_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

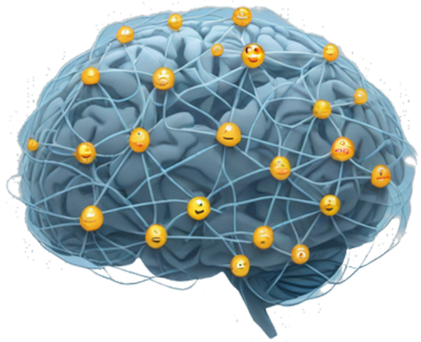
Kriston

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@s-4meP7A0u6oPh1
Password for Windows	Th1s1sMYp@ssw0rd$

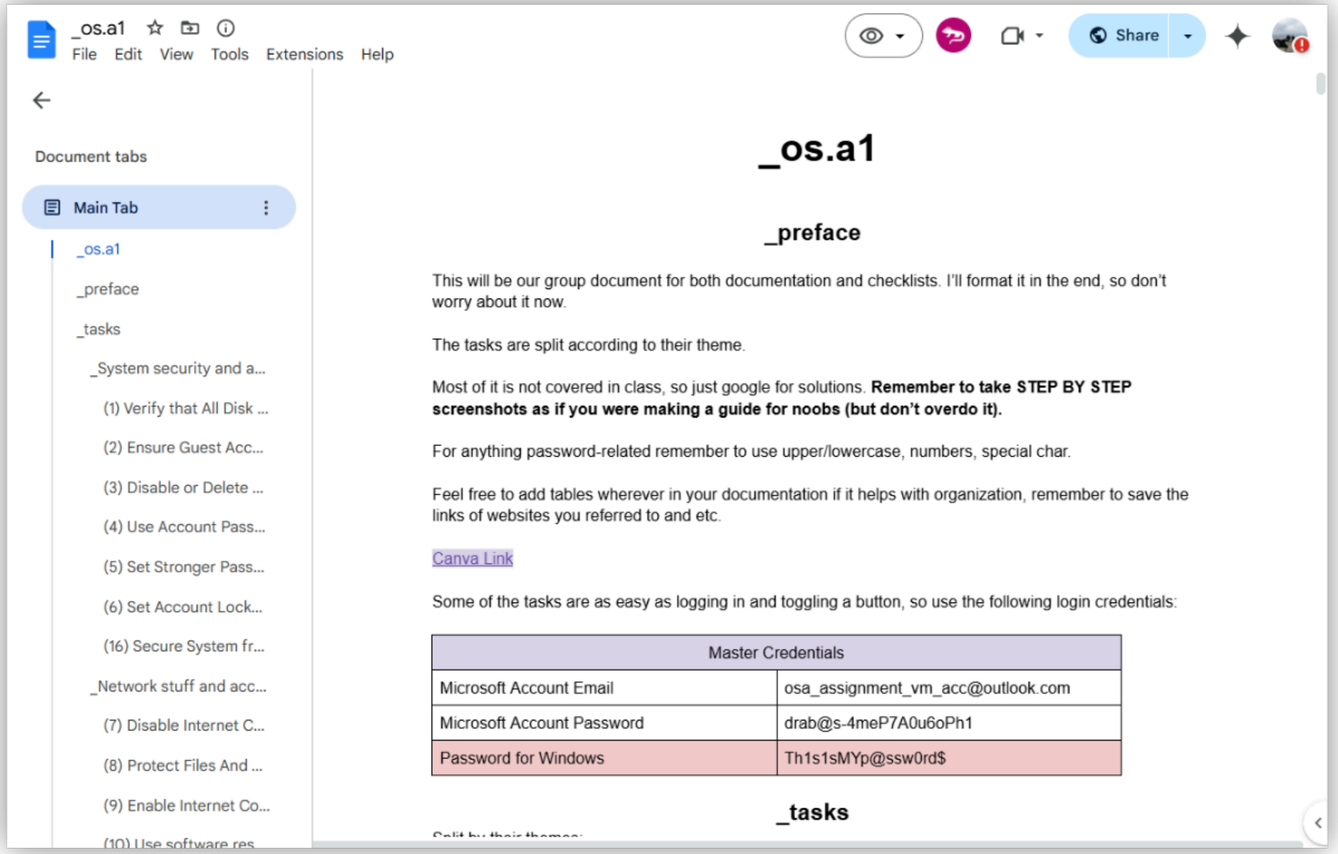
_preface: *documentation*

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 documentaion.

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

Acssesible here: _os.a1



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

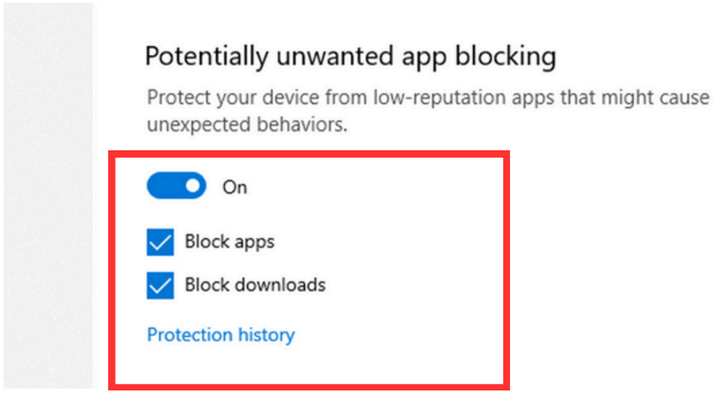
} additional tasks

_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.



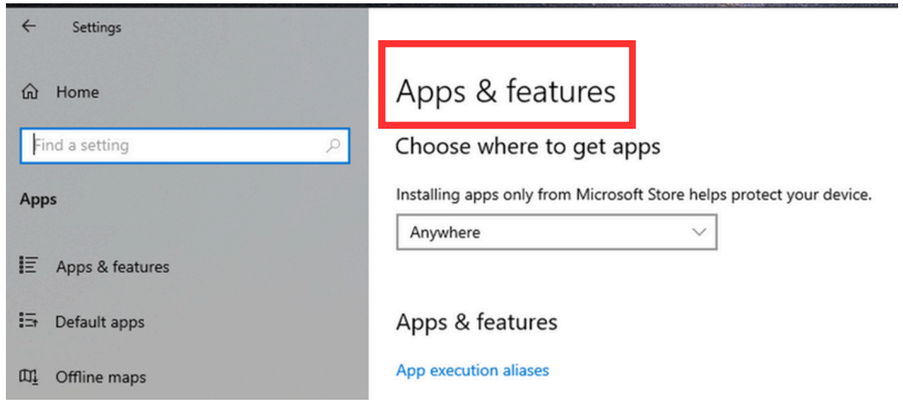
This protects your device from unexpected behaviors caused by low-reputation apps.

protection and backups

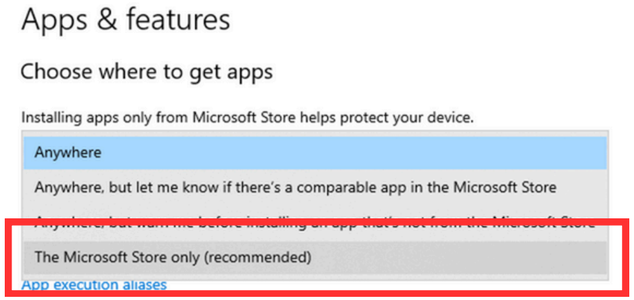
_tasks

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

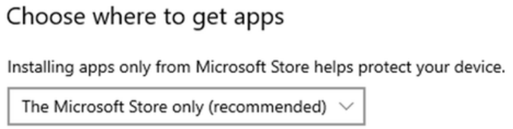
2. Visit Settings > Apps > Apps & features



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.

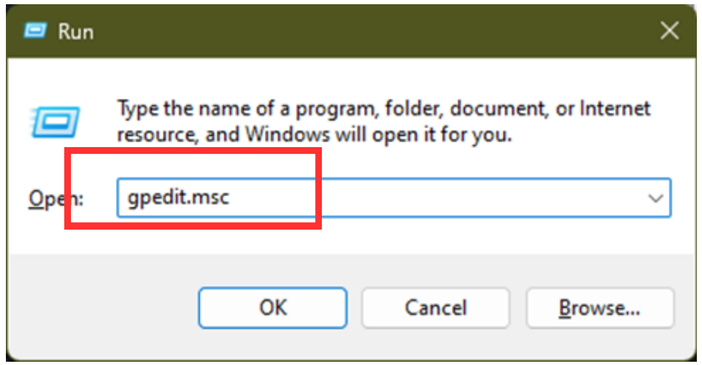


protection and backups

_tasks

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

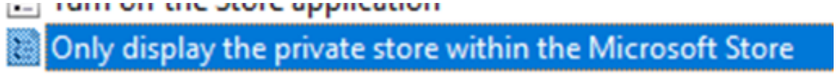
3. Restrict App Sources Using Group Policy



Win + R > gpedit.msc > OK

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

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.

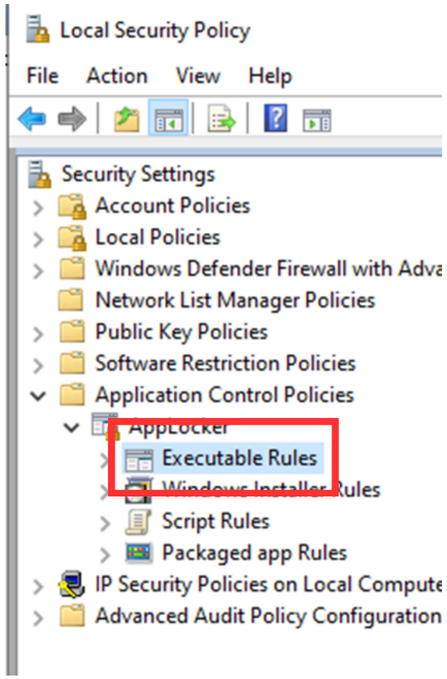
protection and backups

_tasks

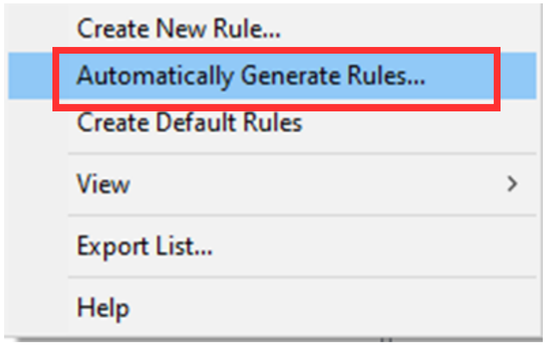
(18) App Management - Only allow the installation of approved applications from controlled software repositories or application marketplaces

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.

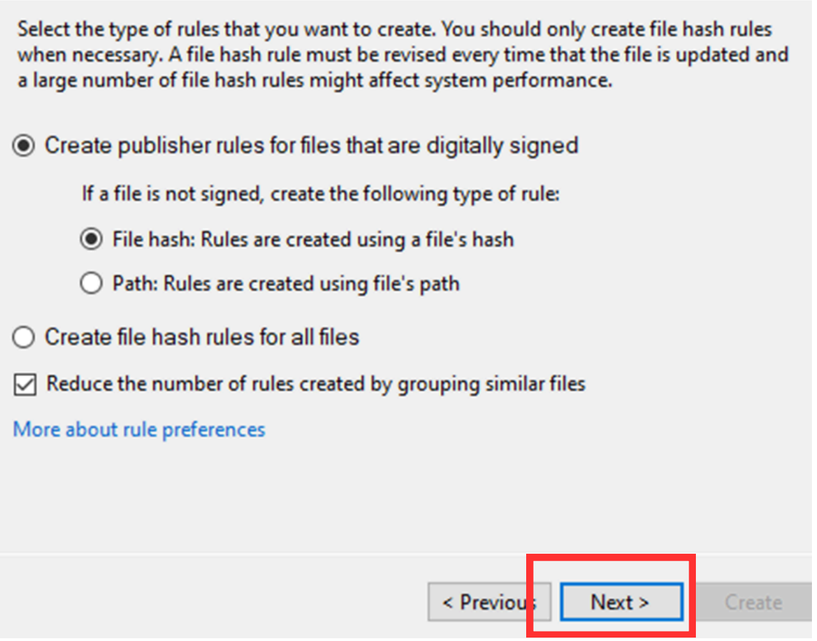


protection and backups

_tasks

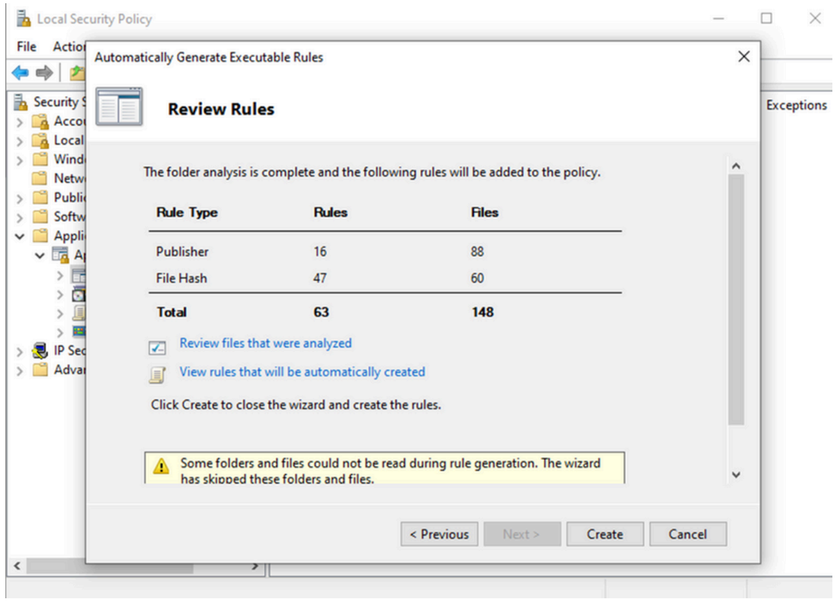
(18) App Management - Only allow the installation of approved applications from controlled software repositories or application marketplaces

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.

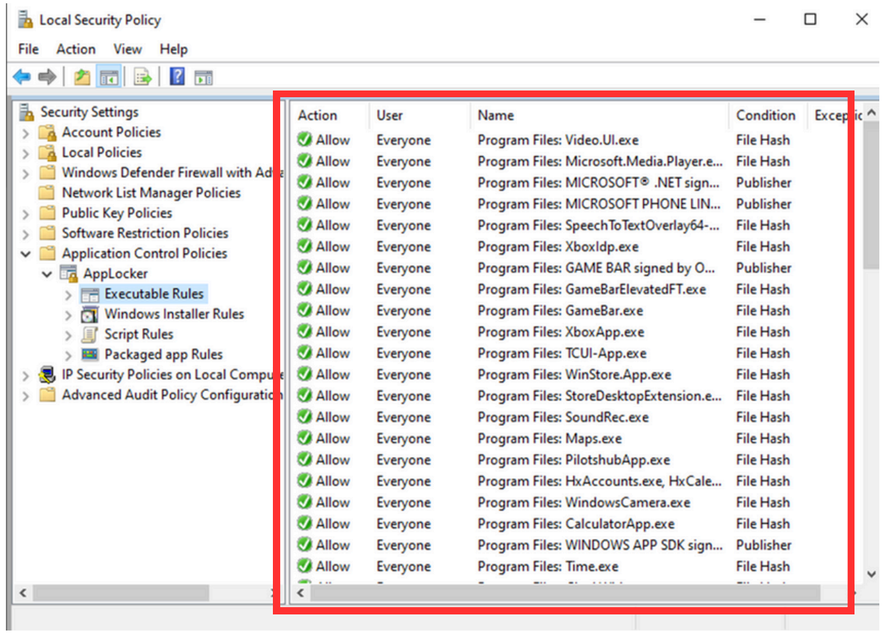


Edit as per your specific needs, etc.

_tasks

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

4. Confirmation of our Executable Rules.

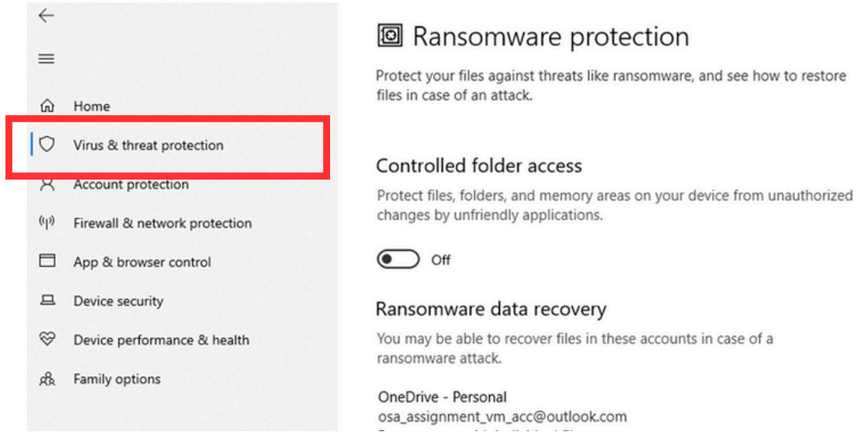


protection and backups

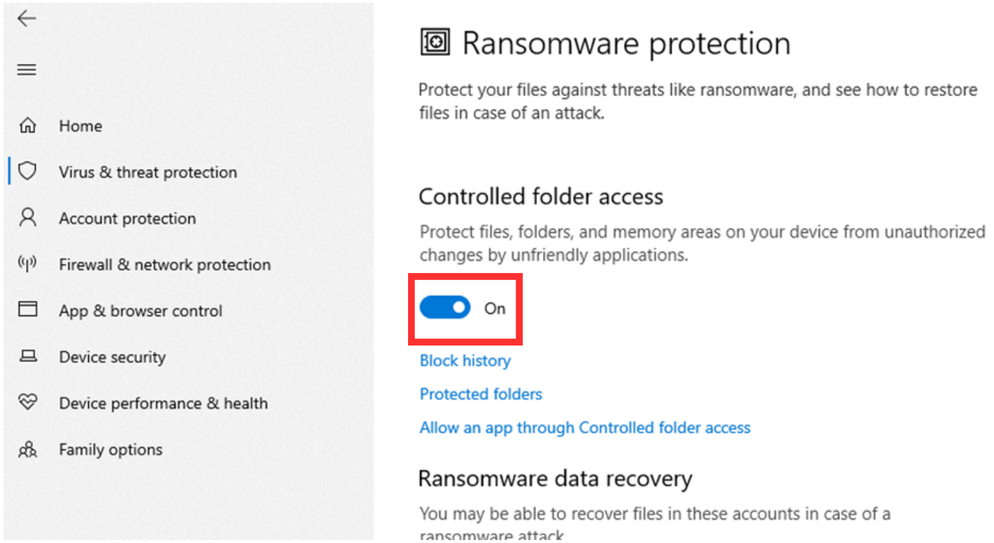
_tasks

(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.



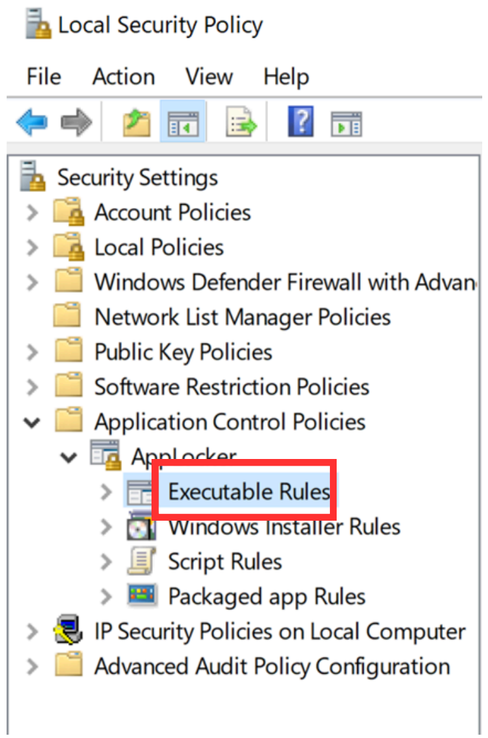
protection and backups

_tasks

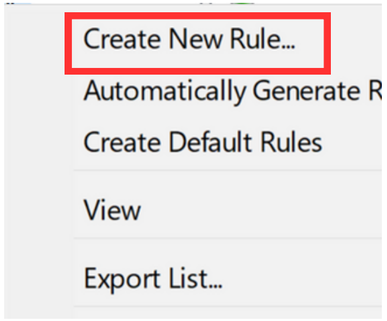
(19) Application Control - Whitelisting and blacklisting of executables or apps

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

Application Control Policies > AppLocker > Right-click Executable Rules



Create New Rule...



