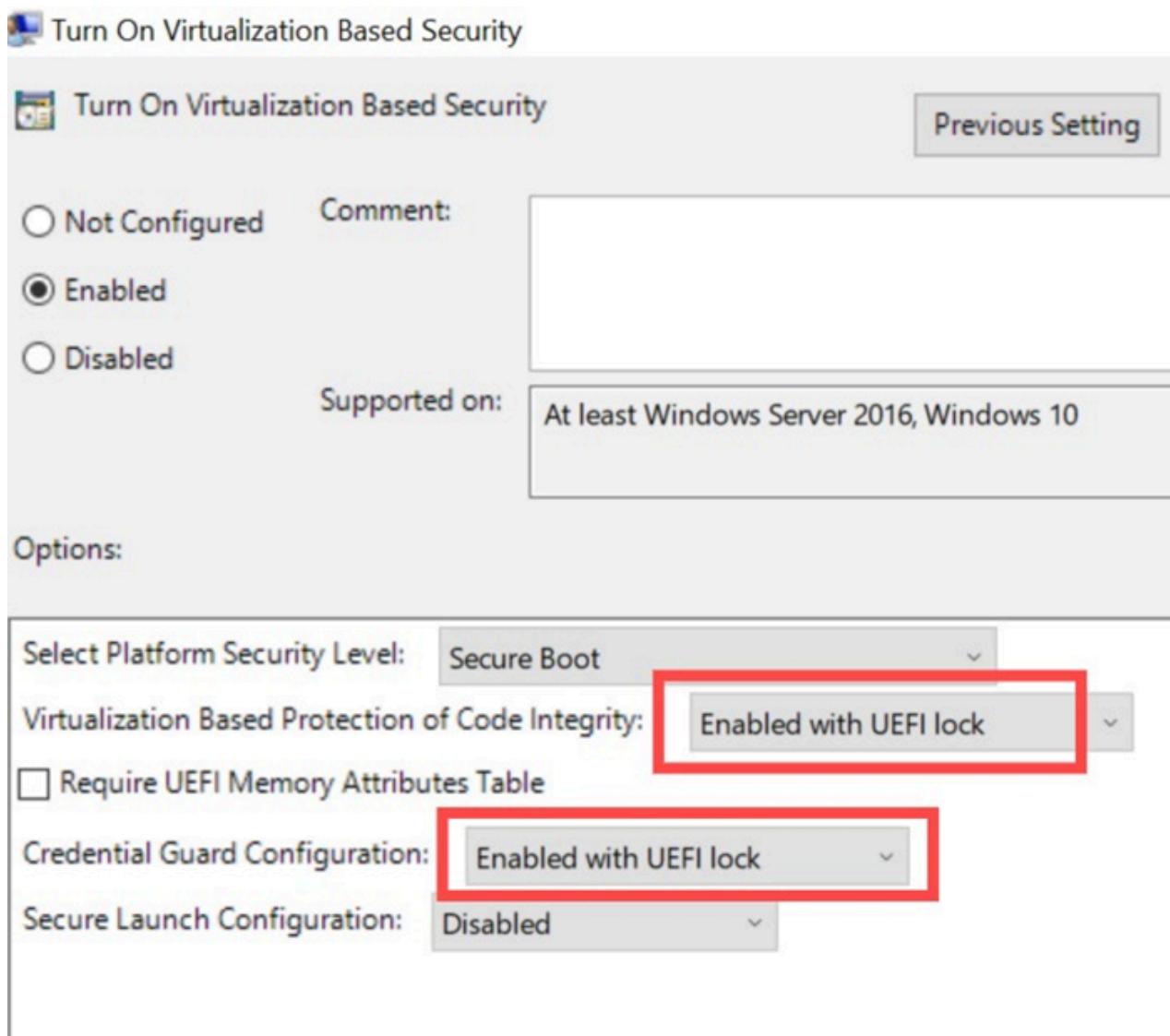
2. Double Click 'Turn On Virtualization Based Security' and set it to enabled



tasks

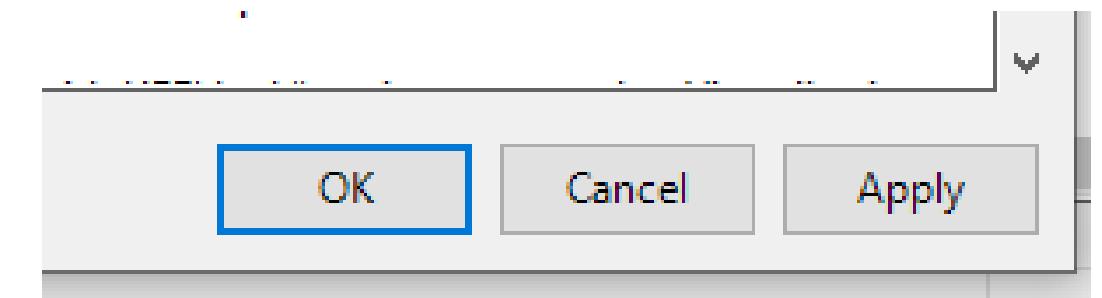
(20) Maximize or Enhance Windows Defender Features (Credential Guard)