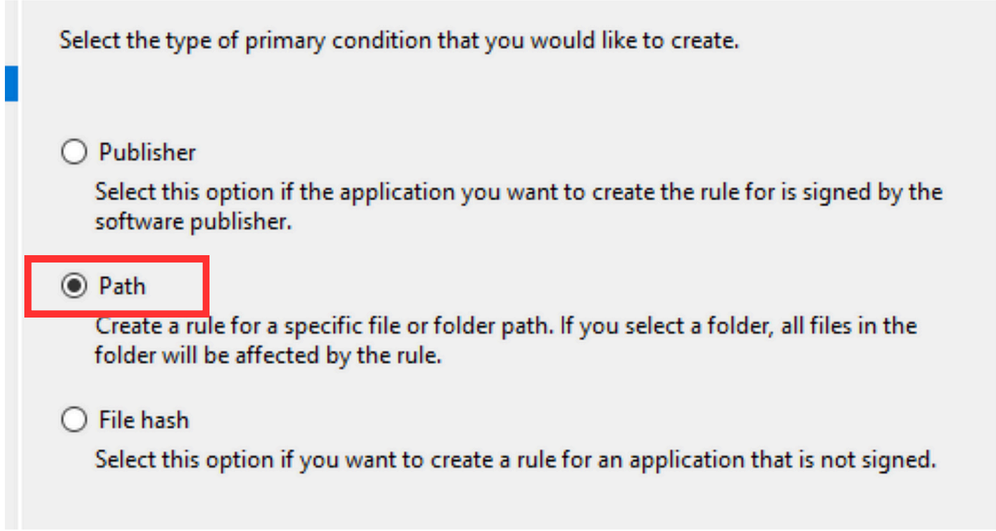
Choose Allow as the action and specify everyone > Next.

protection and backups

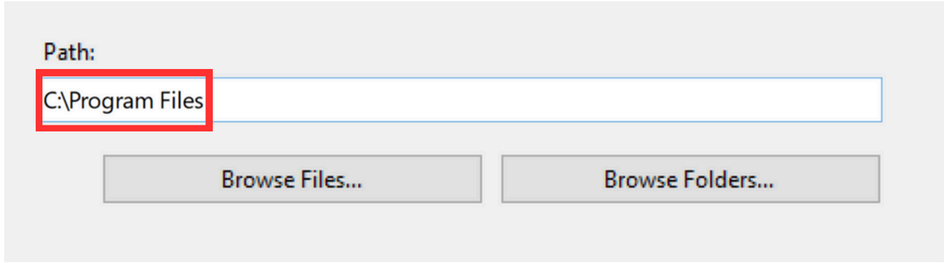
_tasks

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

3. Choose to specify the Path > Next.



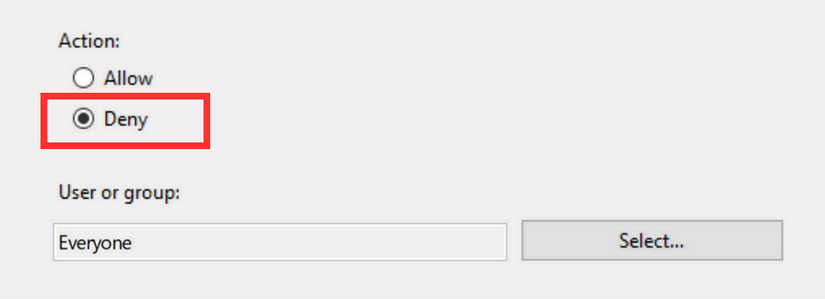
Specify the following > Create:



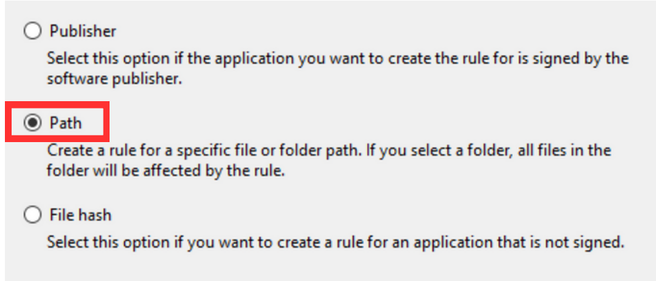
_tasks

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

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

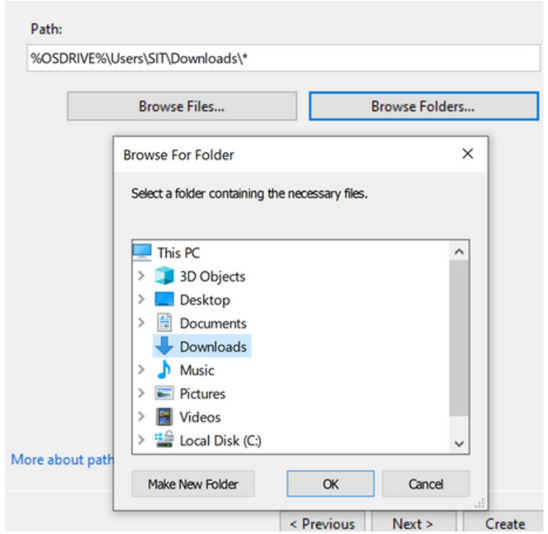


Select Path.

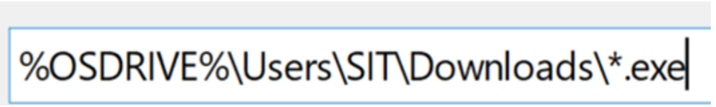


protection and backups

Browse Path > select the Downloads folder > OK.



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



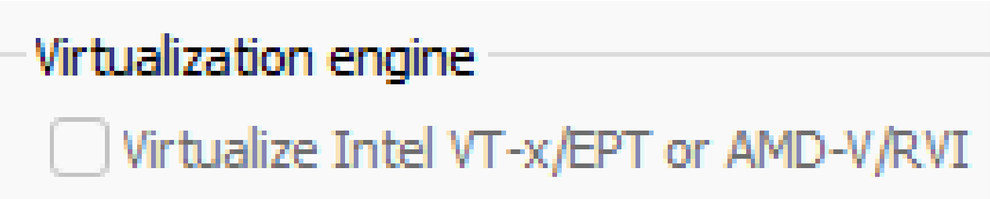
Next > Complete the Wizard

_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

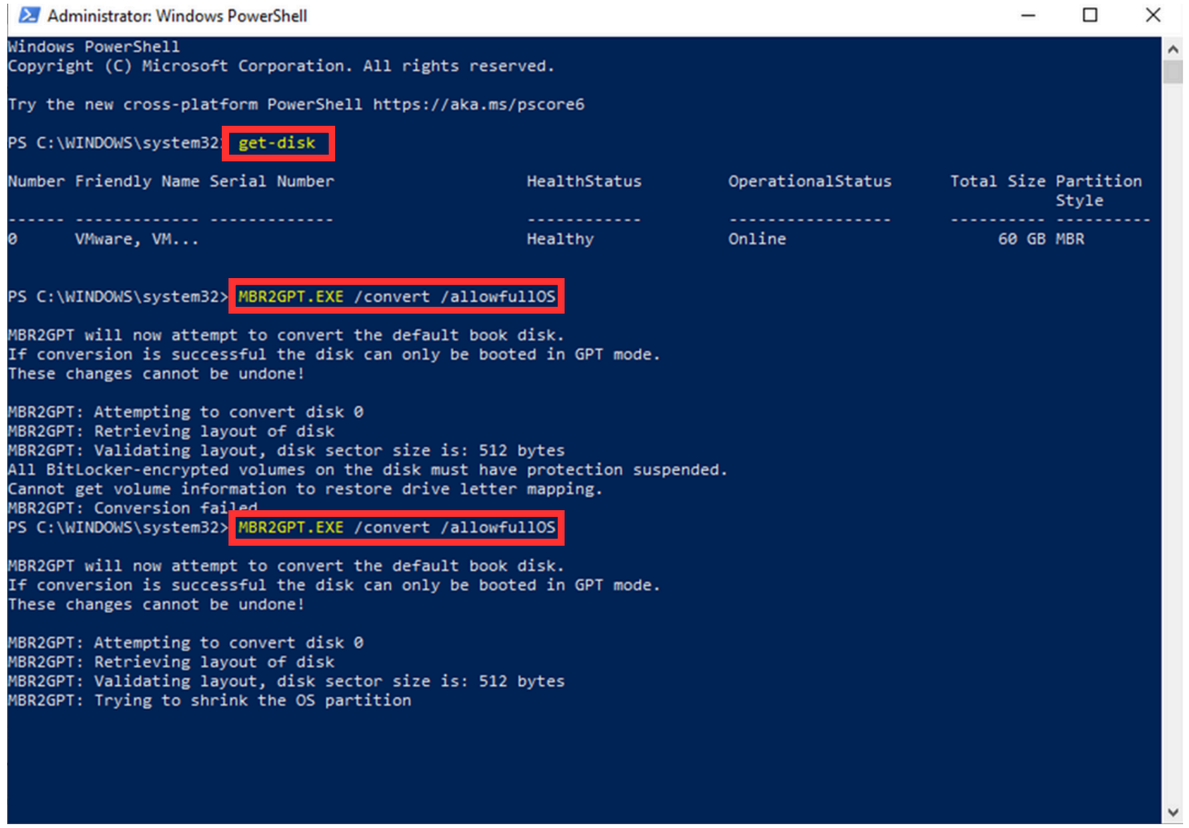
1. Launch Powershell as Administrator

> 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.)

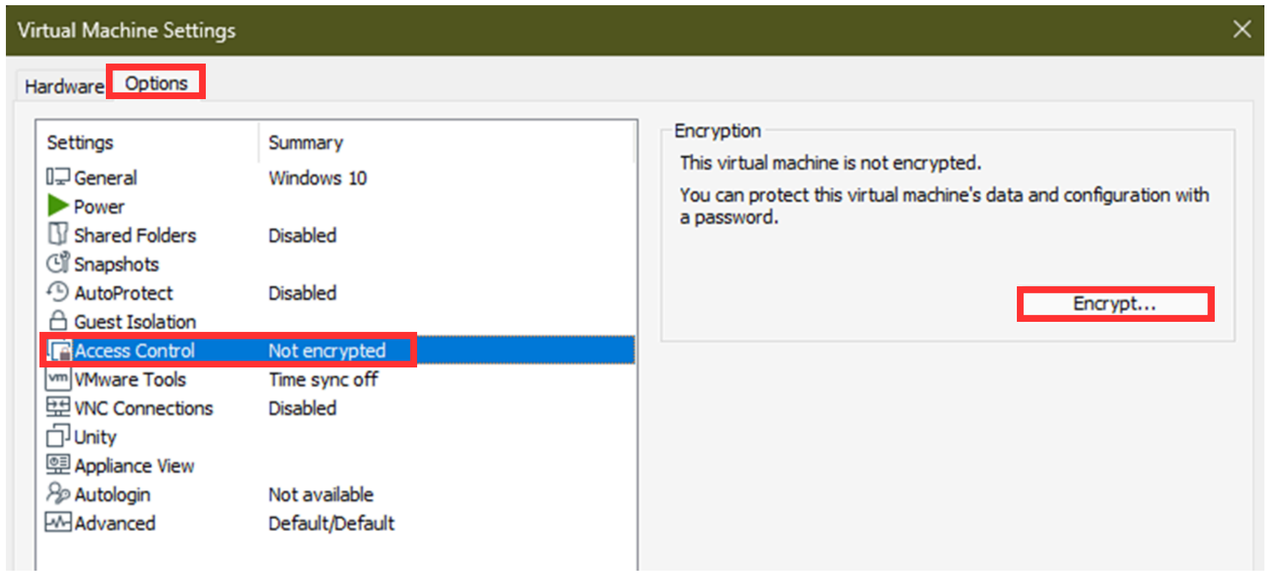
> Power down the VM after.



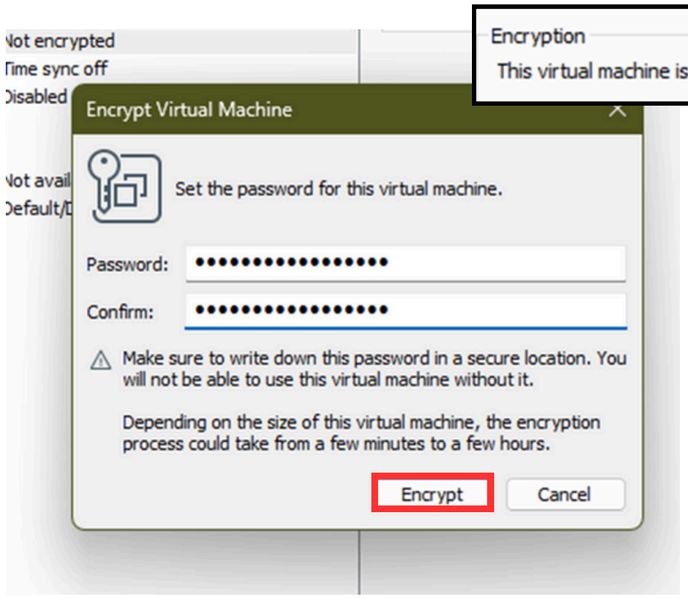
_tasks

(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



Confirmation

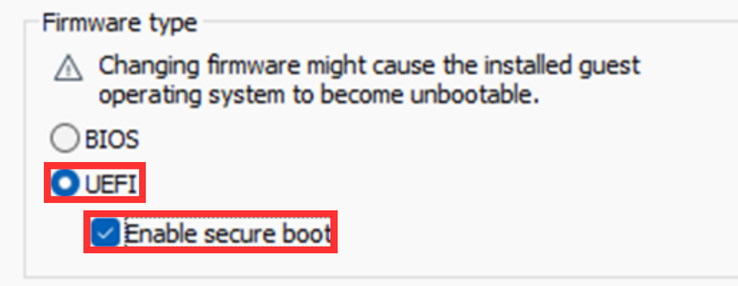


protection and backups

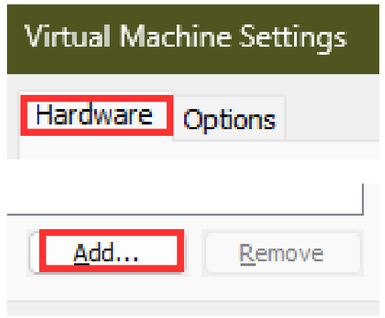
_tasks

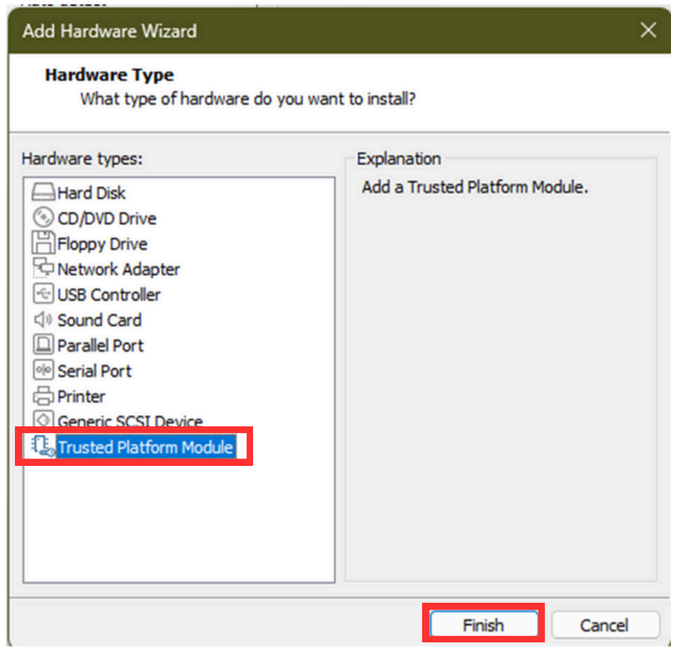
(24) Enable Windows Secure Boot

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



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





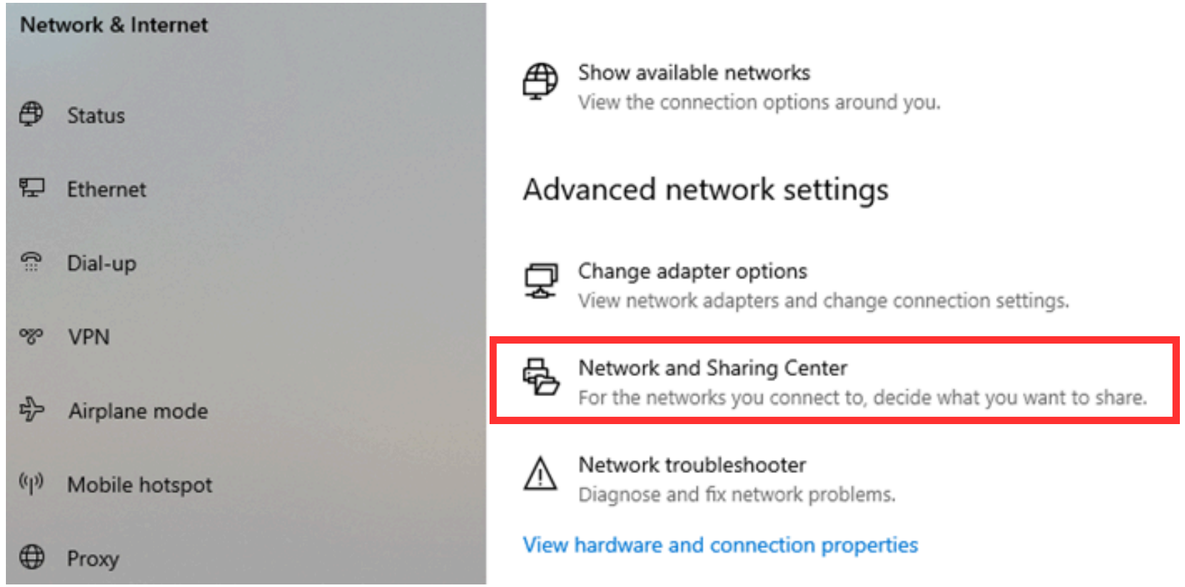
You will now be able to boot with UEFI + Secure Boot + have a TPM (more security).

protection and backups

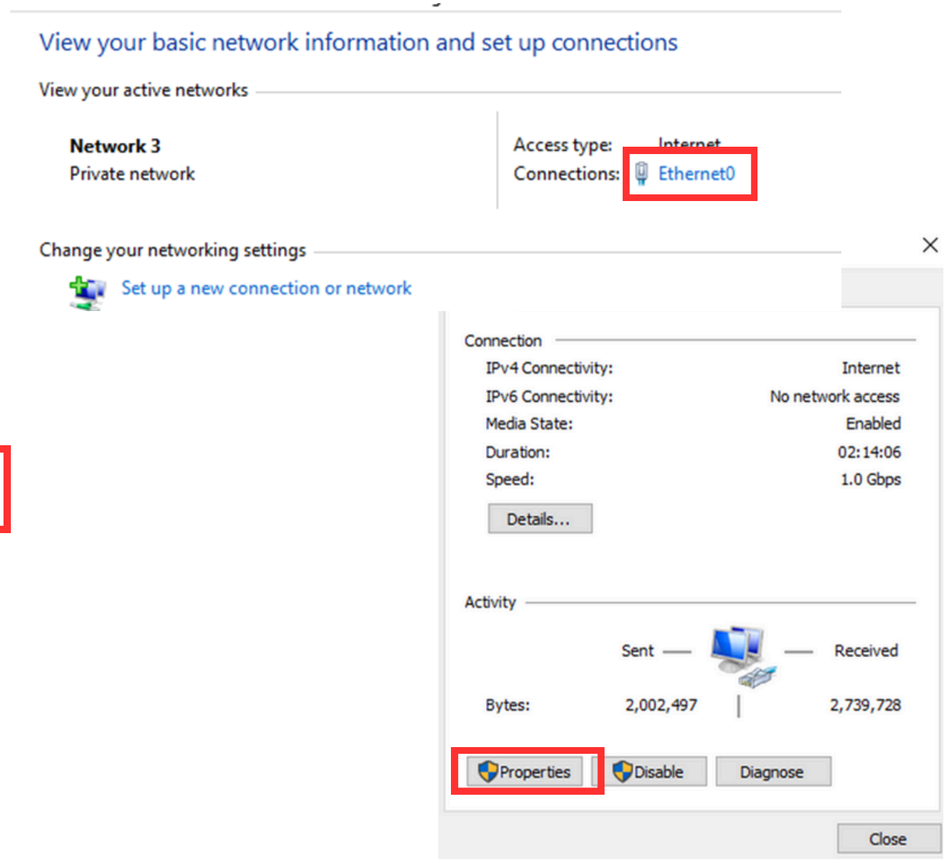
_tasks

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

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



2. Click on your network (Ethernet0) > Properties

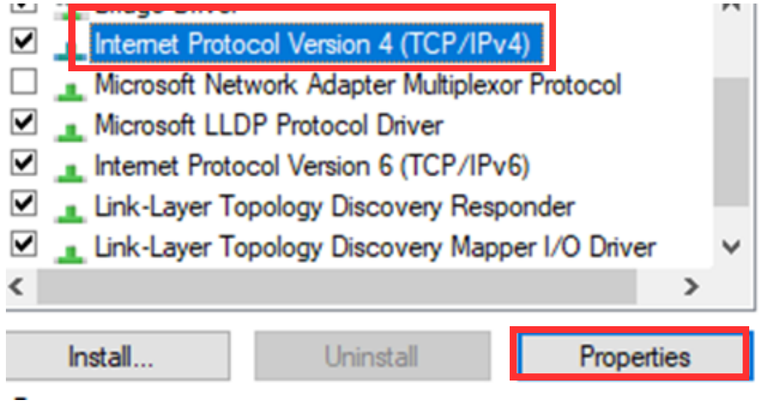


protection and backups

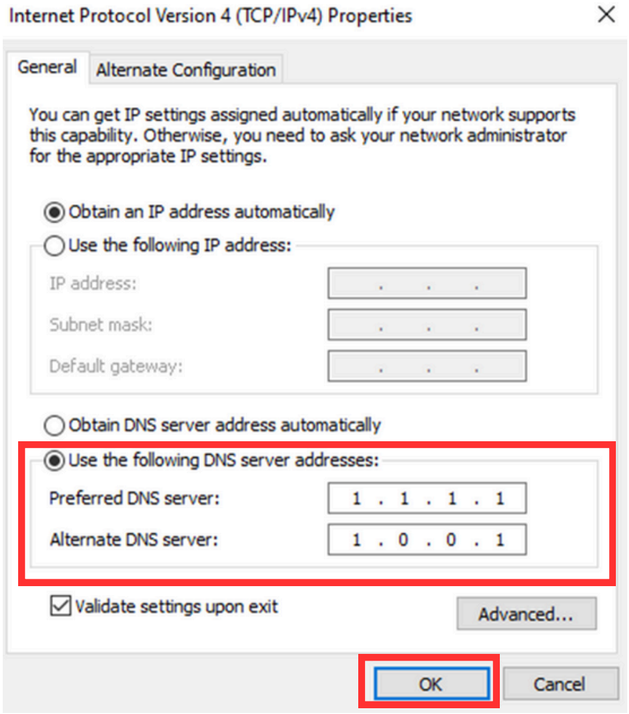
_tasks

(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

base tasks

(30) Create groups for easier account management
    (a) Group Creation
    (b) Adding Members
(31) Implementing Role-Based Access control

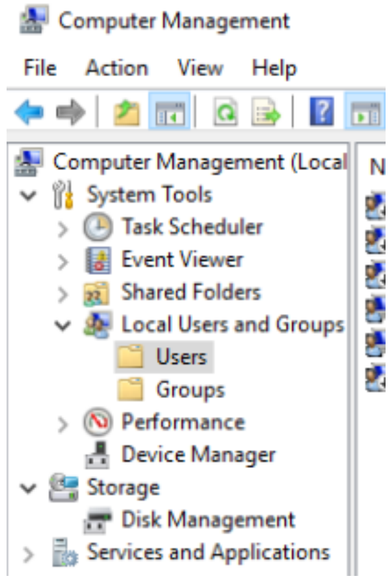
additional tasks

system security and account management

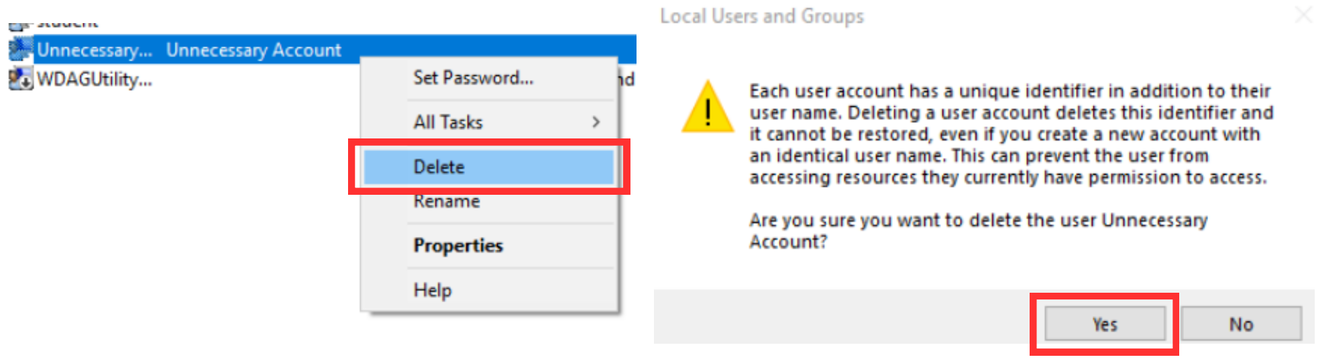
_tasks

(3) Disable or Delete any unnecessary accounts

1. In Computer Management, navigate to “Users”.
Path: System Tools → Local Users and Groups → Users



2. Right-click on any unnecessary accounts and click delete (Click Yes to any prompt on deletion)

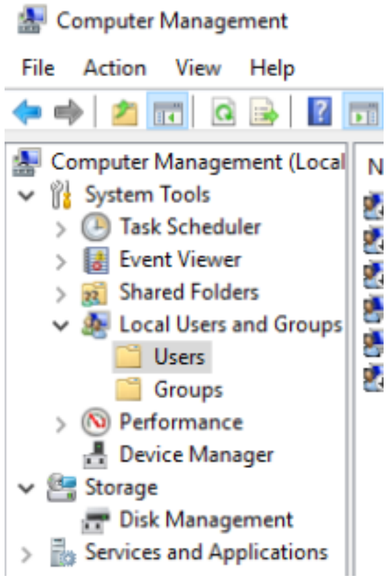


system security and account management

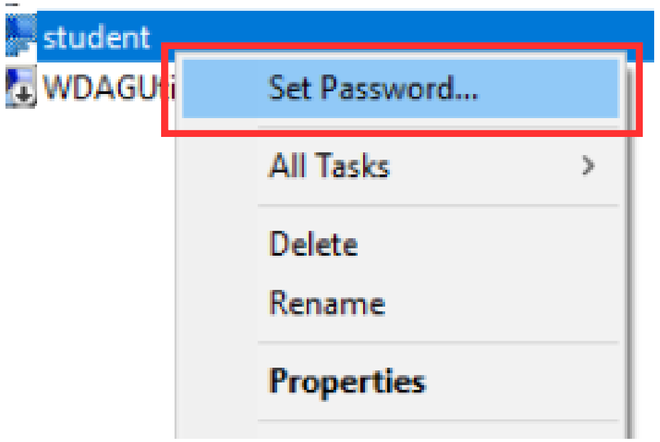
_tasks

(4) Use Account Password

1. In Computer Management, navigate to “Users”.
Path: System Tools → Local Users and Groups → Users



2. Right click on an account that you want to set a password for and click “Set password

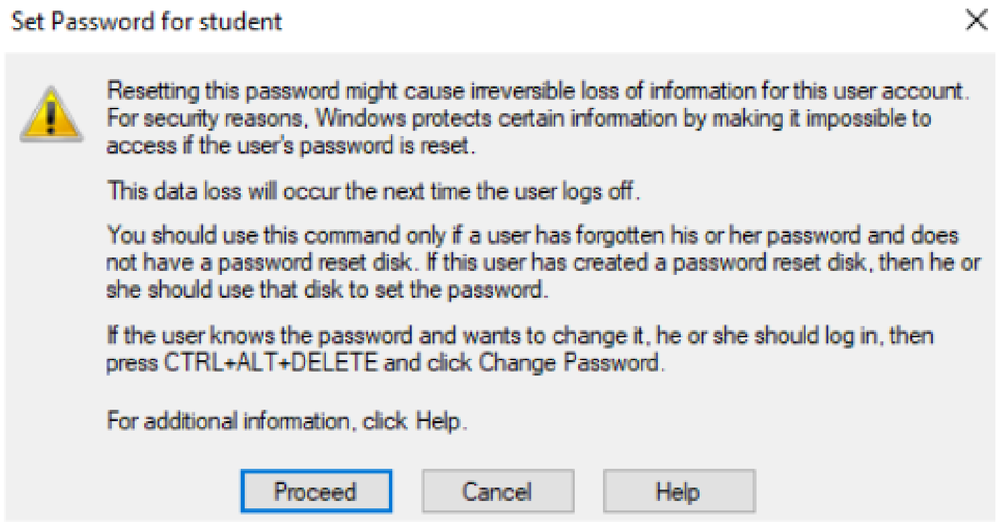


system security and account management

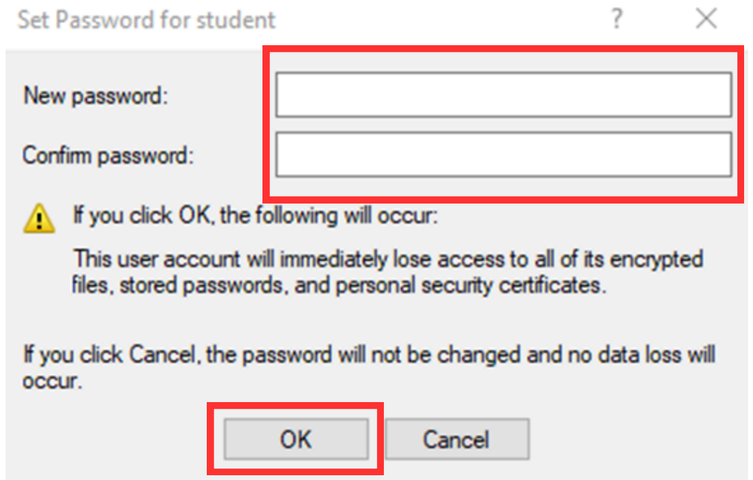
_tasks

(4) Use Account Password

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



Click OK once the password is set

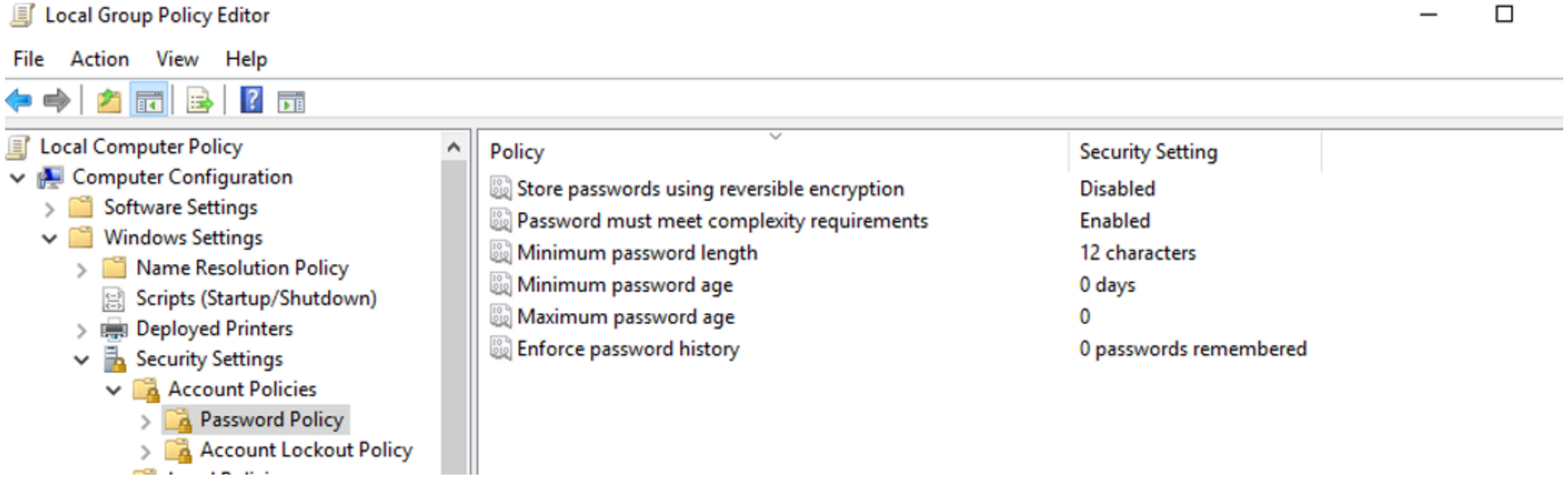


system security and account management

_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

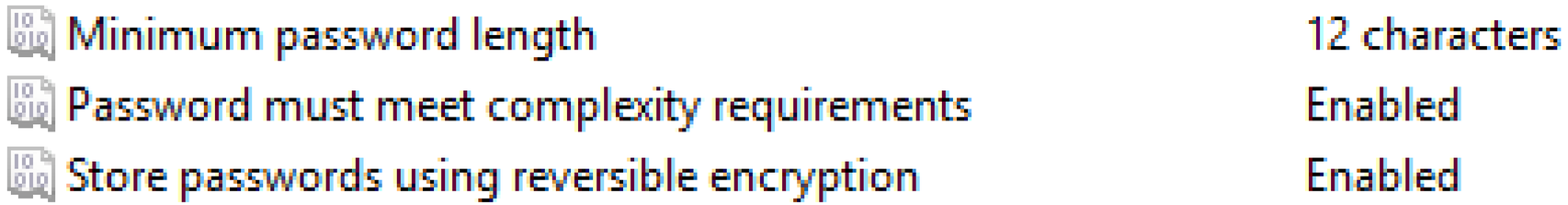


system security and account management

_tasks

(5) Set Stronger Password Policies

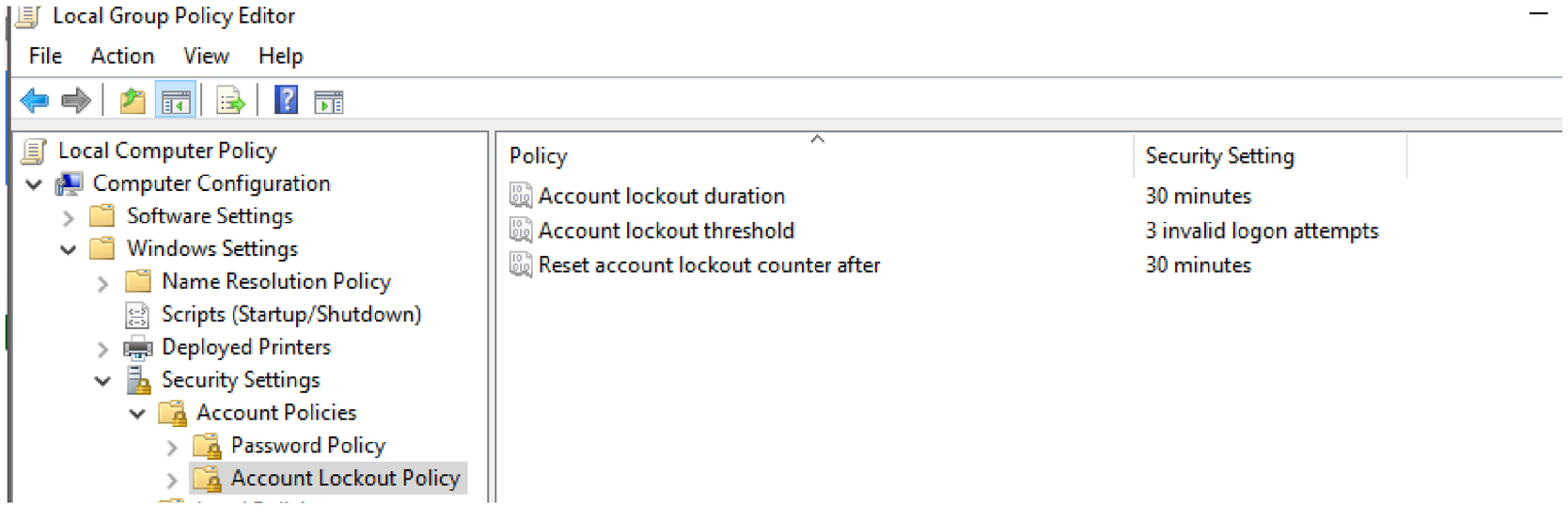
3. Set minimum password length to 12,
   Set “Password must meet complexity requirements” to enabled,
   Set “Store passwords using reversible encryption” to enabled
   Click Apply in the window that pops up in after a change



_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

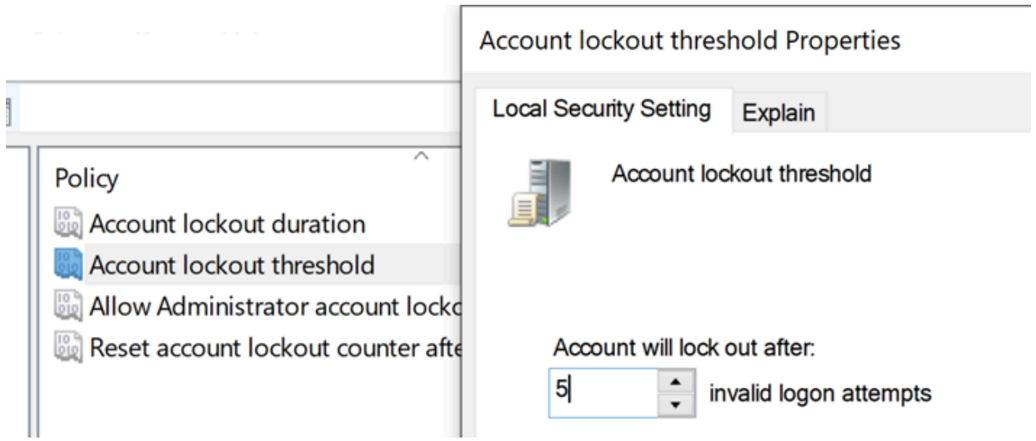


system security and account management

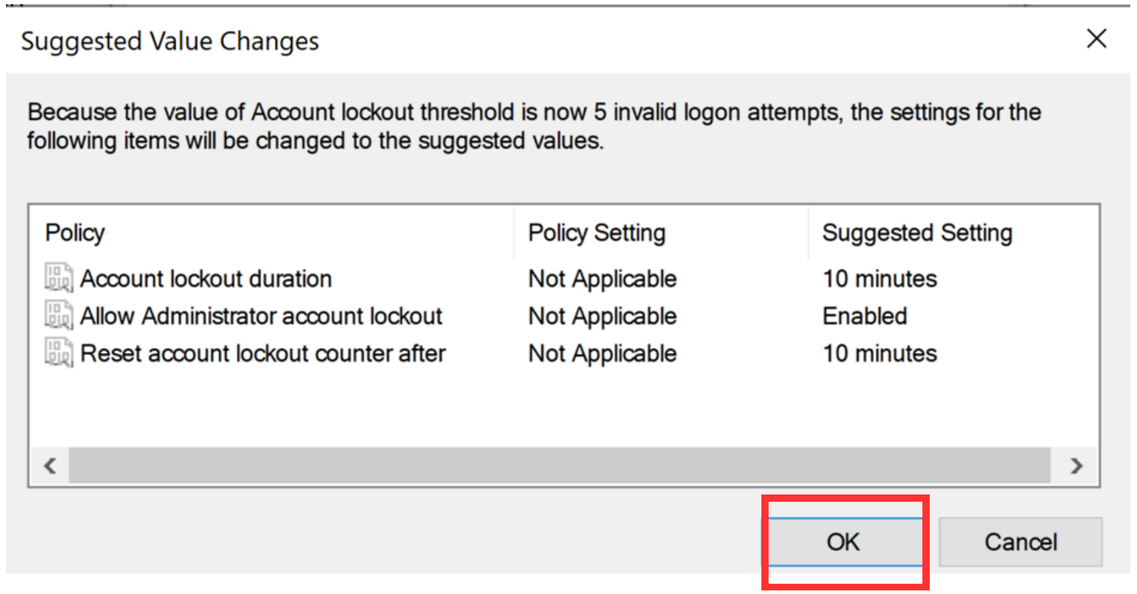
_tasks

(6) Set Stronger Password Policies

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



Click OK to the prompt that pops up.