3. Next to Virtualization Based Protection of Code Integrity and Credential Guard Configuration, select Enabled with UEFI lock



device protection and malware stuff

Press Apply then OK

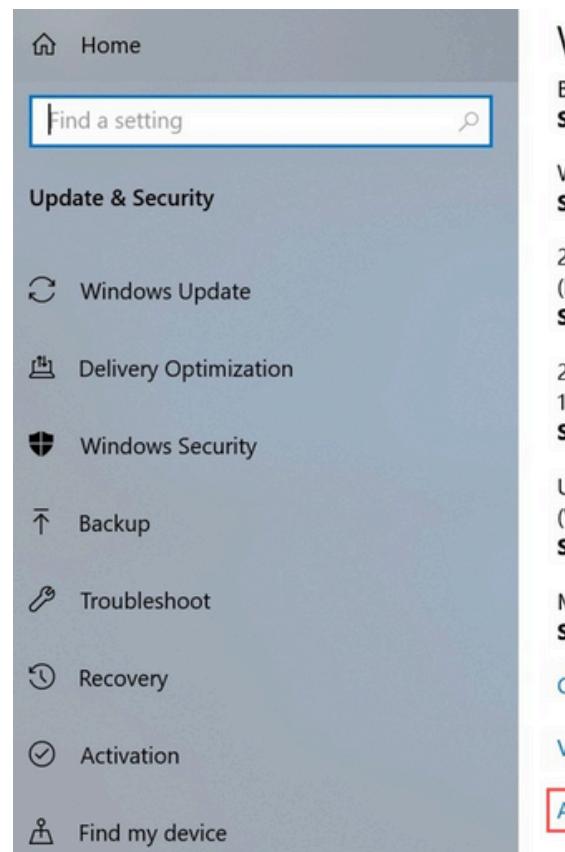


Then Restart for it to take action

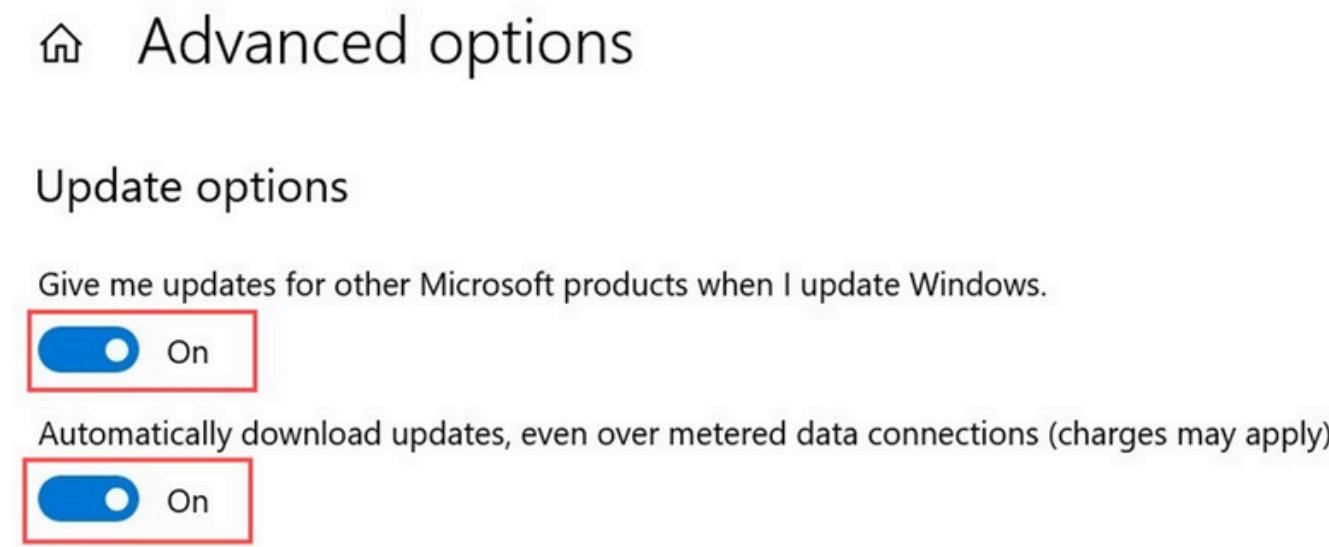
_tasks

(17) Enable Auto Updates

1. Open Settings > Update & Security > Advanced Options.



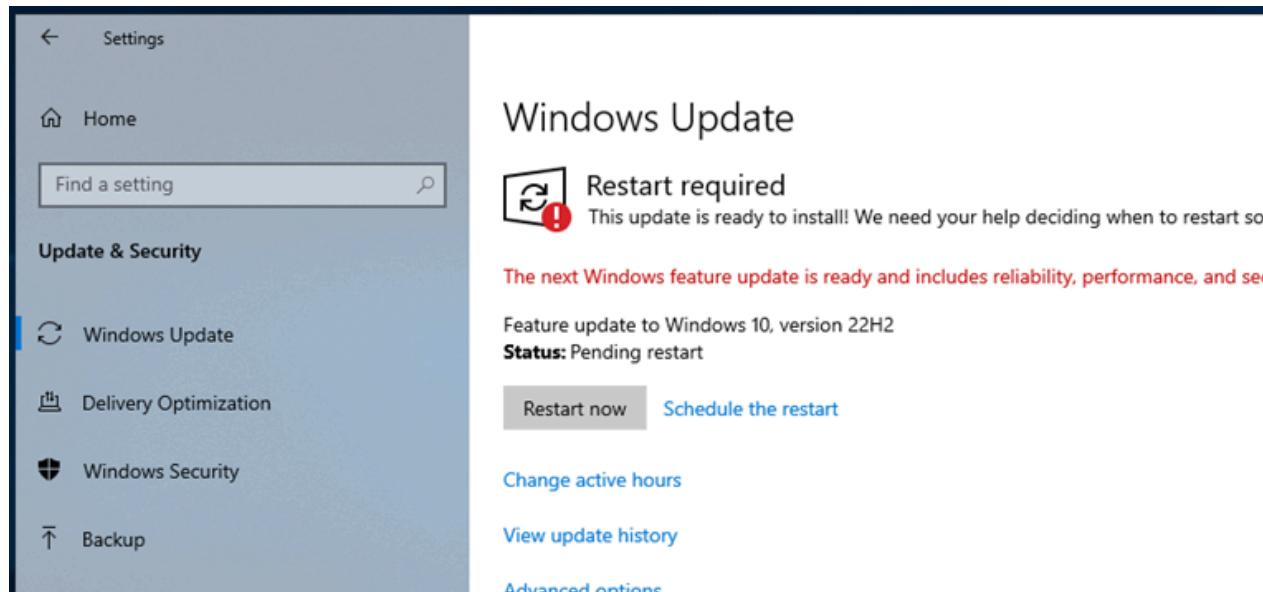
2. Toggle on 'Give me updates' and 'Automatically download updates'