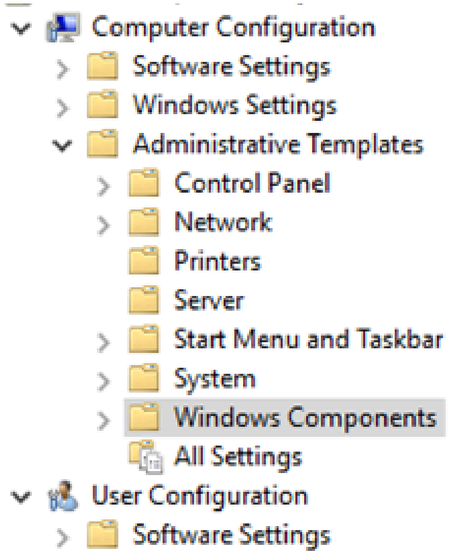


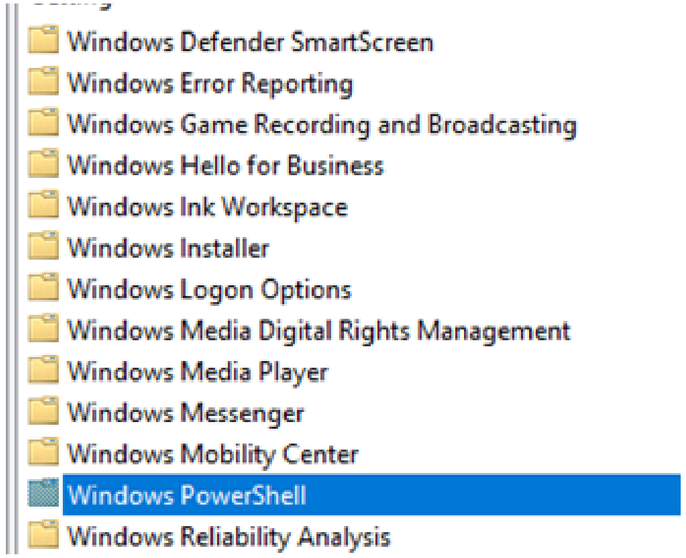
system security and account management

_tasks

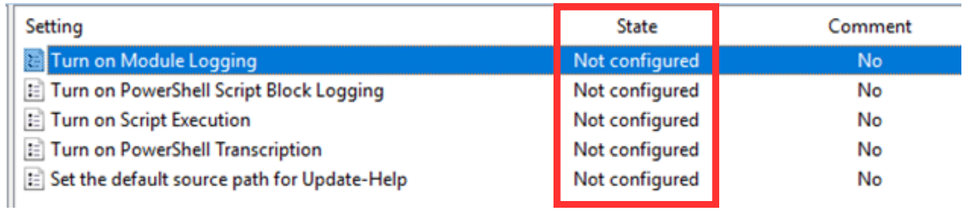
(16) Secure System from PowerShell Exploits

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

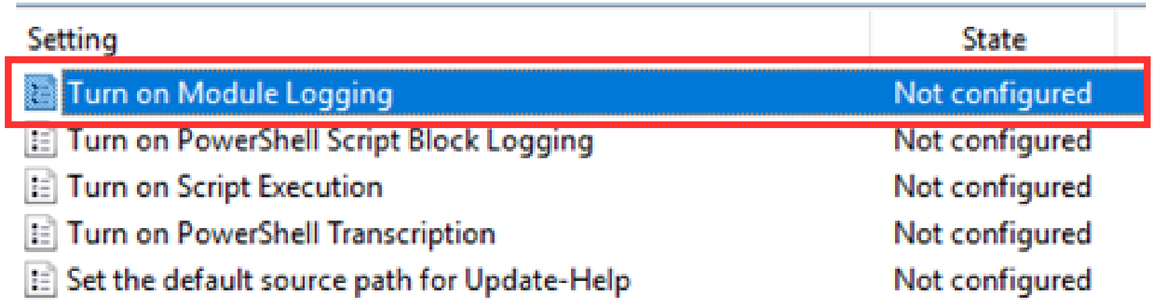
This means PowerShell exploits can run and not be detected

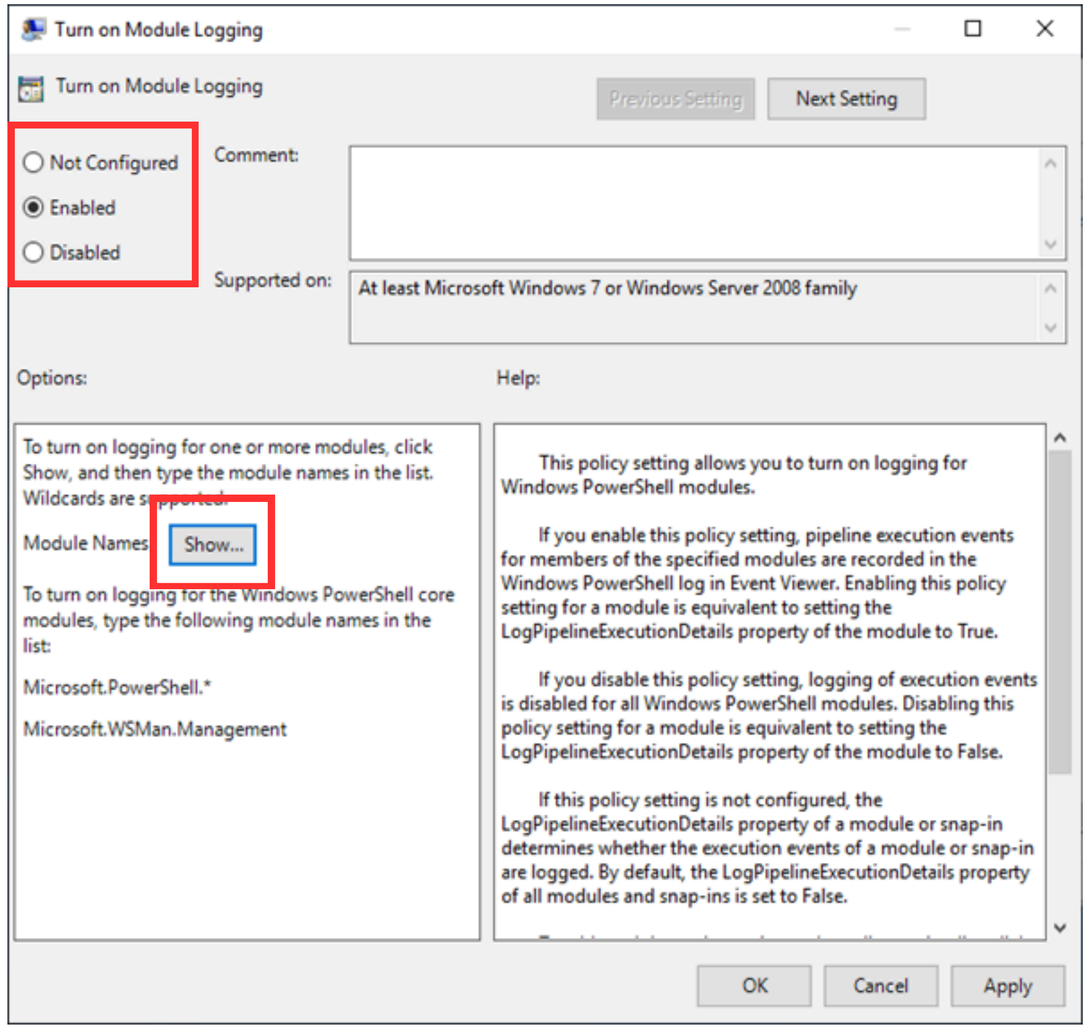
system security and account management

_tasks

(16) Secure System from PowerShell Exploits

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



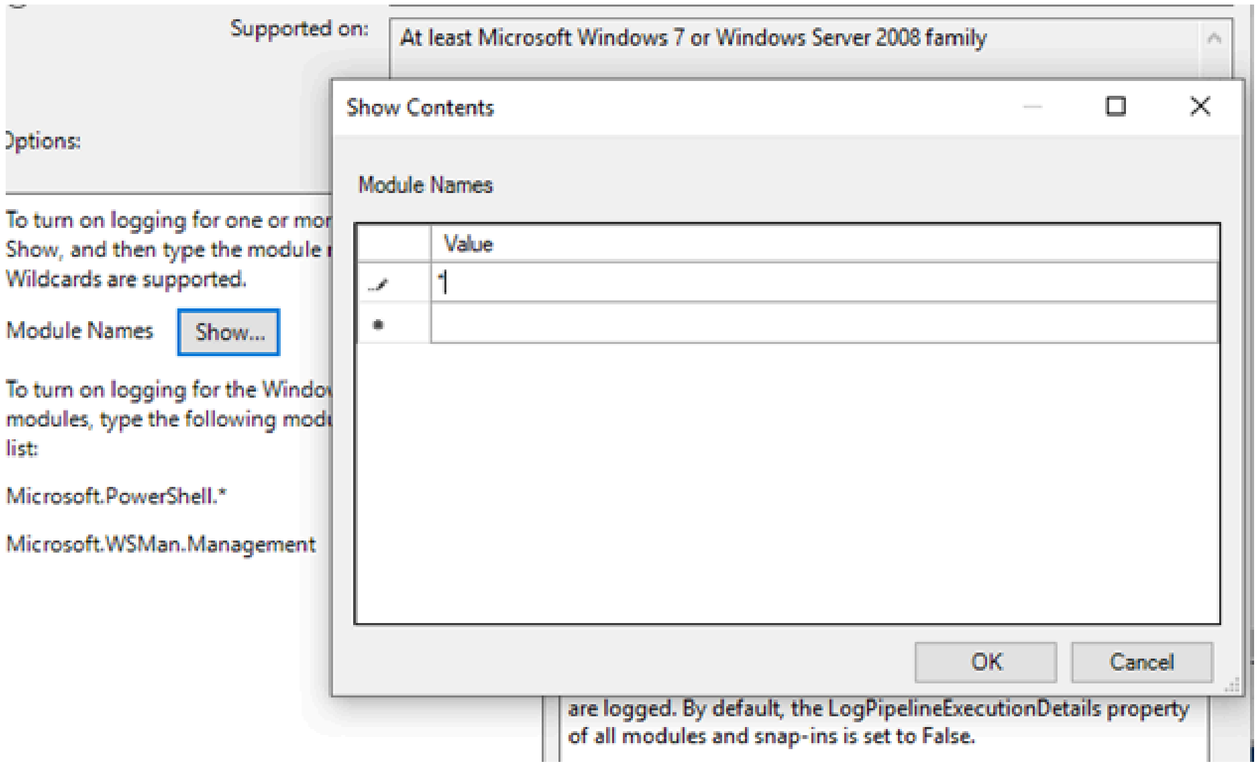


_tasks

(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

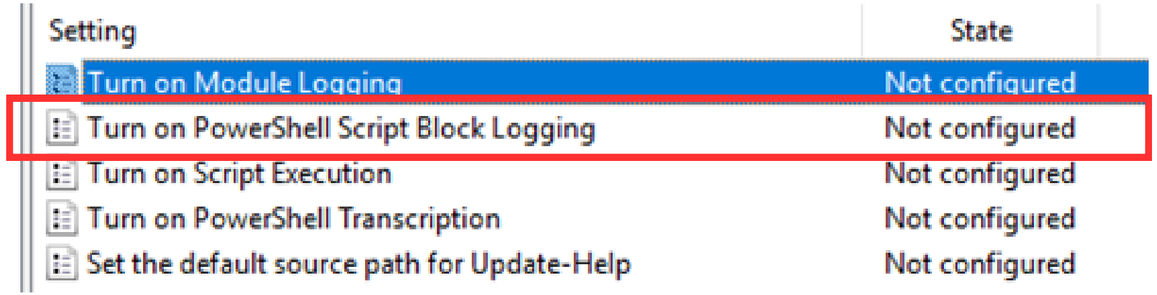
This will cause the computer to log all the scripts that are run



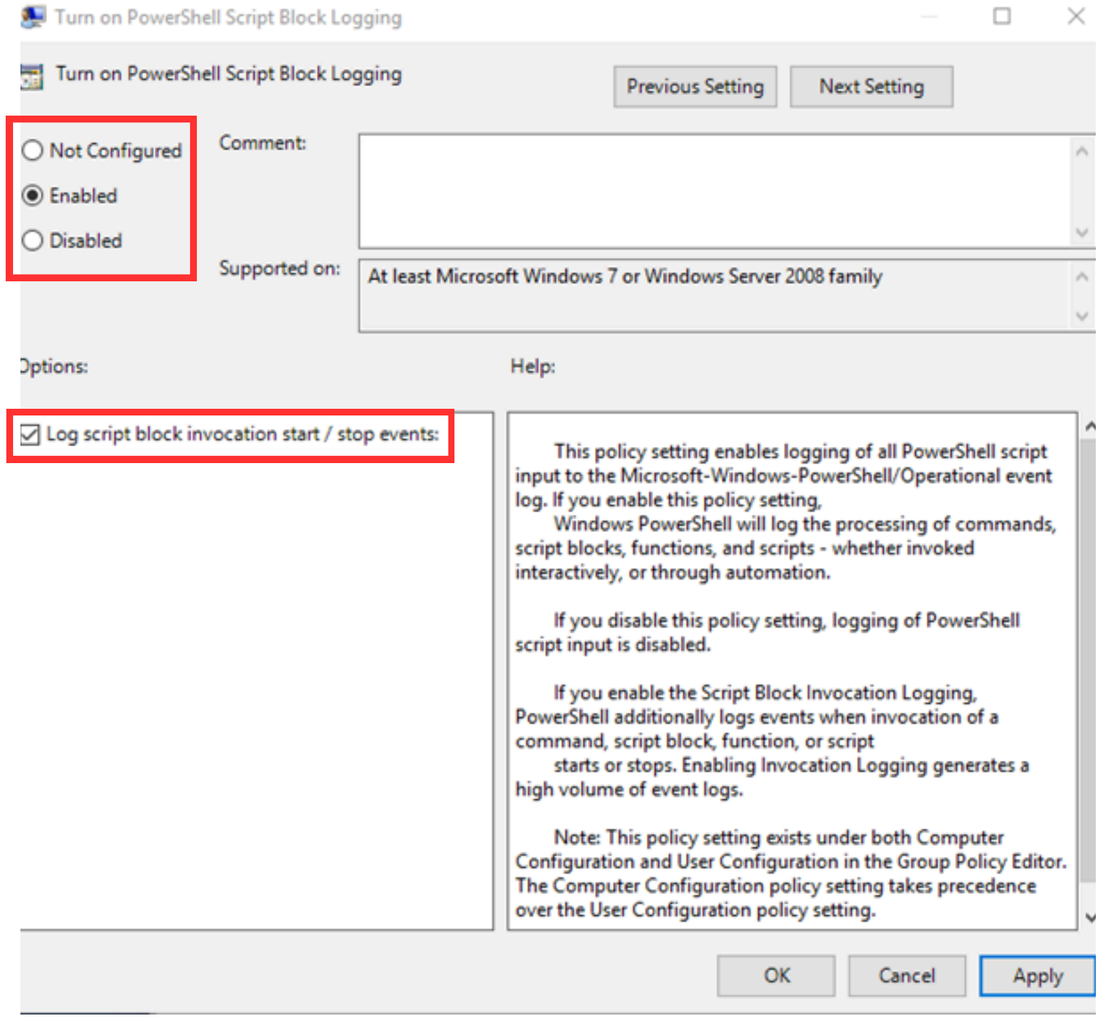
_tasks

(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



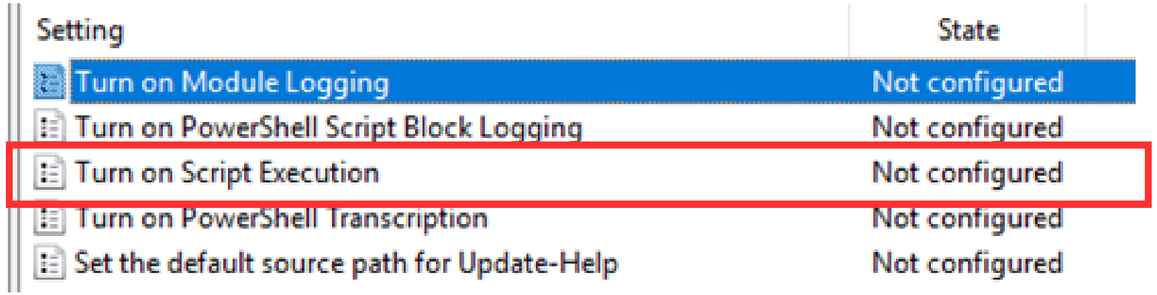
This will log all blocked scripts when enabled



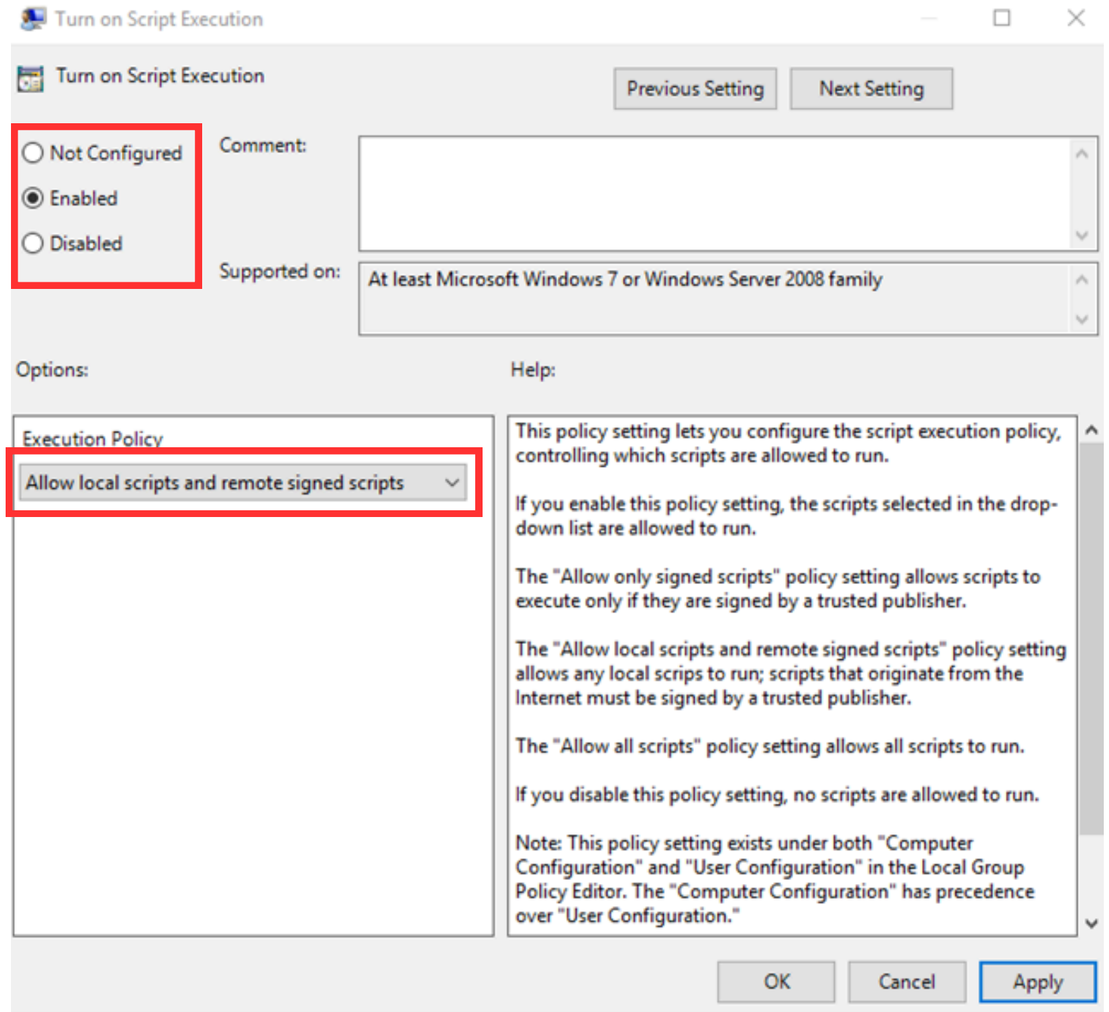
_tasks

(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



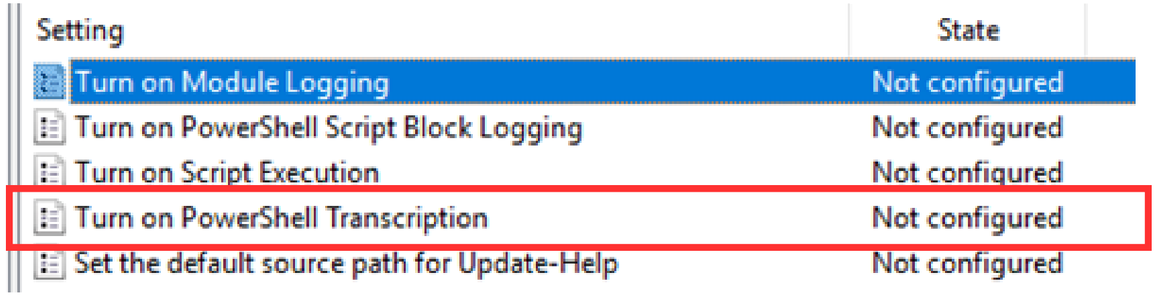
This setting will only allow local scripts and remote signed scripts to run. E.g. Microsoft signed scripts

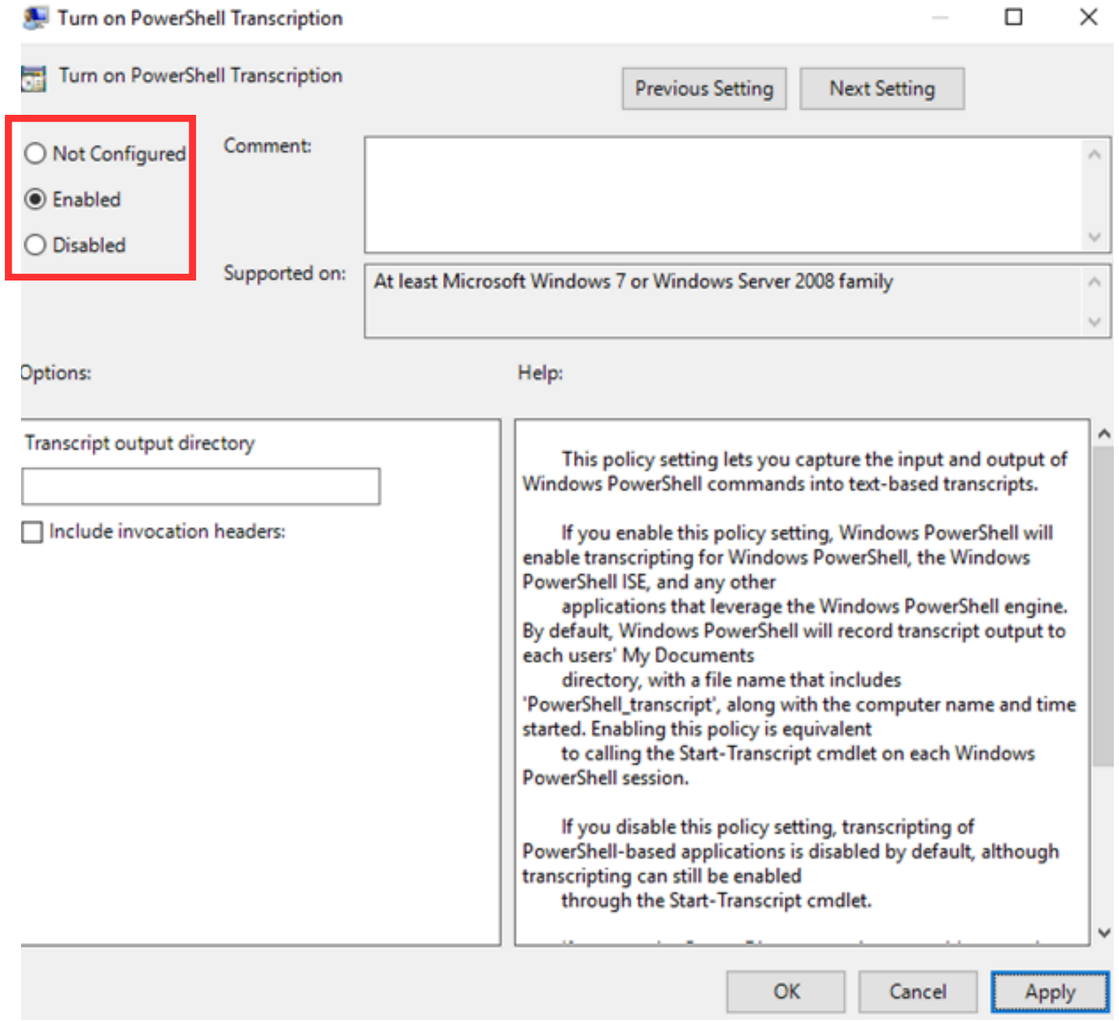


_tasks

(16) Secure System from PowerShell Exploits

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

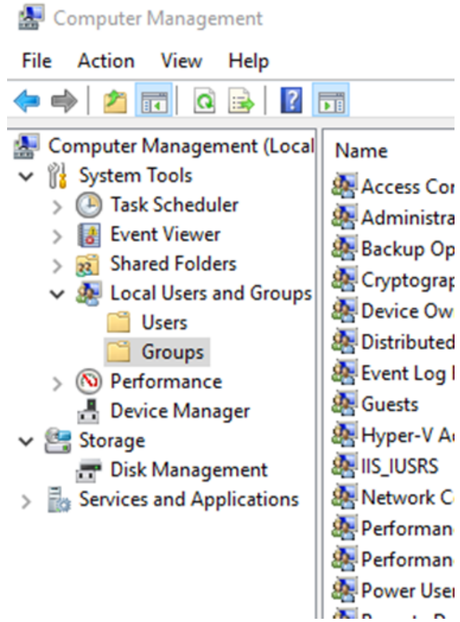




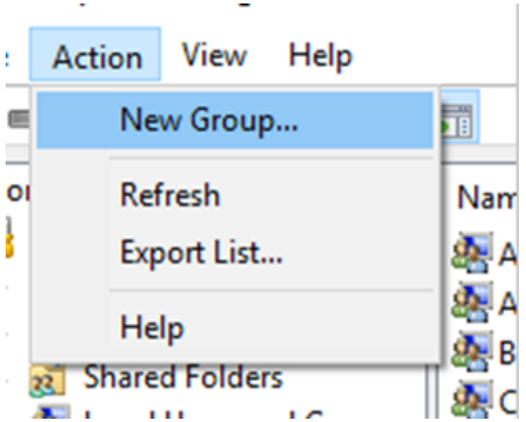
_tasks

(30) Create groups for easier account management

1. In the Computer Management dialog box, navigate to "Groups".
Path: System Tools → Local Users and Groups → Groups



2. Click on Action > click on "New group..."

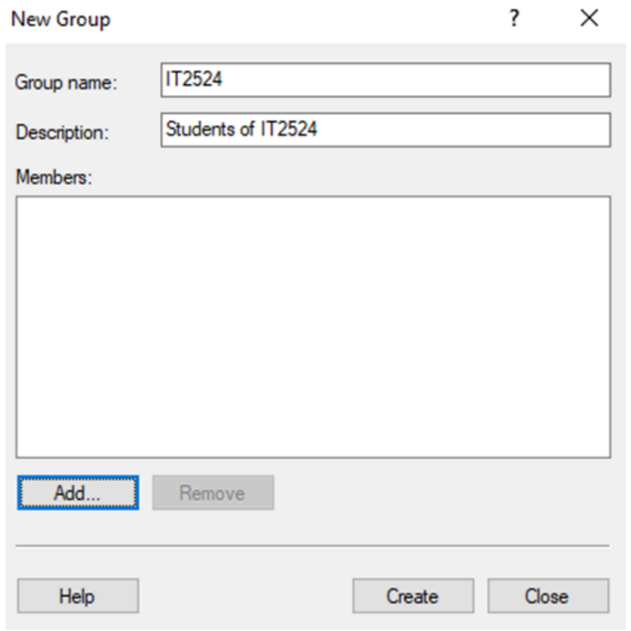


system security and account management

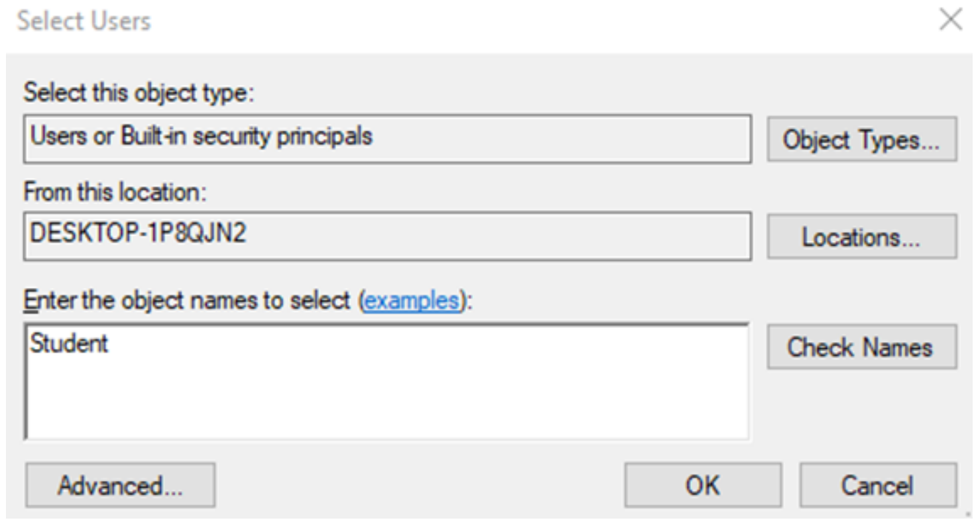
_tasks

(30) Create groups for easier account management

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



Enter name of user then click ok



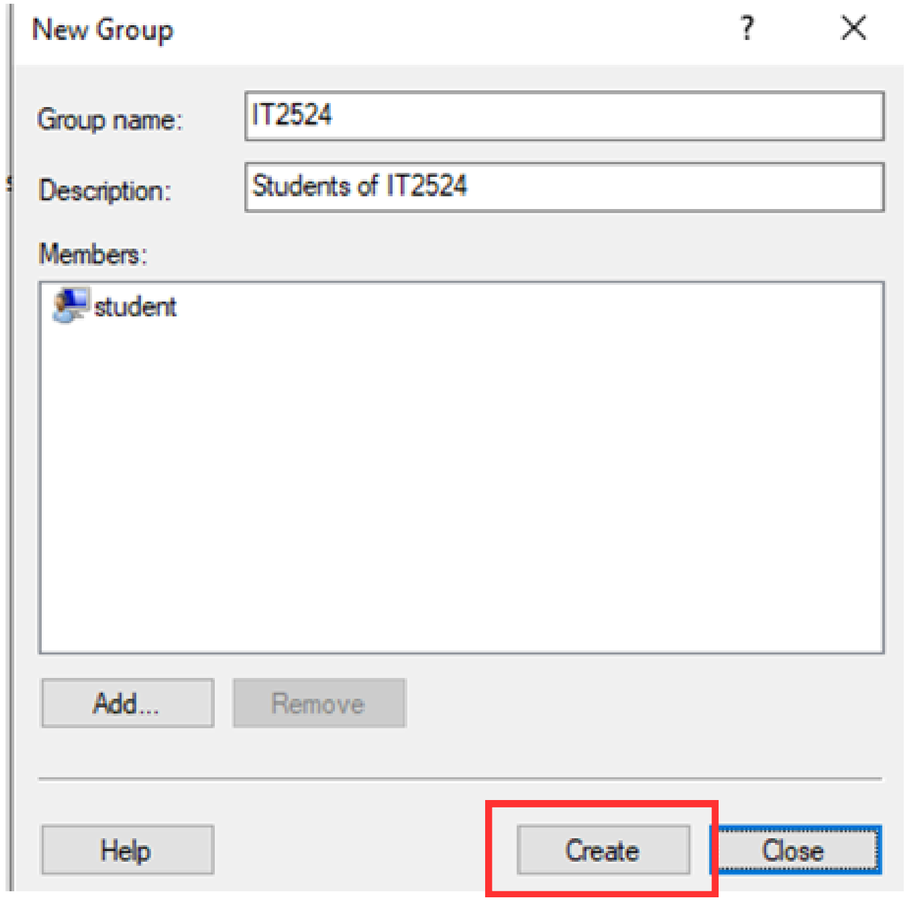
system security and account management

_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

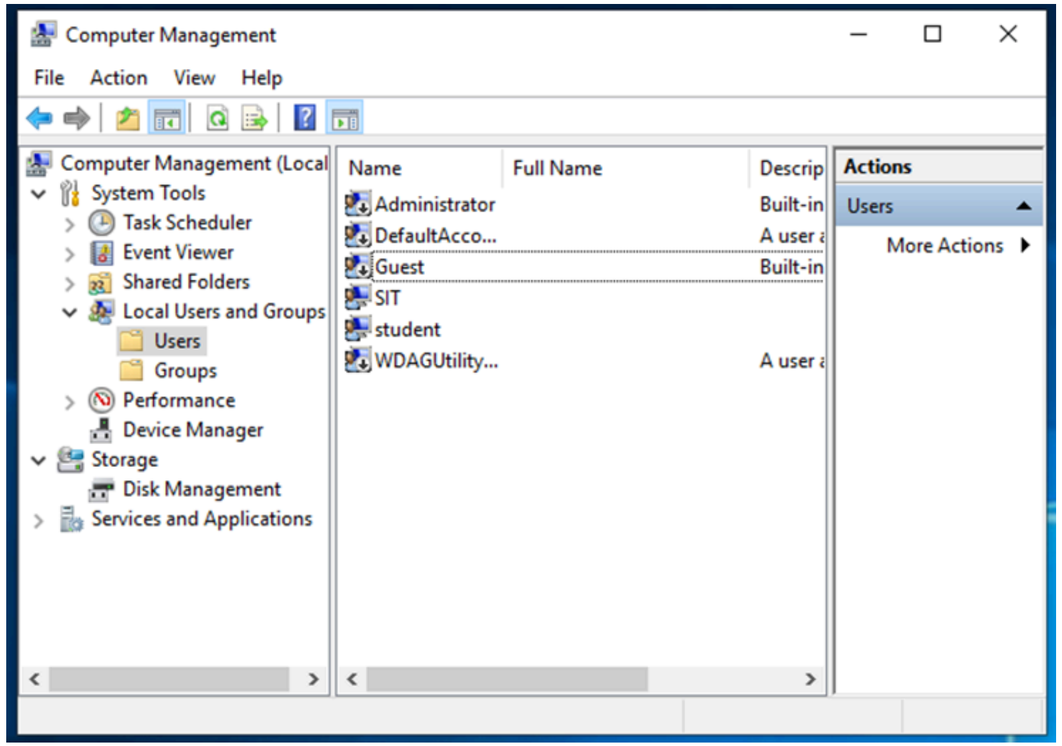


_tasks

(30) Create groups for easier account management

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

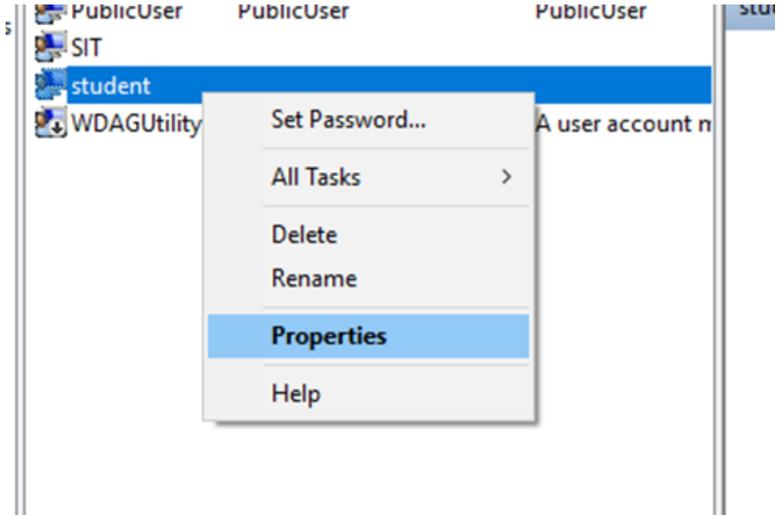
6. In the Computer Management dialog box, navigate to "Users".
Path: System Tools → Local Users and Groups → Users



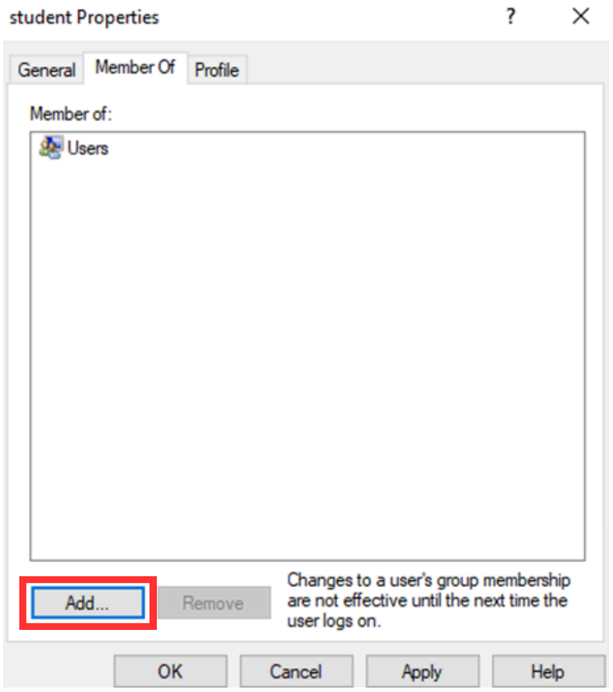
_tasks

(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...”