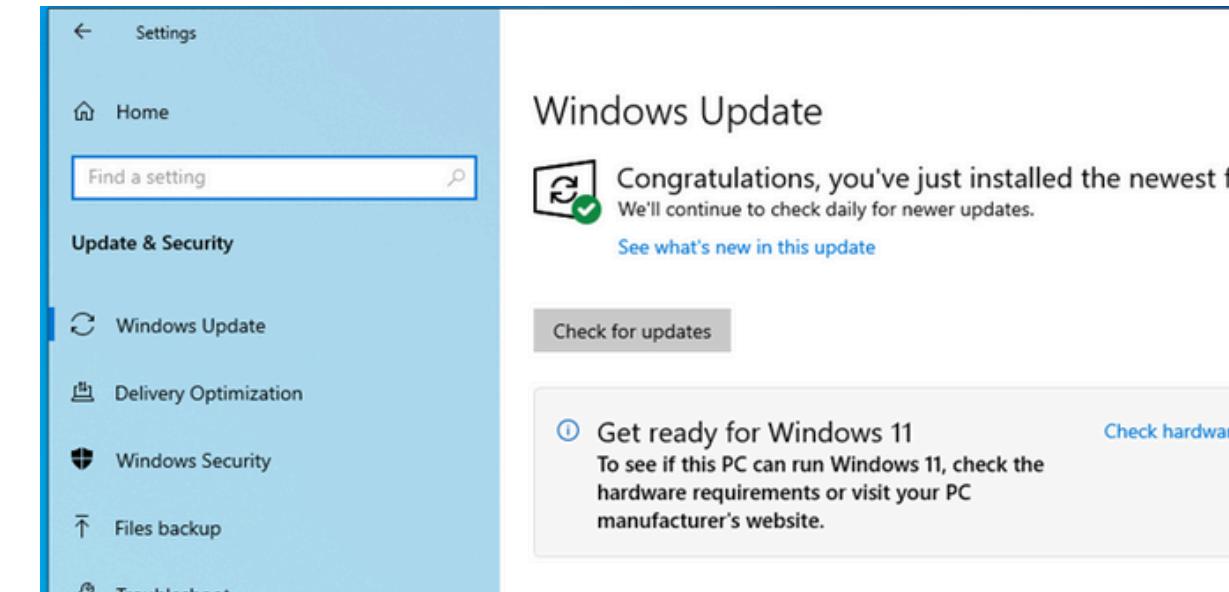
tasks

(14) Keep up to date on the latest security updates

1. Visit Settings > Update & Security > Windows Update



2. After installing and rebooting, you're all set

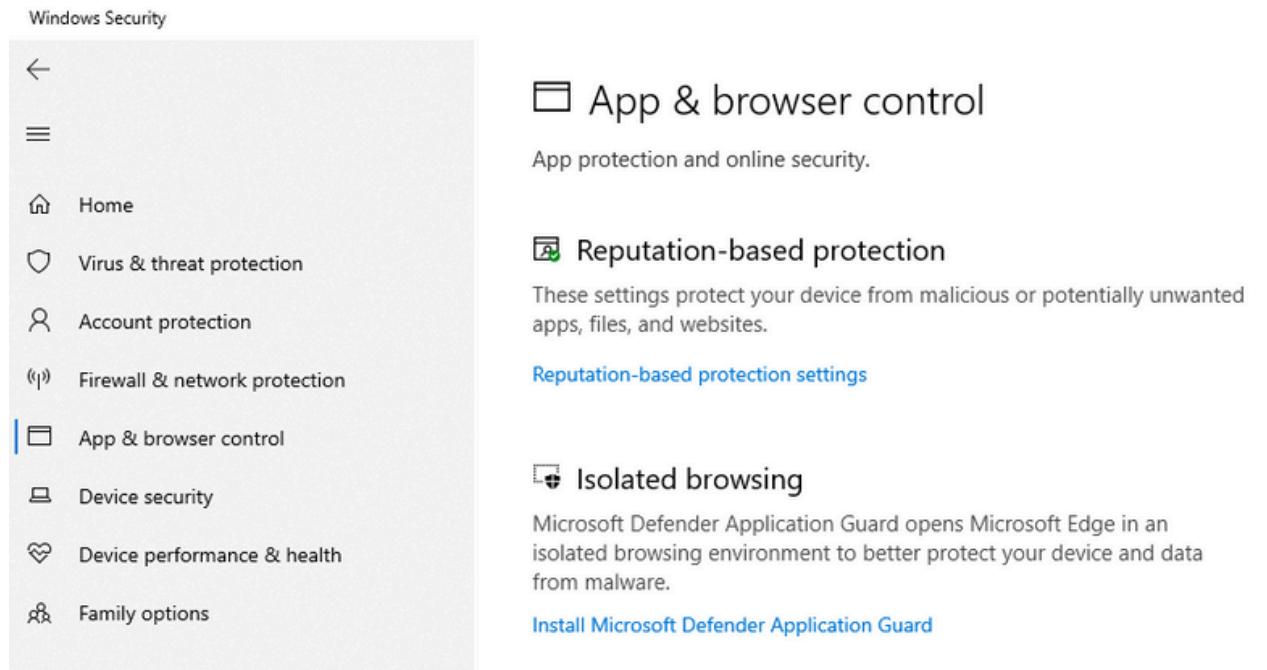


device protection and malware stuff

tasks

(21) Enable Microsoft SmartScreen

1. Visit Windows Security > App & browser control



2. Click on Reputation-based protection settings

Reputation-based protection

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

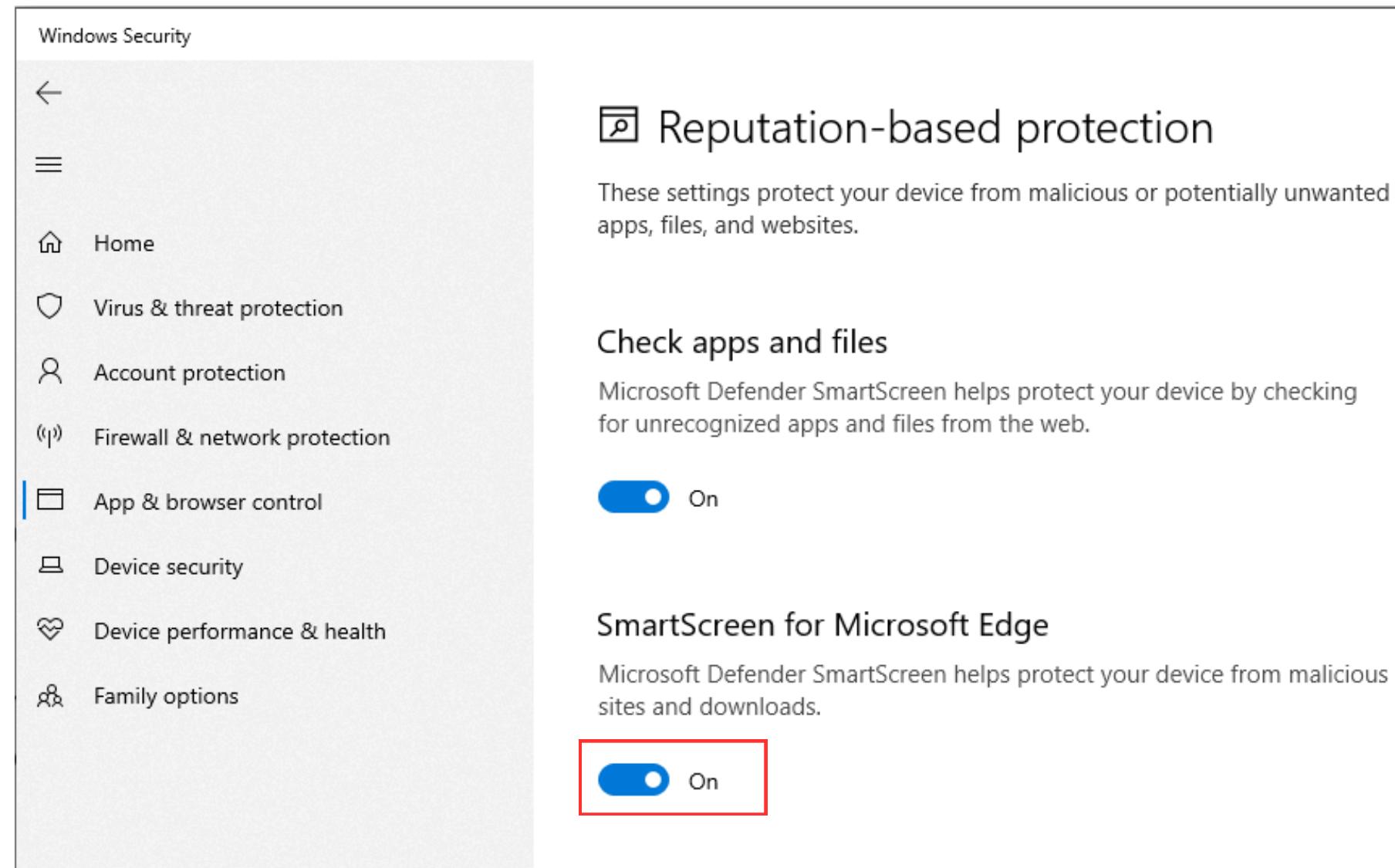
[Reputation-based protection settings](#)