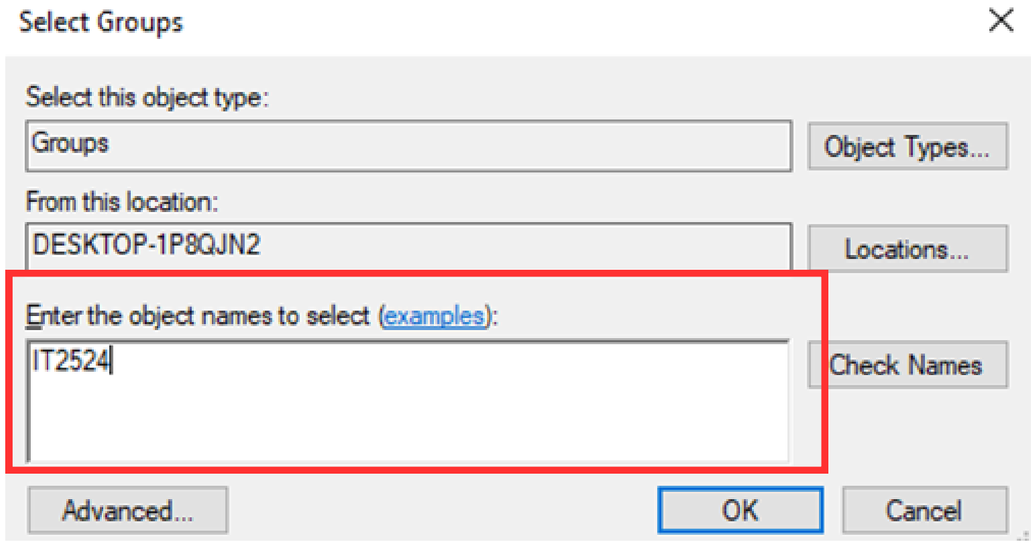


system security and account management

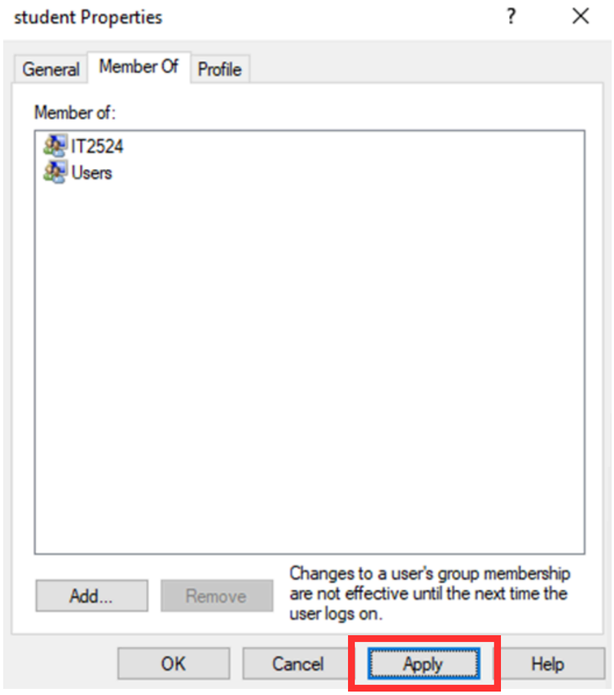
_tasks

(30) Create groups for easier account management

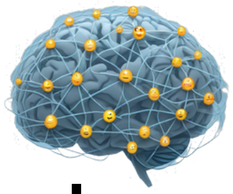
9. Enter the group name and click ok



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

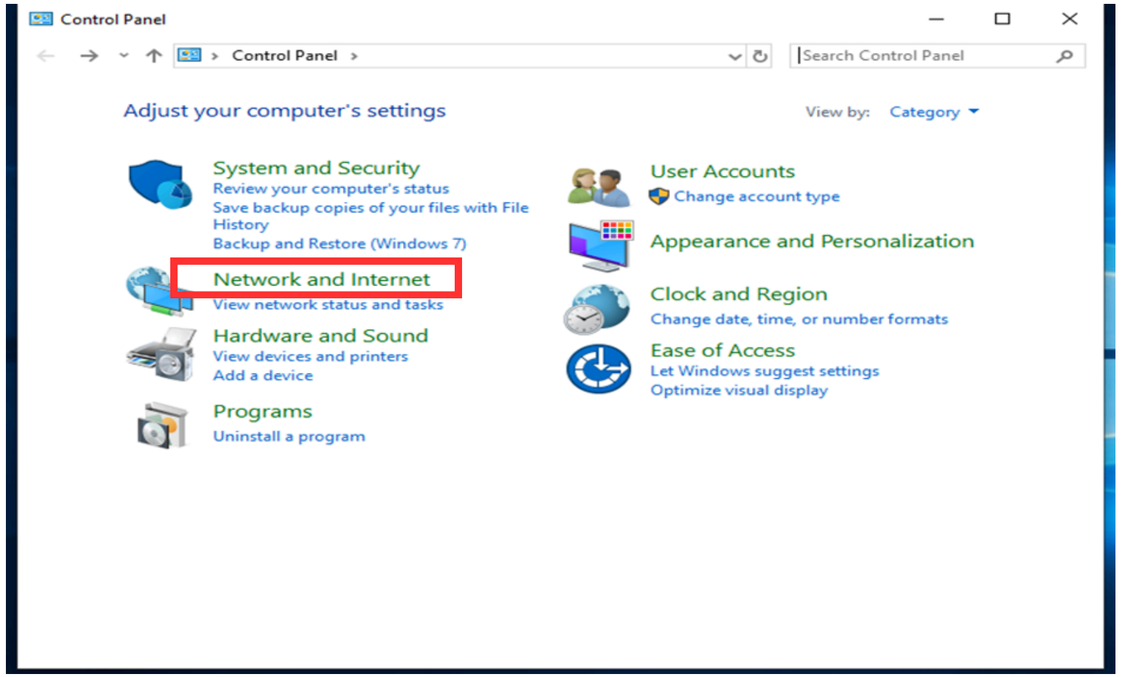
} additional tasks

network stuff and access control

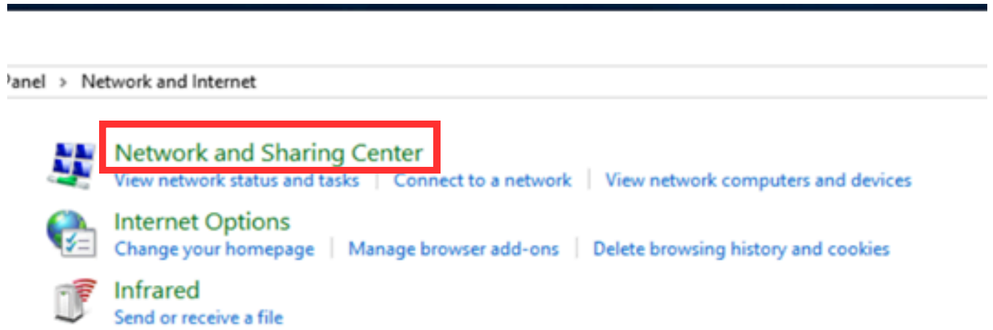
_tasks

(8) Protect Files And Shared Folders

1. Open ‘Control Panel’ and click on ‘Network and Internet’



2. Click on ‘Network and Sharing Centre’.

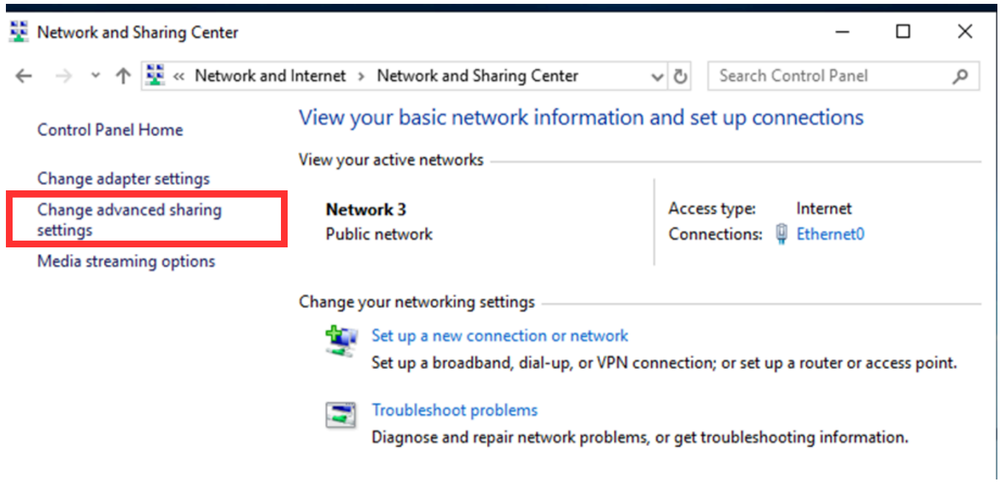


network stuff and access control

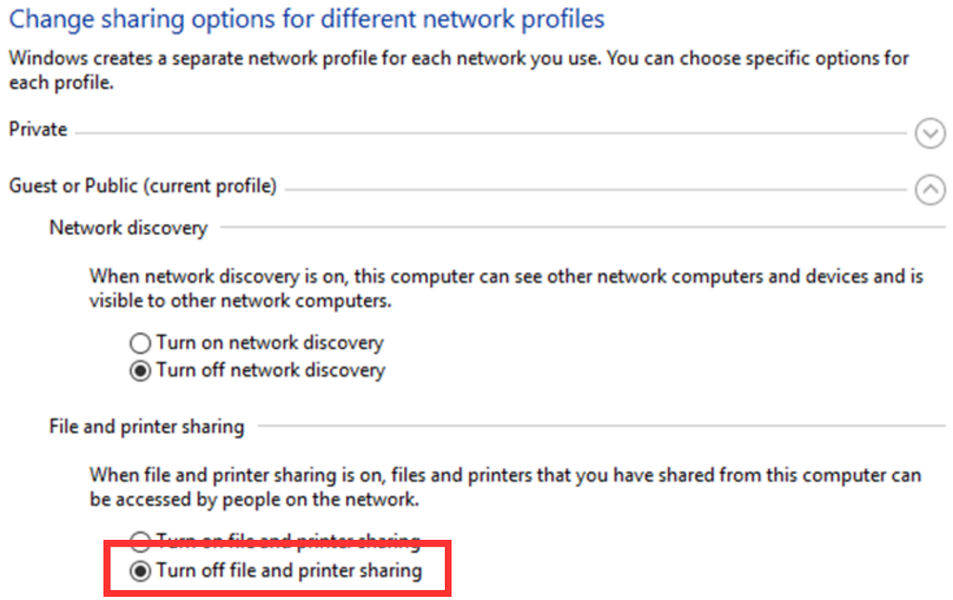
_tasks

(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.

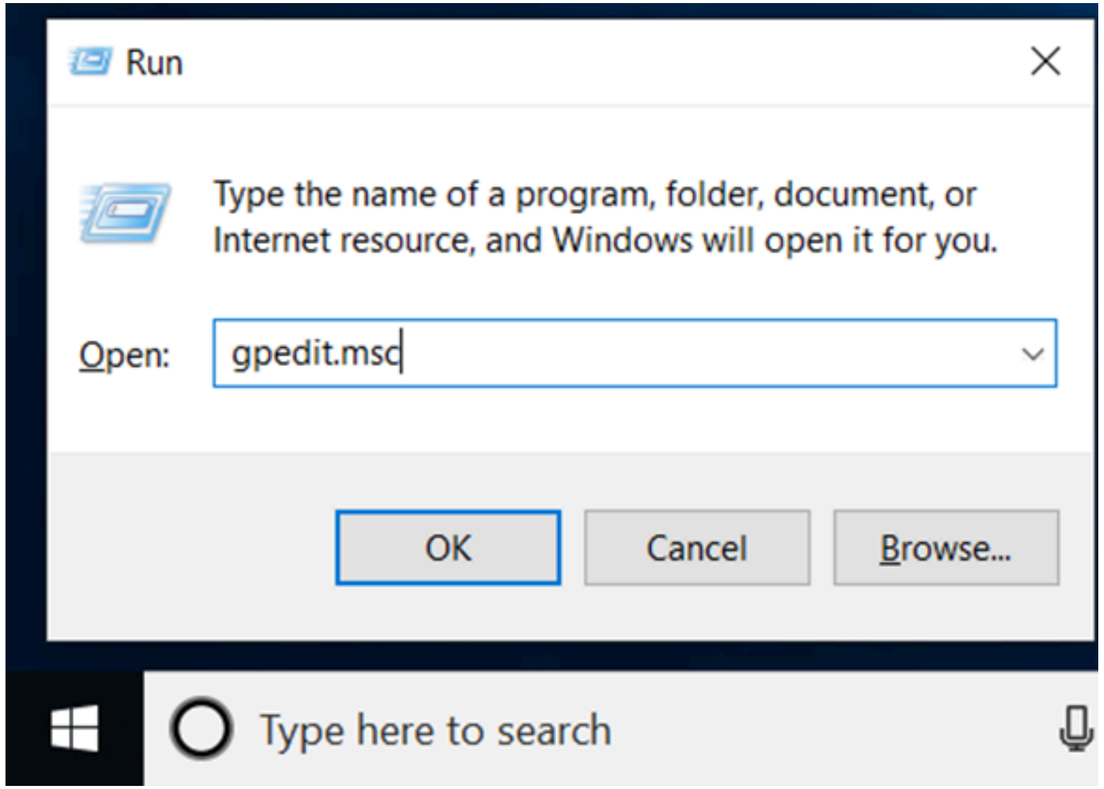


network stuff and access control

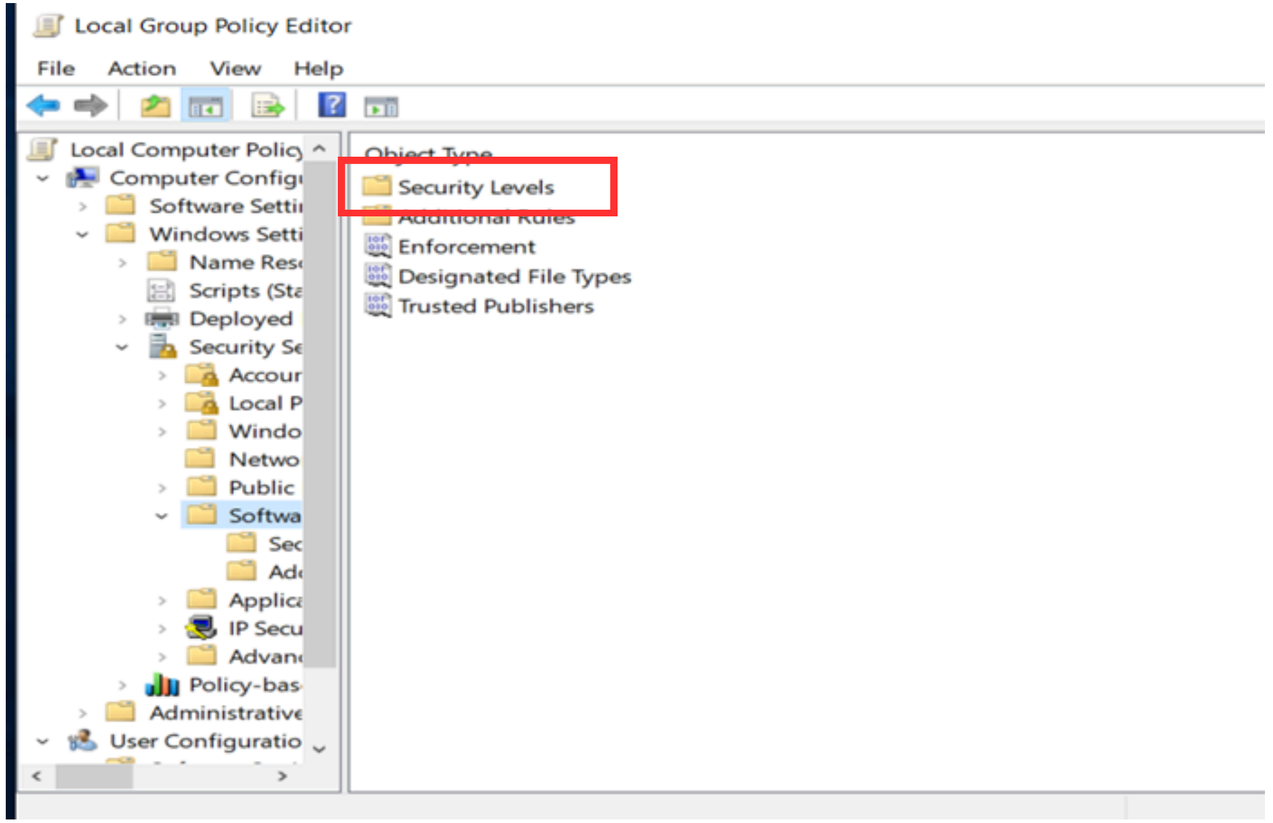
_tasks

(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

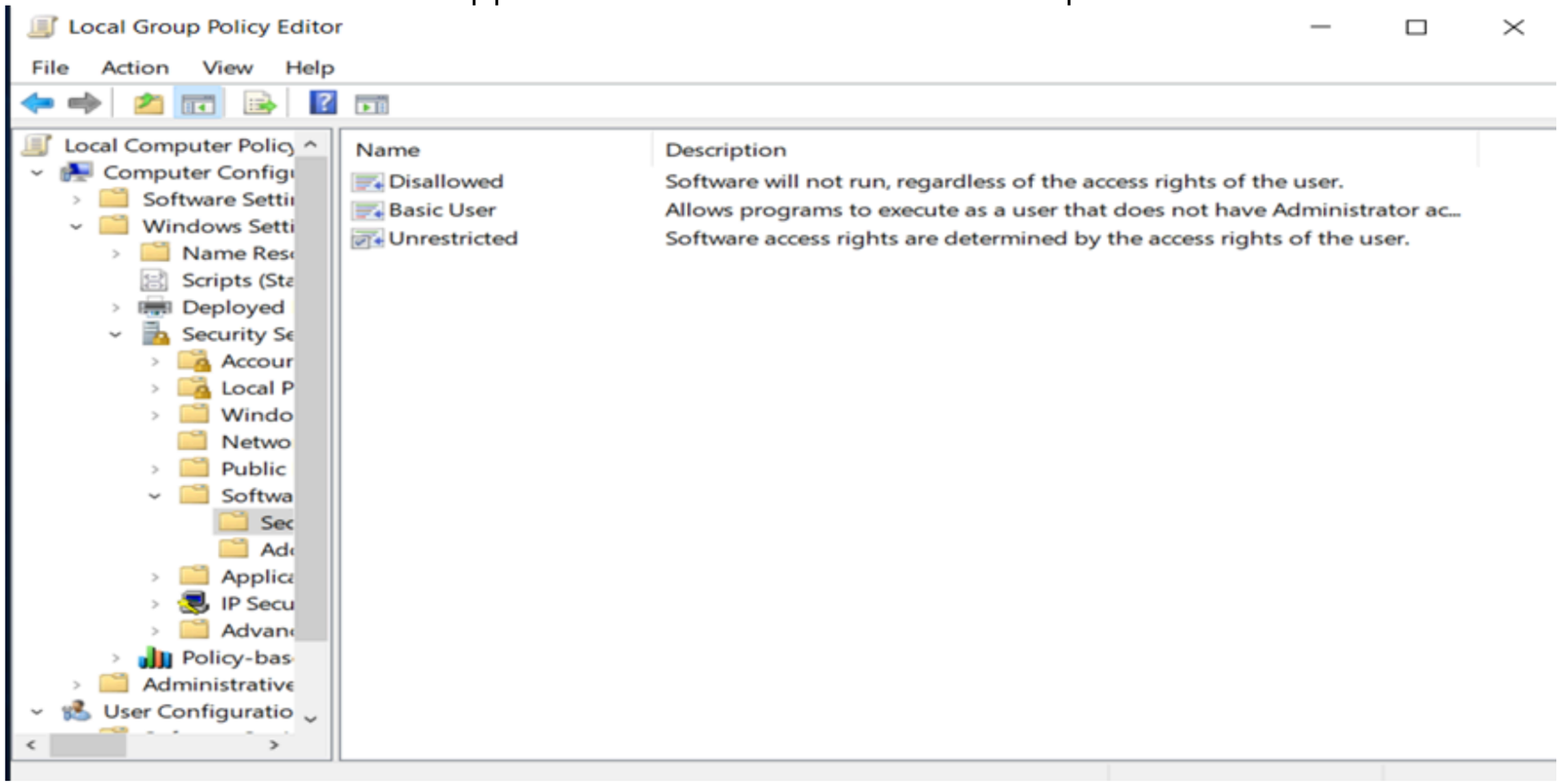
(10) Use software restriction policies

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.