device protection and malware stuff

tasks

(21) Enable Microsoft SmartScreen

3. Make sure SmartScreen
for Microsoft Edge is
enabled

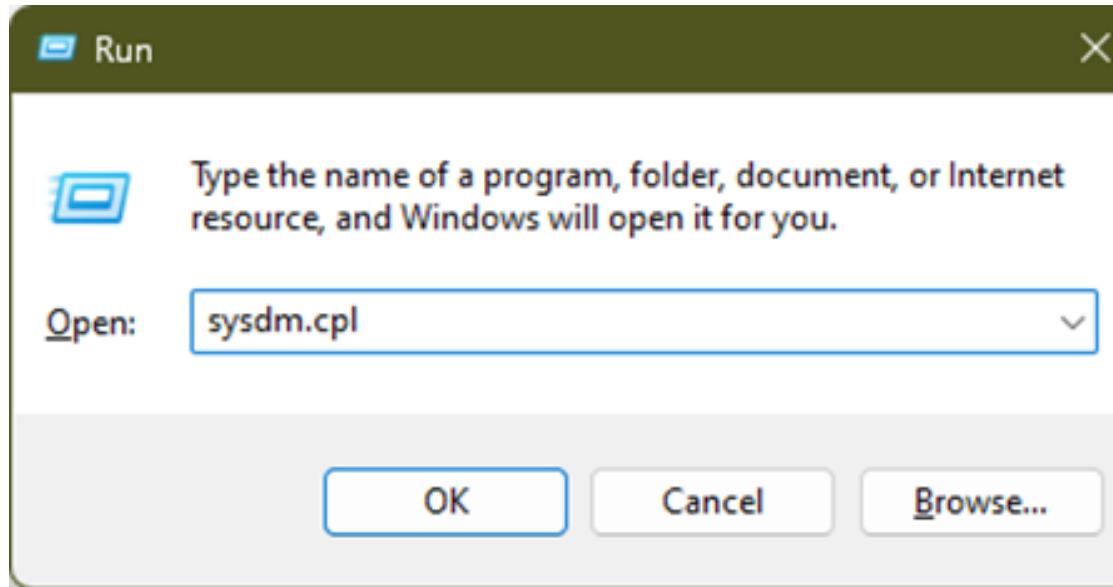


device protection and malware stuff

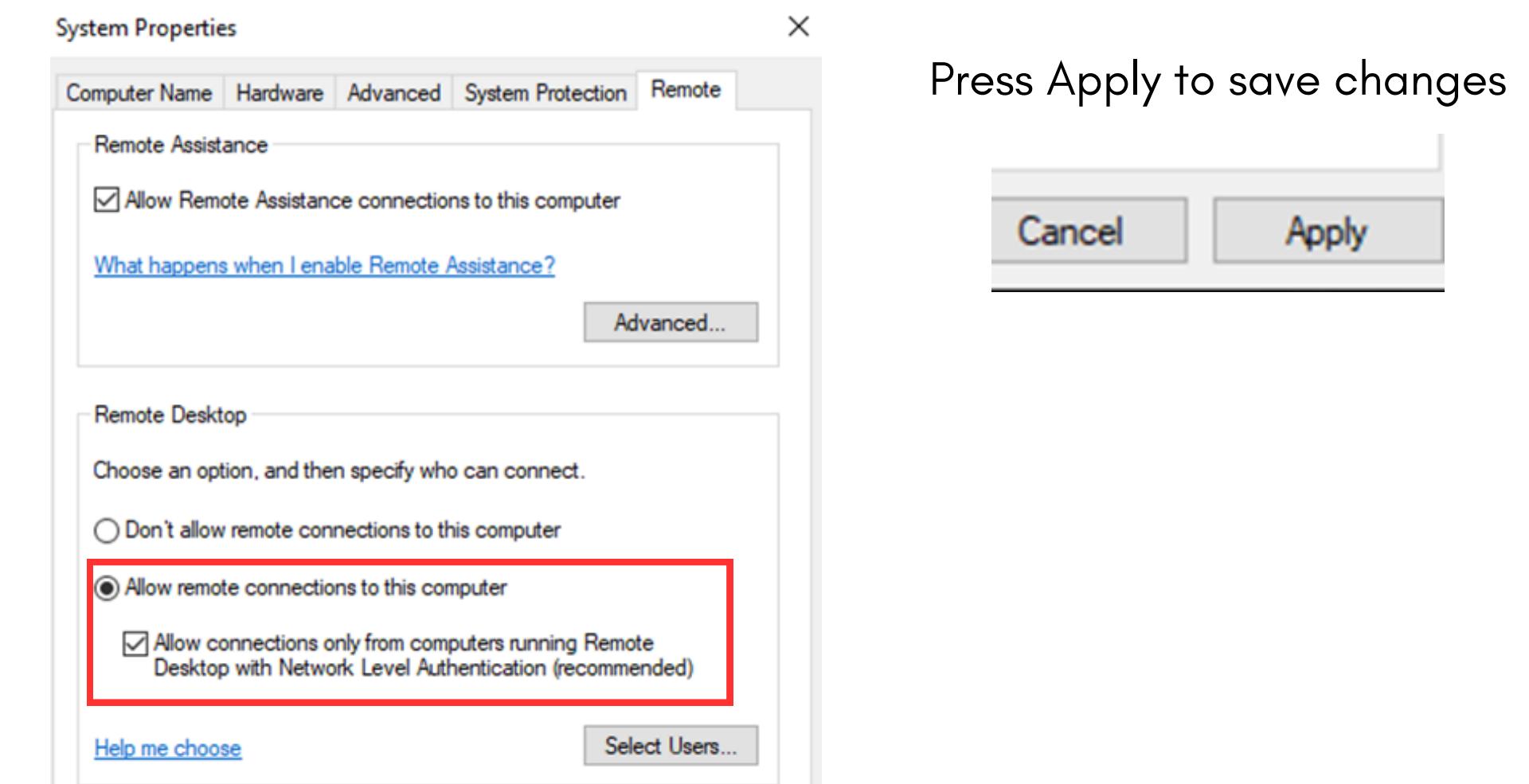
tasks

(34) Network Level Authentication (NLA) for RDP –requires users to authenticate before establishing a remote desktop connection to a Windows machine

1. Open System Properties, Win + R > sysdm.cpl > OK



2. Visit Remote tab > Remote Desktop > Allow remote connections to this computer

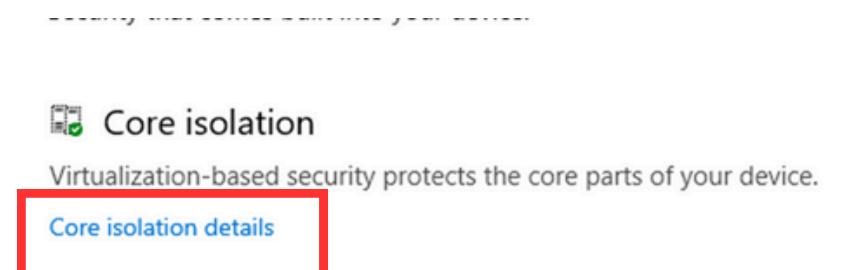
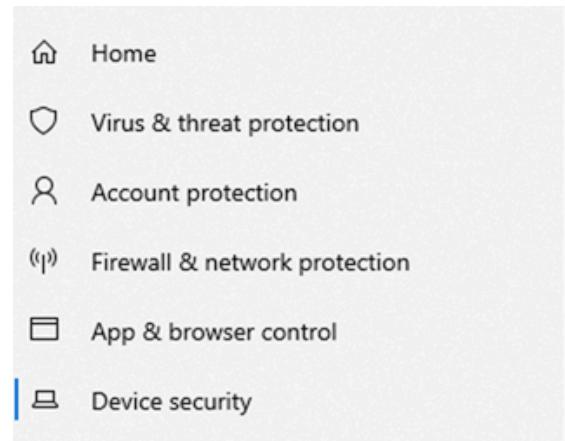


device protection and malware stuff

tasks

(37) Enabling Memory Integrity

1. Windows Security > Device Security > Core Isolation Details



2. Switch on 'Memory integrity' then restart.

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.