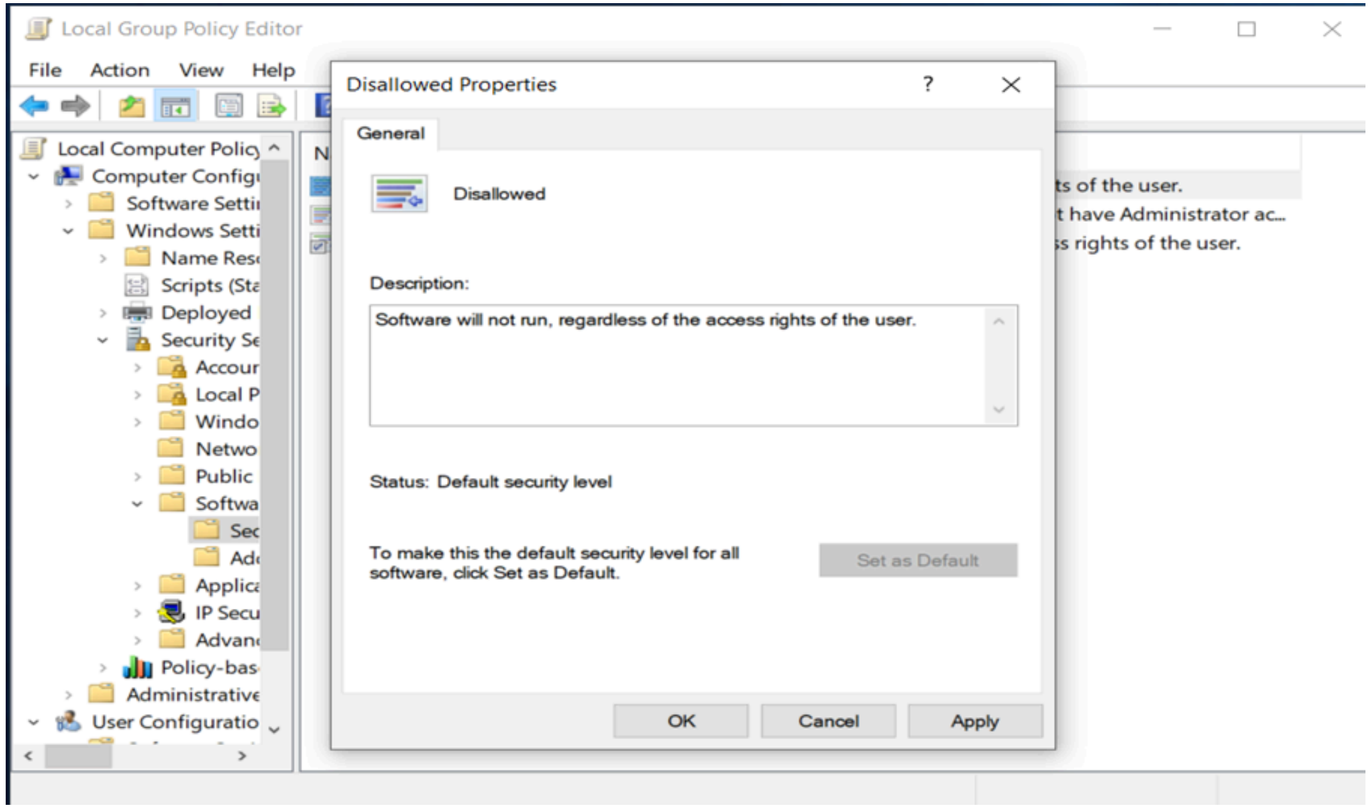
Unrestricted: Allows all applications to run unless there's a specific restriction rule.



_tasks

(10) Use software restriction policies

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

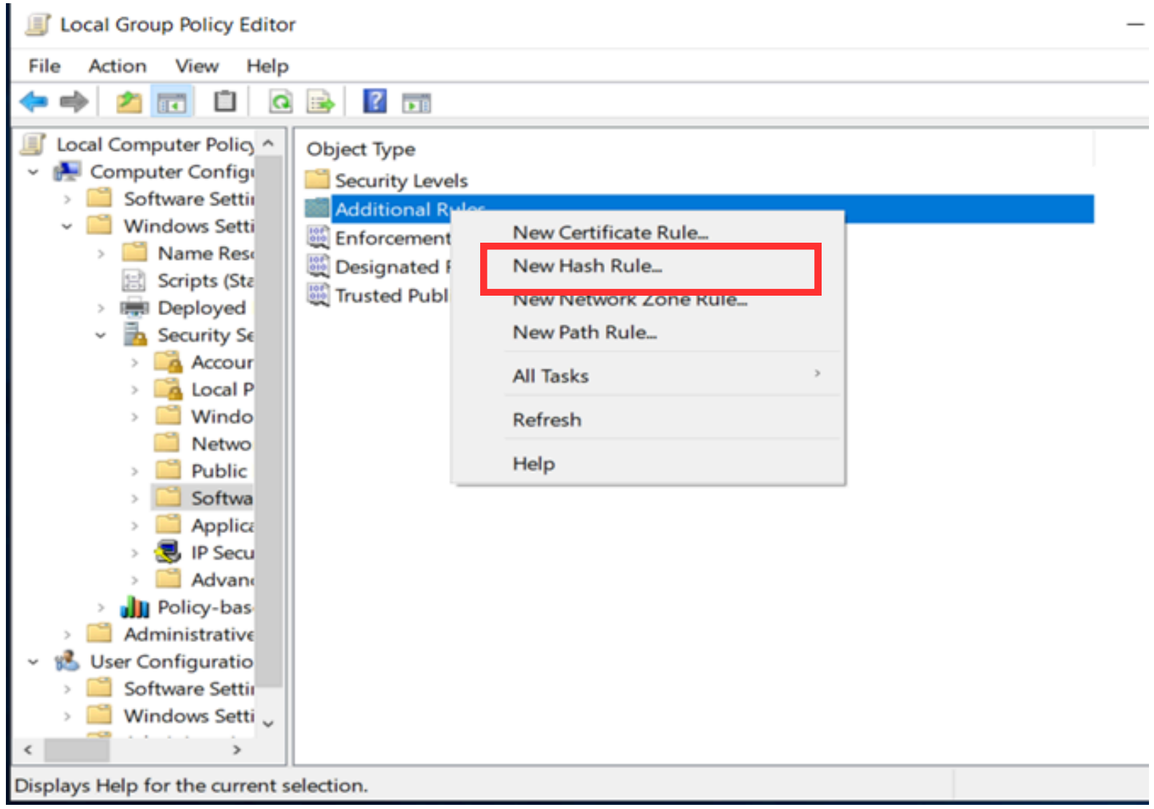


_tasks

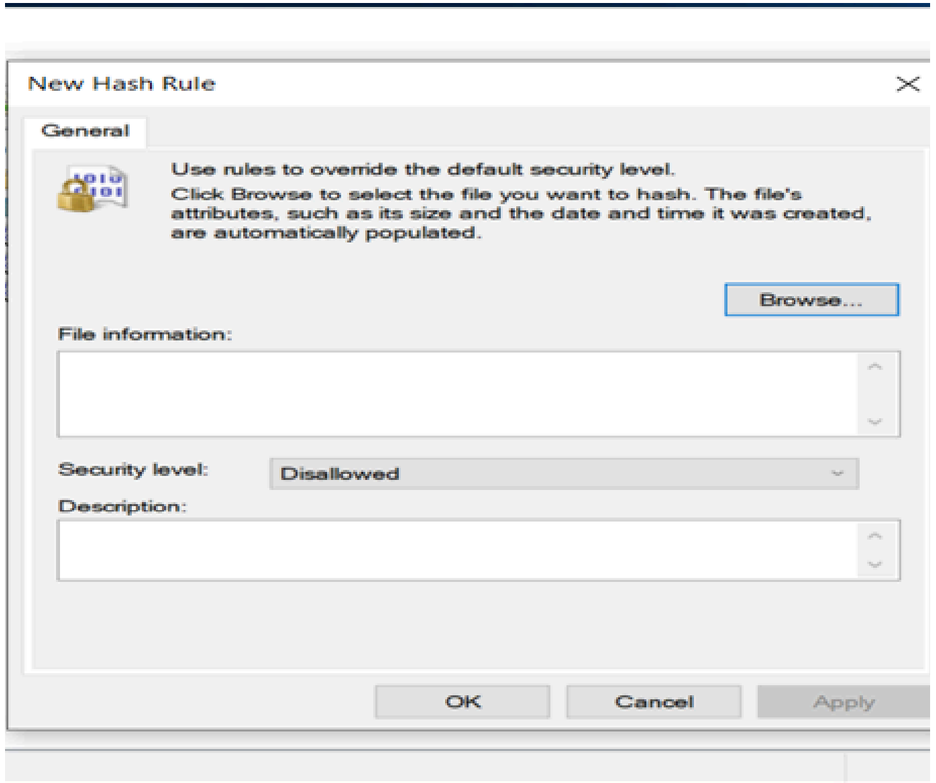
(10) Use software restriction policies

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

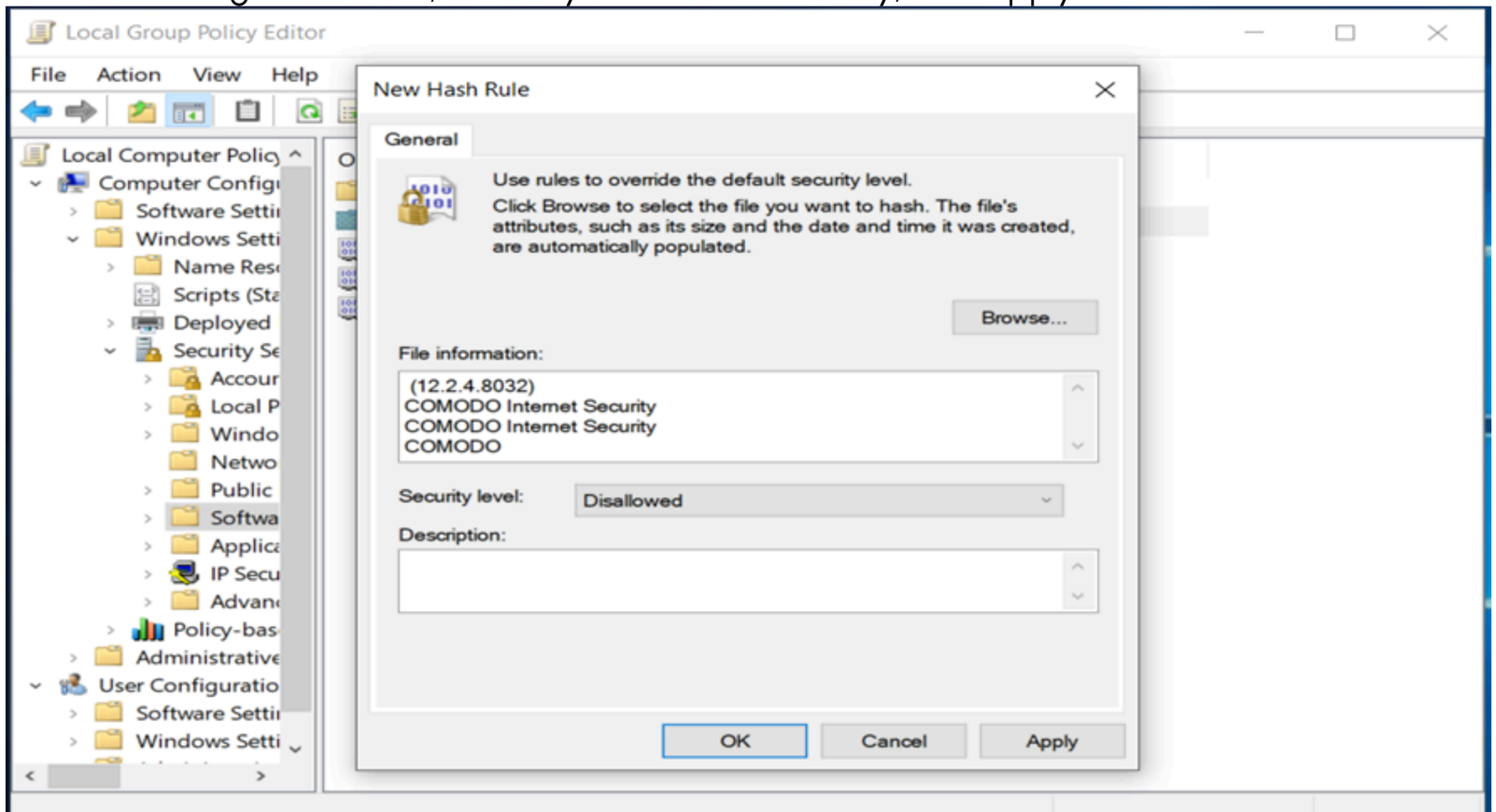


_tasks

(10) Use software restriction policies

Additional way to use software policy

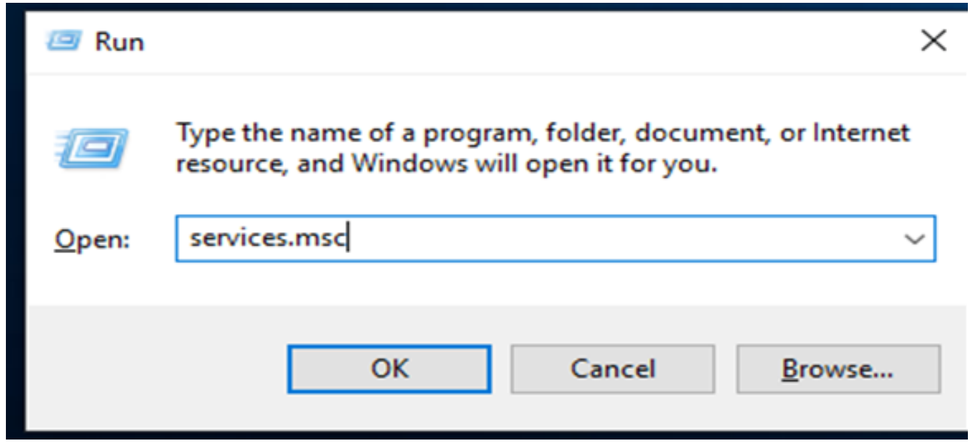
3.after searching for the file,choose your level of security,click apply and ok