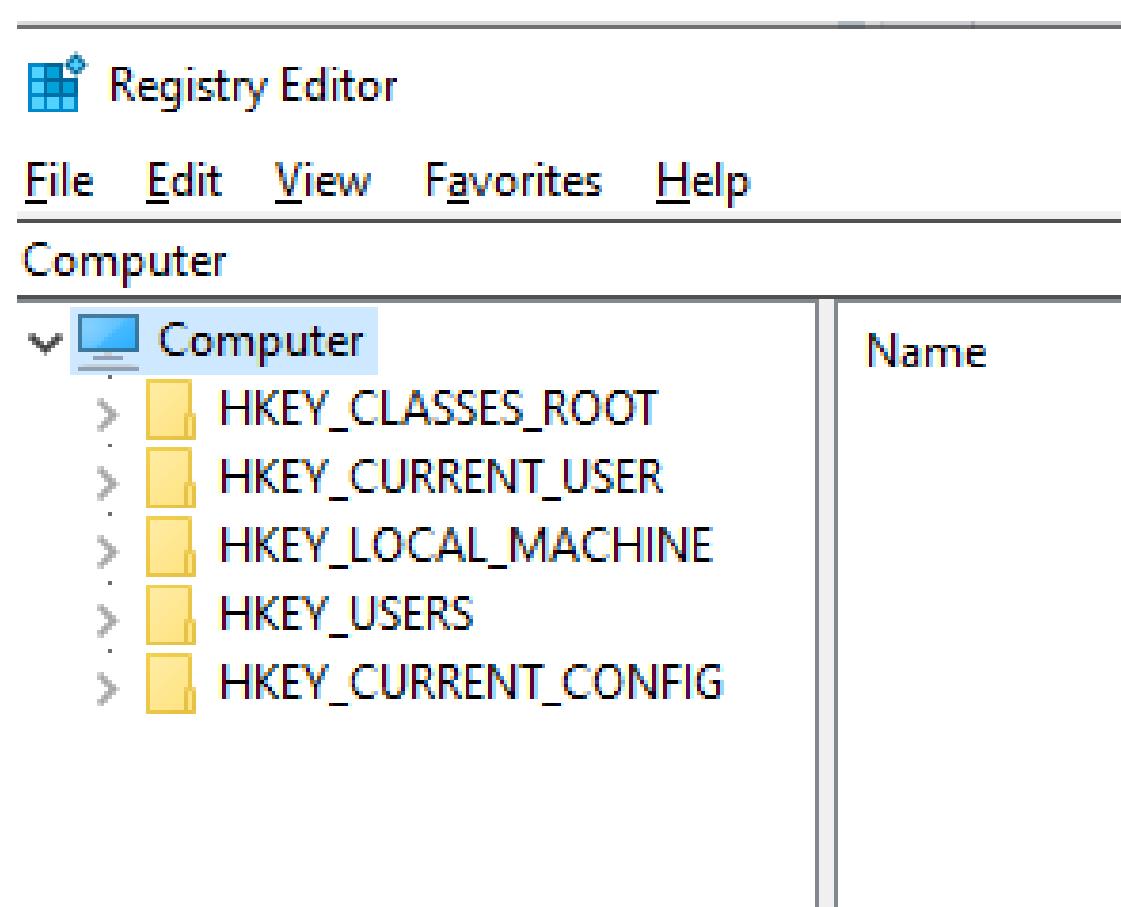
[Learn more](#)

device protection and malware stuff

_tasks

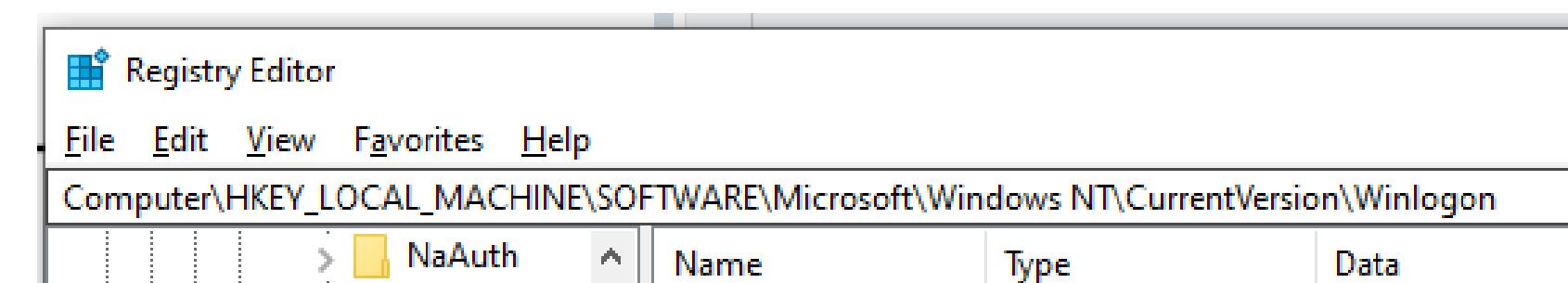
(38) Disabling automatic login

1. Open Registry Editor



2. Navigate to this path:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon



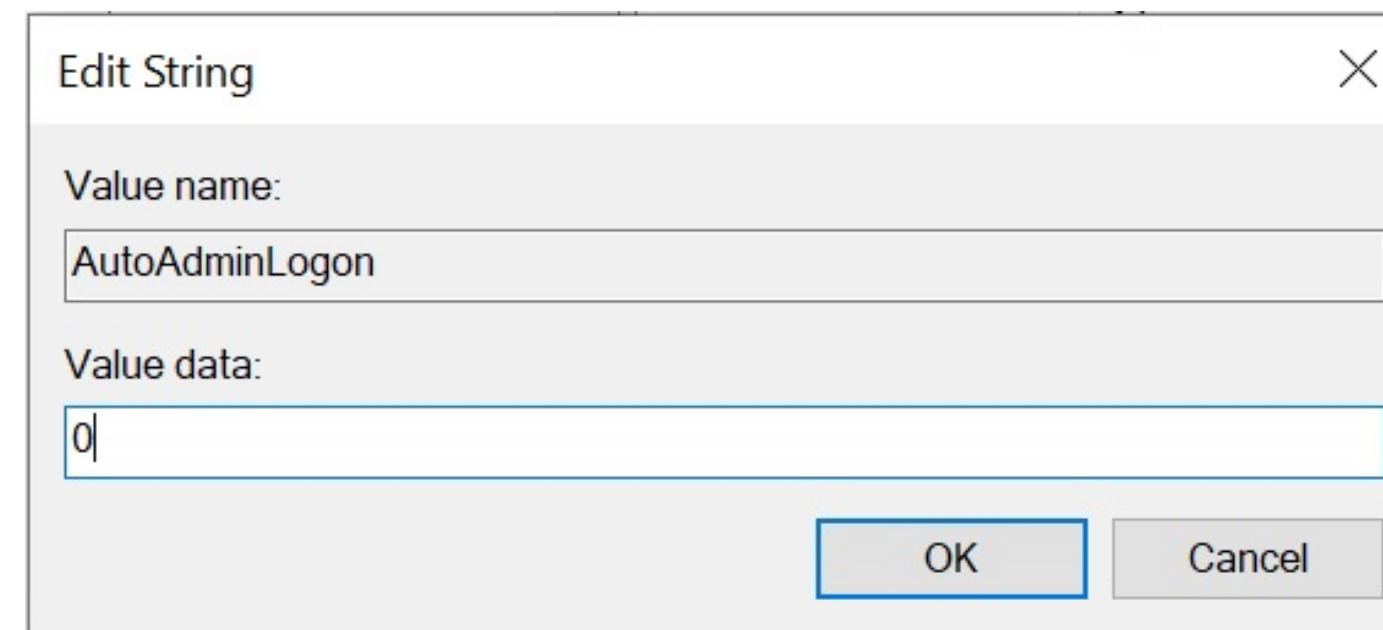
_tasks

(38) Disabling automatic login

3. Double Click on AutoAdminLogon

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon			
	Name	Type	Data
> Terminal Server	ab (Default)	REG_SZ	(value not set)
> TileDataModel	AutoAdminLogon	REG_SZ	1
> Time Zones	AutoLogonSID	REG_SZ	S-1-5-21-14
> TokenBroker			

4. Change the value to 0



device protection and malware stuff

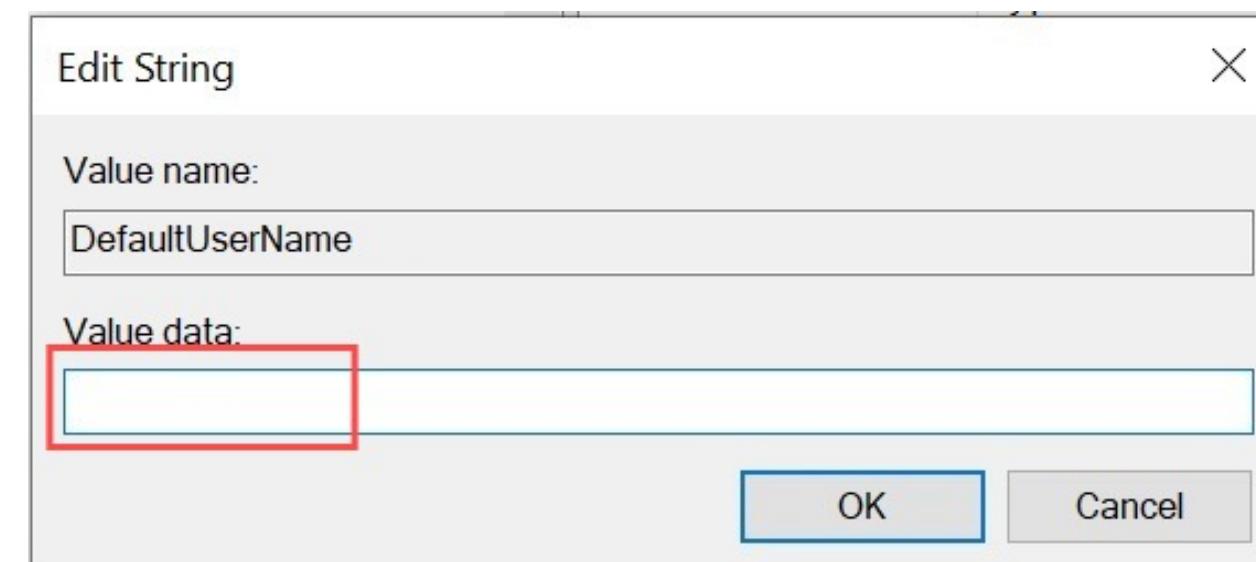
_tasks

(38) Disabling automatic login

5. Double Click on DefaultUserName

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon			
	Name	Type	Data
>	Terminal Server	REG_SZ	(value not set)
>	TileDataModel	REG_SZ	
>	Time Zones	REG_SZ	
>	TokenBroker	REG_SZ	
>	Tracing	REG_SZ	
>	UAC	REG_SZ	
>	Update	REG_SZ	
>	Userinstallable.dri	REG_SZ	
>	VersionsList	REG_SZ	
>	Virtualization	REG_SZ	
>	VolatileNotificatio	REG_SZ	
>	WbemPerf	REG_SZ	
>	WiFiDirectAPI	REG_SZ	
>	Windows	REG_SZ	
>	Winlogon	REG_SZ	
	AlternateShells	REG_SZ	
	AutoLogonChe	REG_SZ	
	GPExtensions	REG_SZ	
	UserDefaults	REG_SZ	
	VolatileUserMc	REG_SZ	
	WinSAT	REG_SZ	
>	DisableBackButton	REG_DWORD	0x00000001 (1)
>	DisableCAD	REG_DWORD	0x00000001 (1)
>	EnableFirstLogon...	REG_DWORD	0x00000001 (1)
>	EnableSIHostInte...	REG_DWORD	0x00000001 (1)
>	ForceUnlockLogon	REG_DWORD	0x00000000 (0)
>	LastLogOffEndTi...	REG_QWORD	0x1ddd77f7 (501053431)
>	LastUsedUserna...	REG_SZ	SIT
>	LegalNoticeCapti...	REG_SZ	
>	LegalNoticeText	REG_SZ	
>	PasswordExpiry...	REG_DWORD	0x00000005 (5)

6. Clear the value data so that it is blank

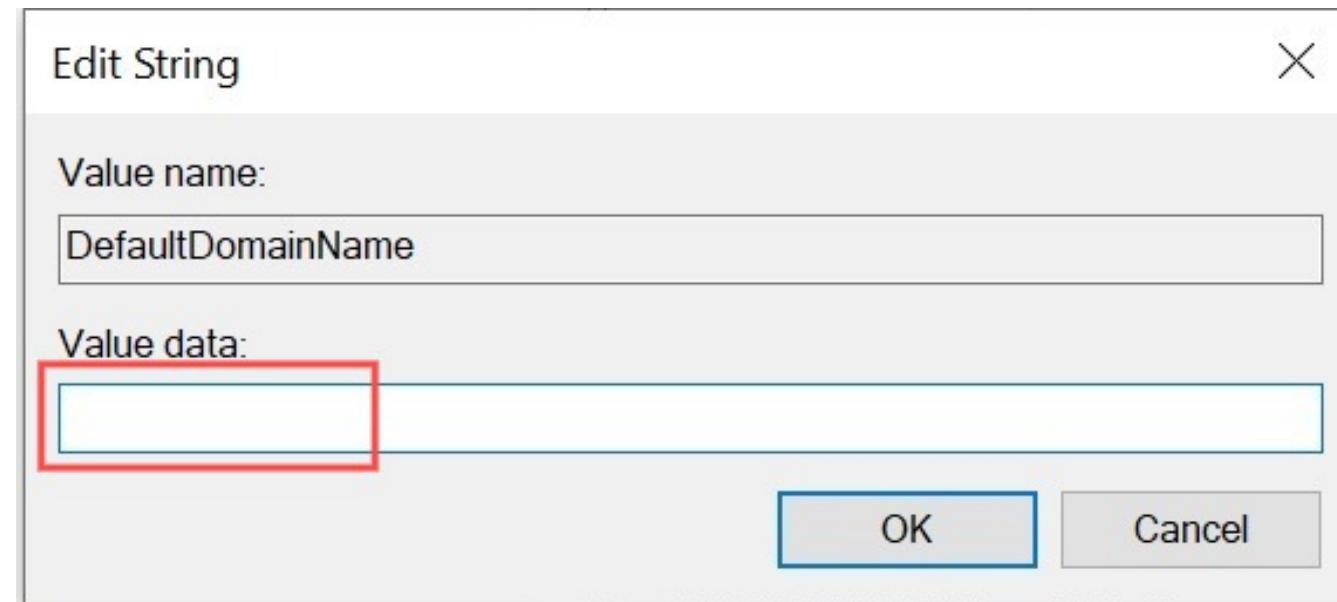


_tasks

(38) Disabling automatic login

7. Repeat steps 5 & 6 on DefaultDomainName

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon			
	Name	Type	Data
>	Terminal Server	REG_SZ	(value not set)
>	TileDataManager	REG_SZ	
>	Time Zones	REG_SZ	
>	TokenBroker	REG_SZ	
>	Tracing	REG_SZ	
>	UAC	REG_SZ	
>	Update	REG_SZ	
>	Userinstallable.driv...	REG_SZ	
>	VersionsList	REG_SZ	
>	Virtualization	REG_SZ	
>	VolatileNotificatio...	REG_SZ	
>	WbemPerf	REG_SZ	
>	WiFiDirectAPI	REG_SZ	
>	Windows	REG_SZ	
>	Winlogon	REG_SZ	
	AlternateShells	REG_SZ	
	AutoLogonCh...	REG_SZ	
	GPExtensions	REG_SZ	
	UserDefault...	REG_SZ	
	VolatileUserM...	REG_SZ	
	WinSAT	REG_SZ	
>	Name	REG_SZ	(value not set)
>	(Default)	REG_SZ	
>	AutoAdminLogon	REG_SZ	1
>	AutoLogonSID	REG_SZ	S-1-5-21-14237642-115767227
>	AutoRestartShell	REG_DWORD	0x00000001 (1)
>	Background	REG_SZ	0 0 0
>	CachedLogonsC...	REG_SZ	10
>	DebugServerCo...	REG_SZ	no
>	DefaultDomainN...	REG_SZ	
>	DefaultUserName	REG_SZ	SIT
>	DisableBackButton	REG_DWORD	0x00000001 (1)
>	DisableCAD	REG_DWORD	0x00000001 (1)
>	EnableFirstLogon...	REG_DWORD	0x00000001 (1)
>	EnableSIHostInte...	REG_DWORD	0x00000001 (1)
>	ForceUnlockLogon	REG_DWORD	0x00000000 (0)
>	LastLogOffEndTi...	REG_QWORD	0x1ddd77f7 (501053431)
>	LastUsedUserna...	REG_SZ	SIT
>	LegalNoticeCapti...	REG_SZ	
>	LegalNoticeText	REG_SZ	
>	PasswordExpiry...	REG_DWORD	0x00000005 (5)



_conclusion



A summary of what we've done.

conclusion

The following generally summarises what was done:

- **Secured Access:** Strengthened account security and passwords.
- **Network Safety:** Blocked insecure ports and applied firewall rules.
- **System Protection:** Enabled Secure Boot, BitLocker, and auto-updates.
- **Controlled Apps:** Restricted unapproved software to prevent malware.
- **Data Recovery:** Set up backups and restore points.

_echo thank you