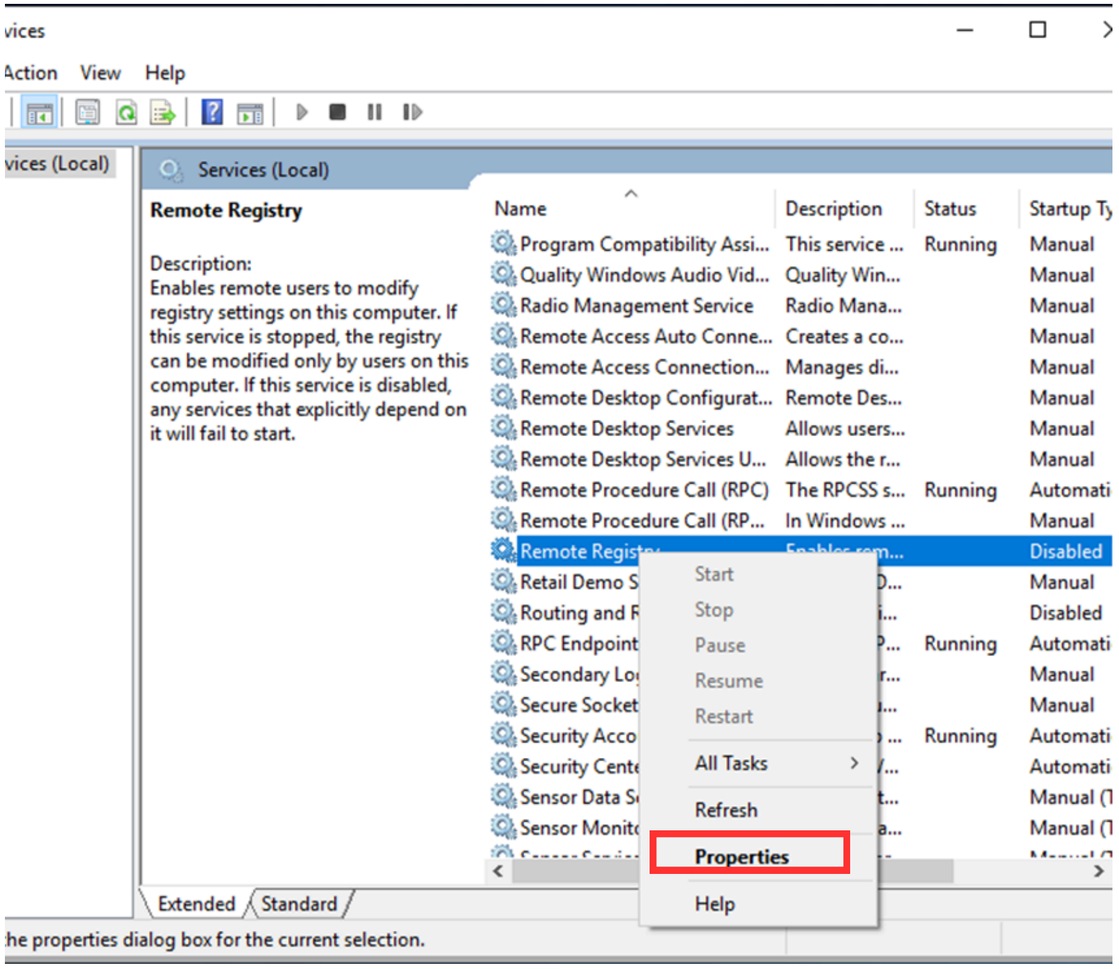
_tasks

(11) Disable unnecessary services

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



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

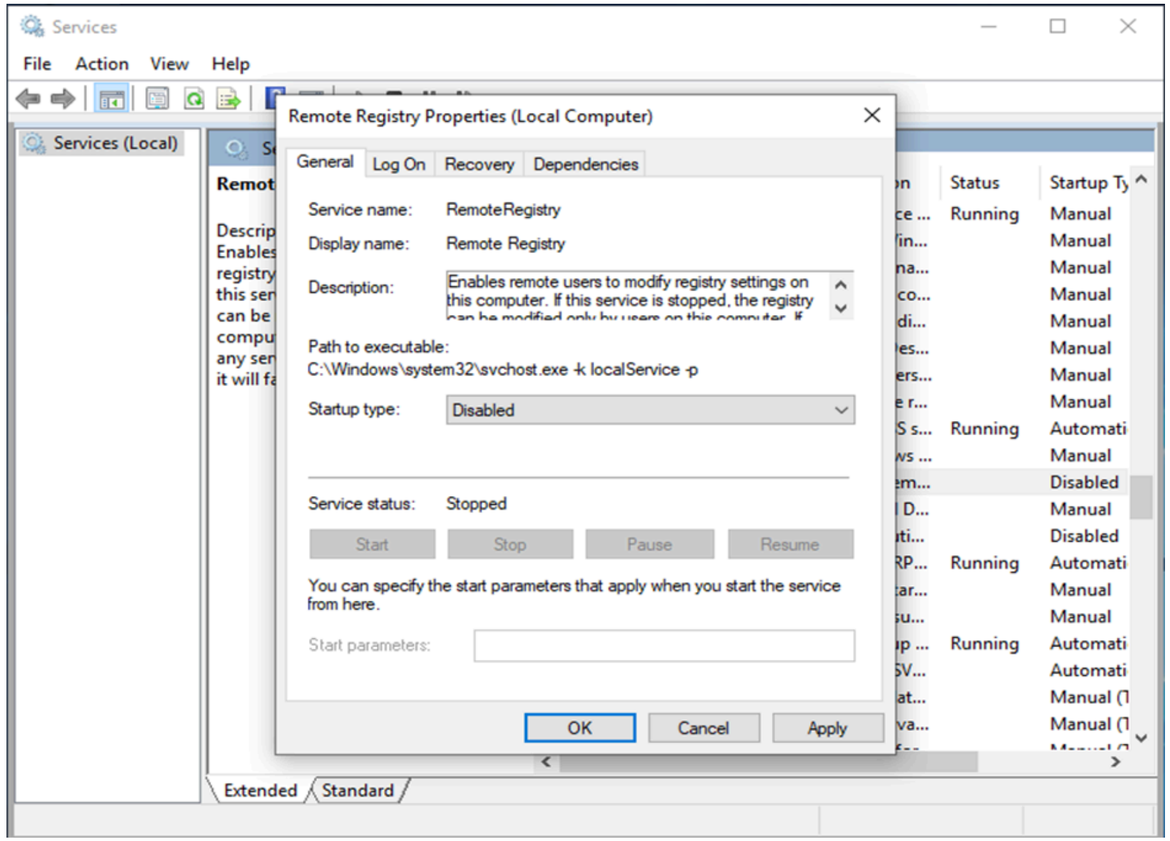


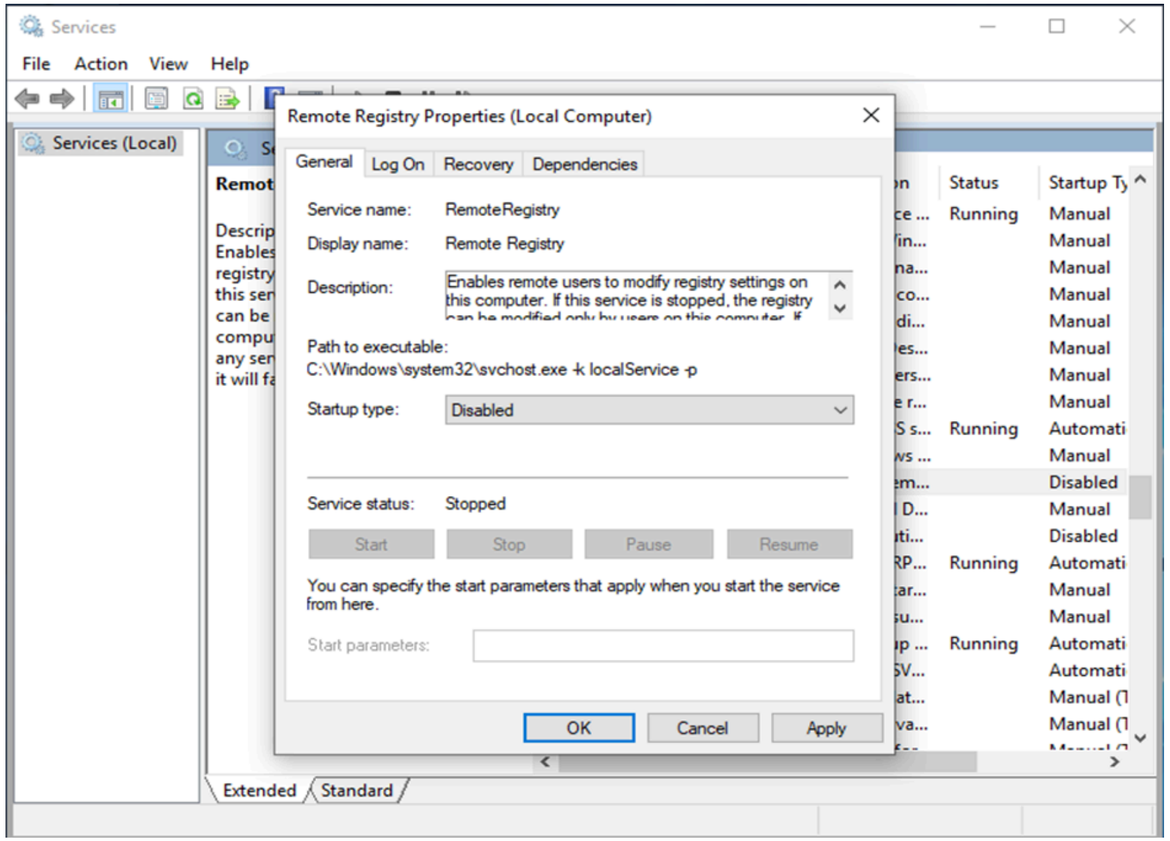
_tasks

(11) Disable unnecessary services

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

E.gDisable FAX

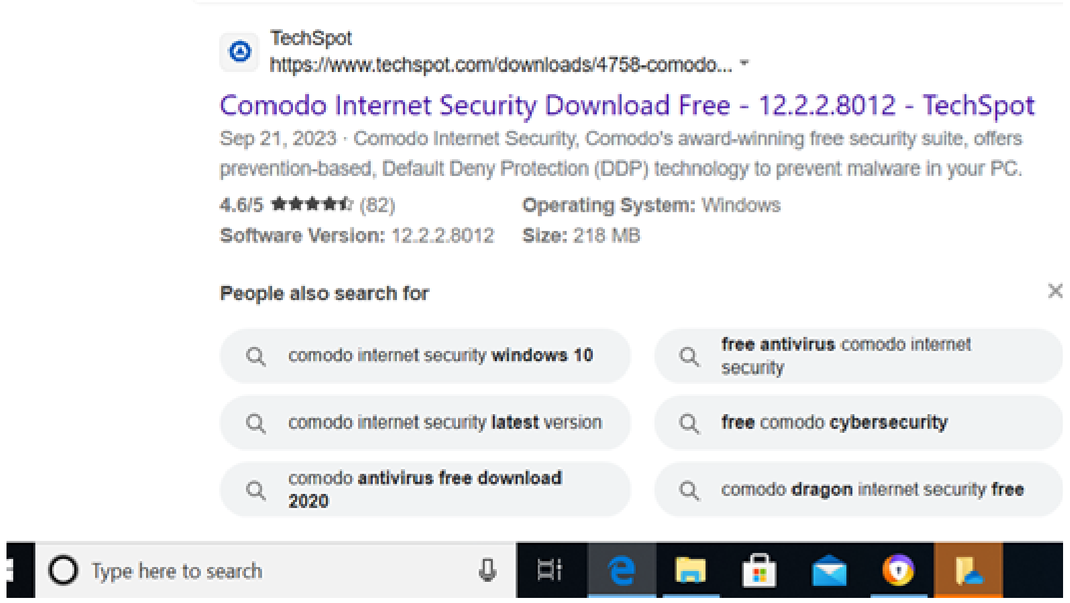




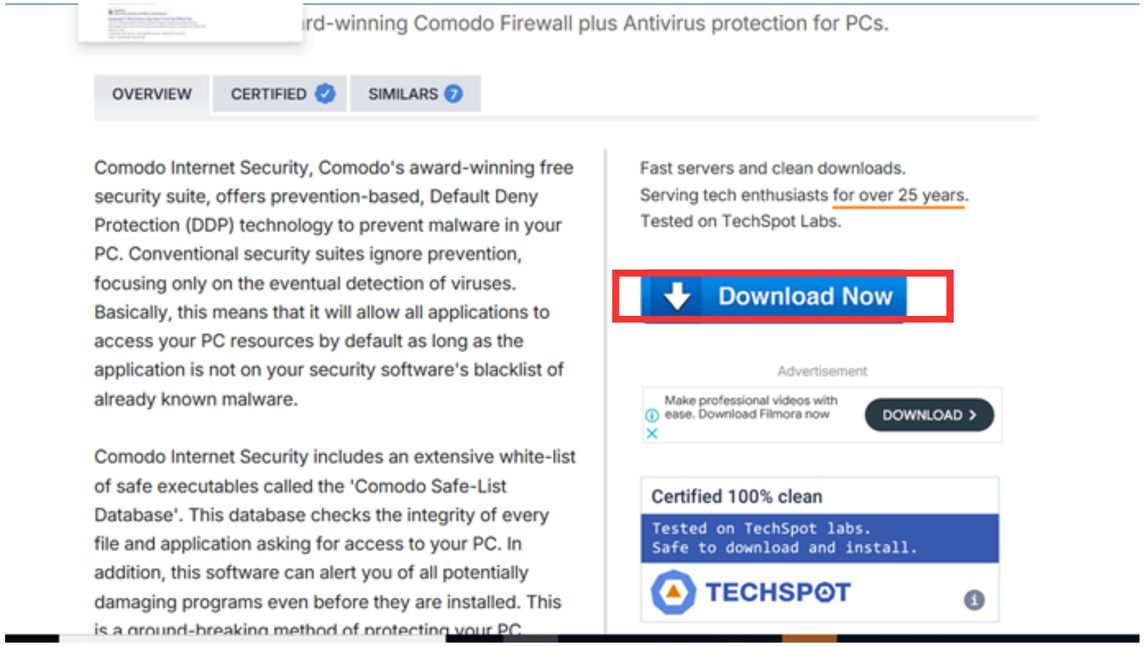
_tasks

(28) Install Host-Based Intrusion Prevention System

1.InstallComodo Internet Security Download - 12.2.2.8012



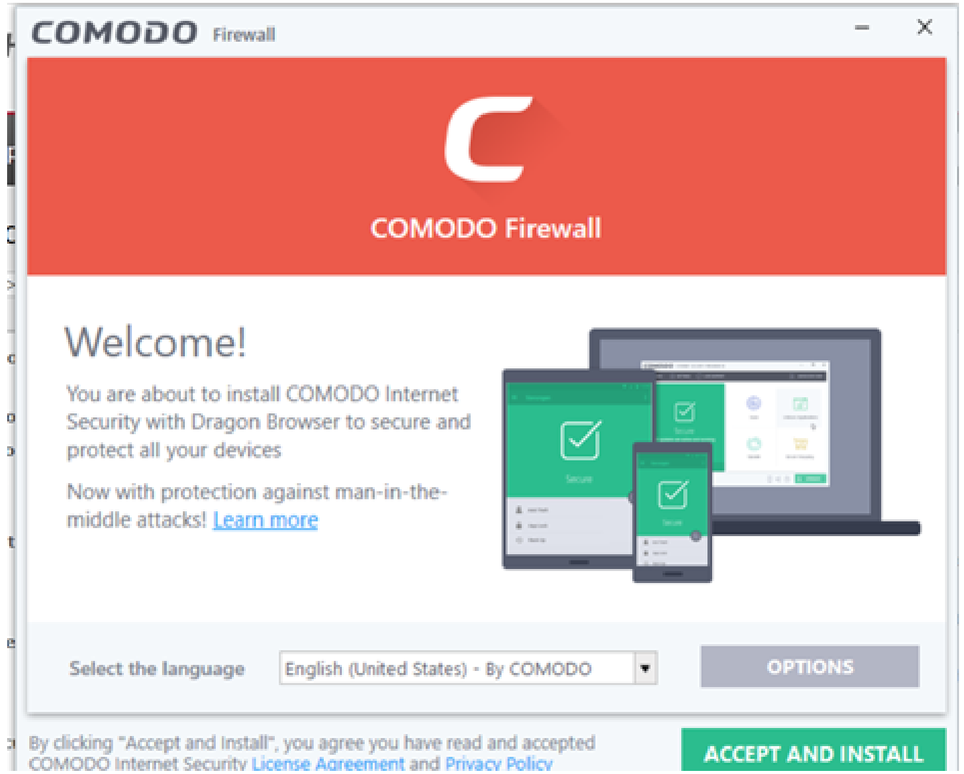
2.Scroll down and click on 'Download Now'



_tasks

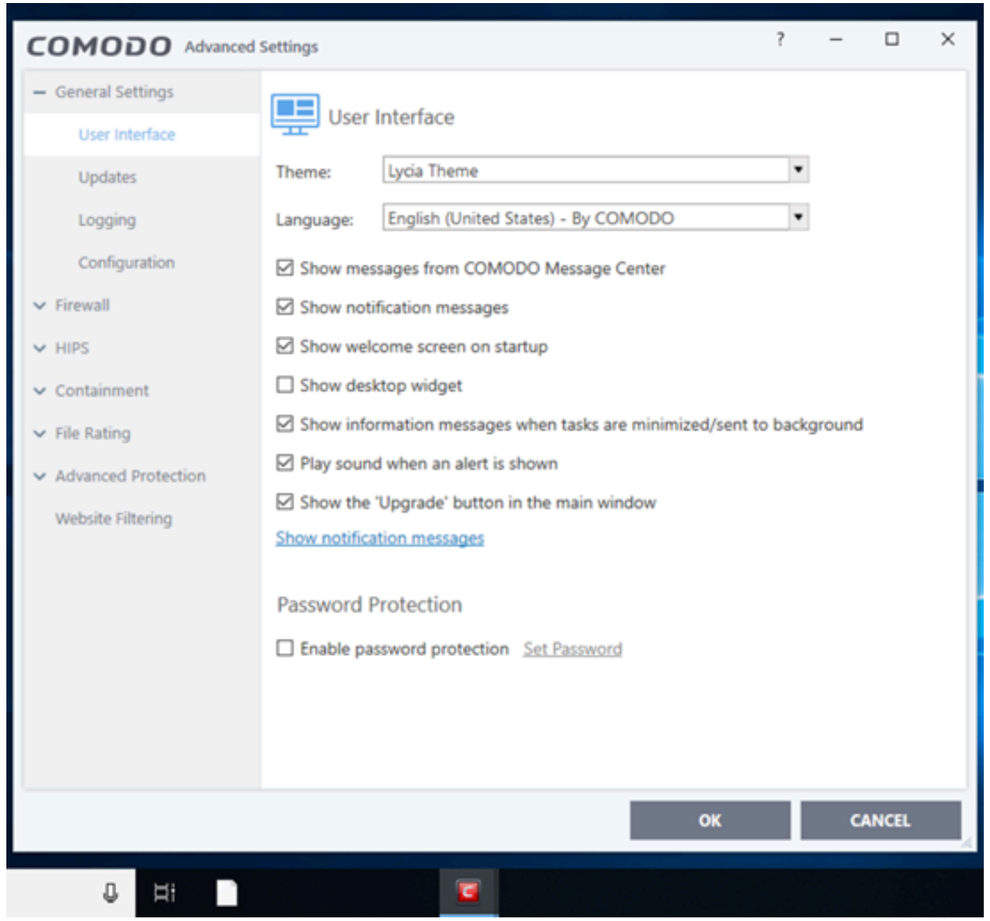
3.When this pop up shows,click yes

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

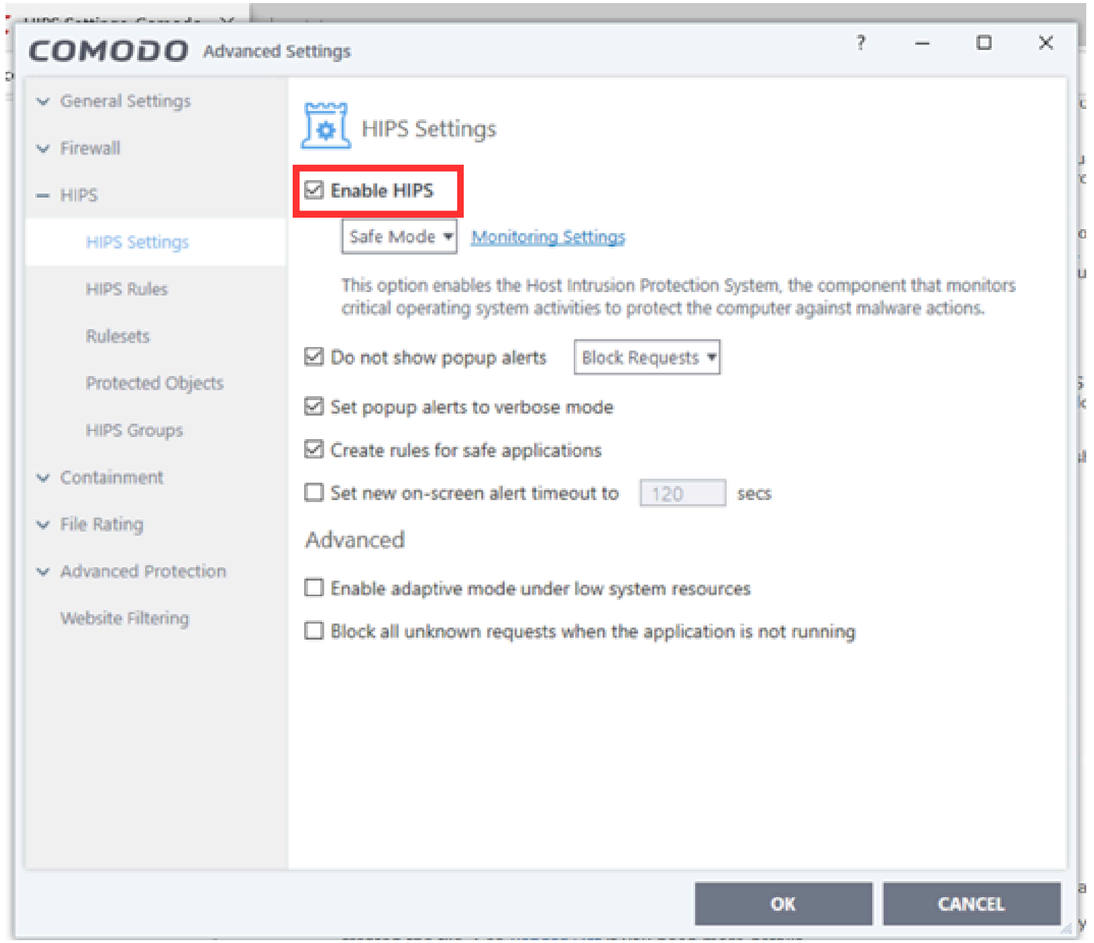


_tasks

5.After Restarting,Open up the Comodo Firewall

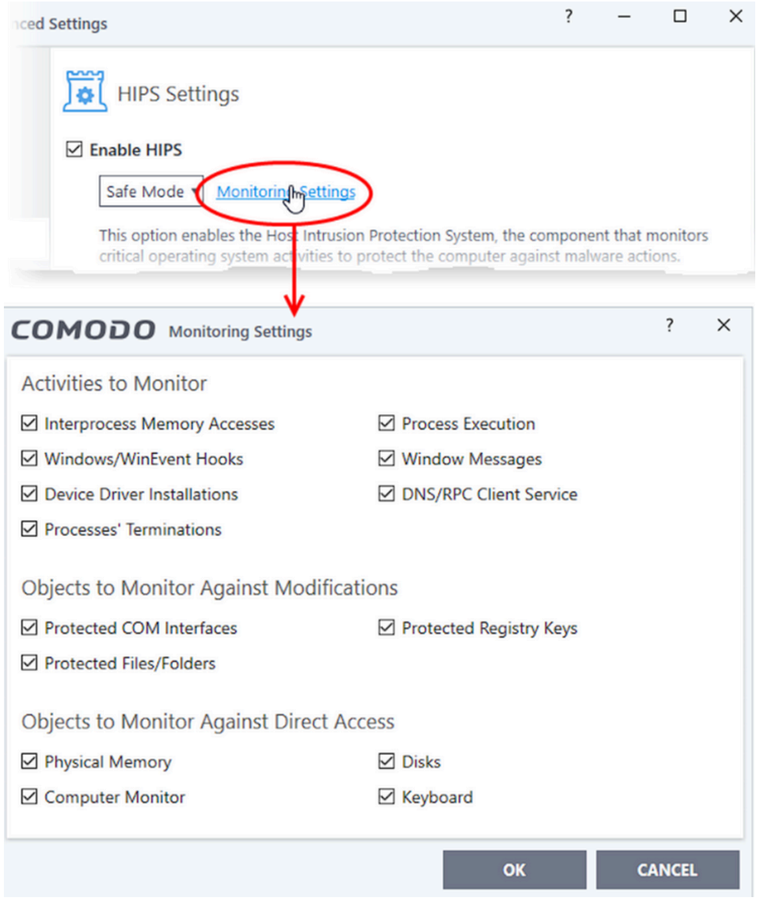


6.Scroll to HIPS settings and click on ‘Enable HIPS’ and click on ‘Safe Mod’

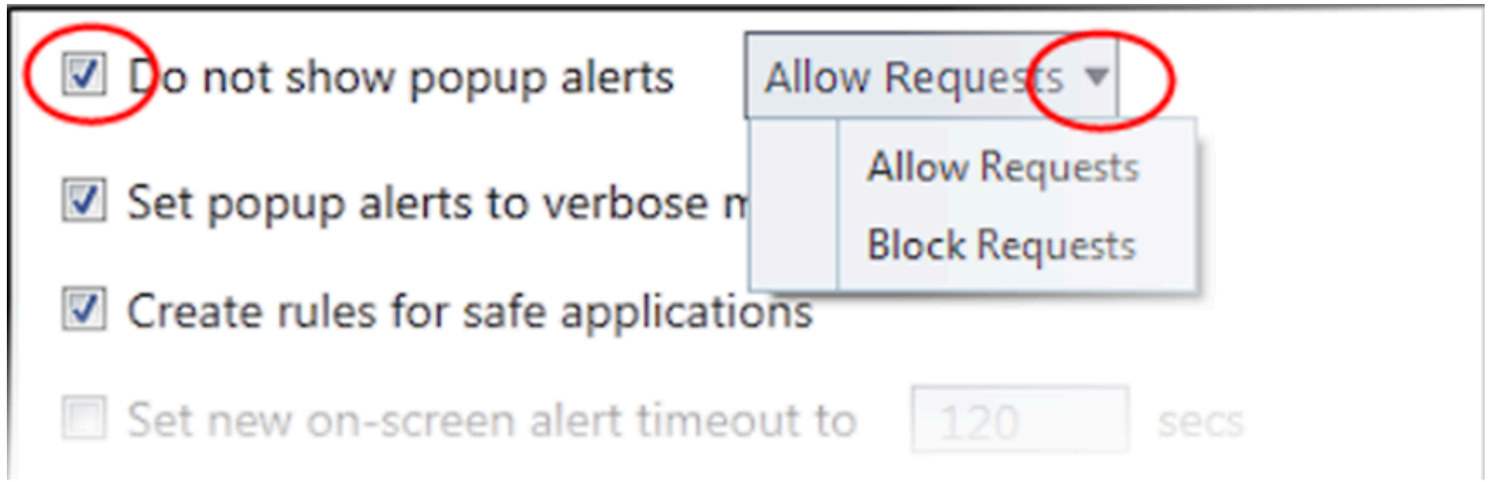


_tasks

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



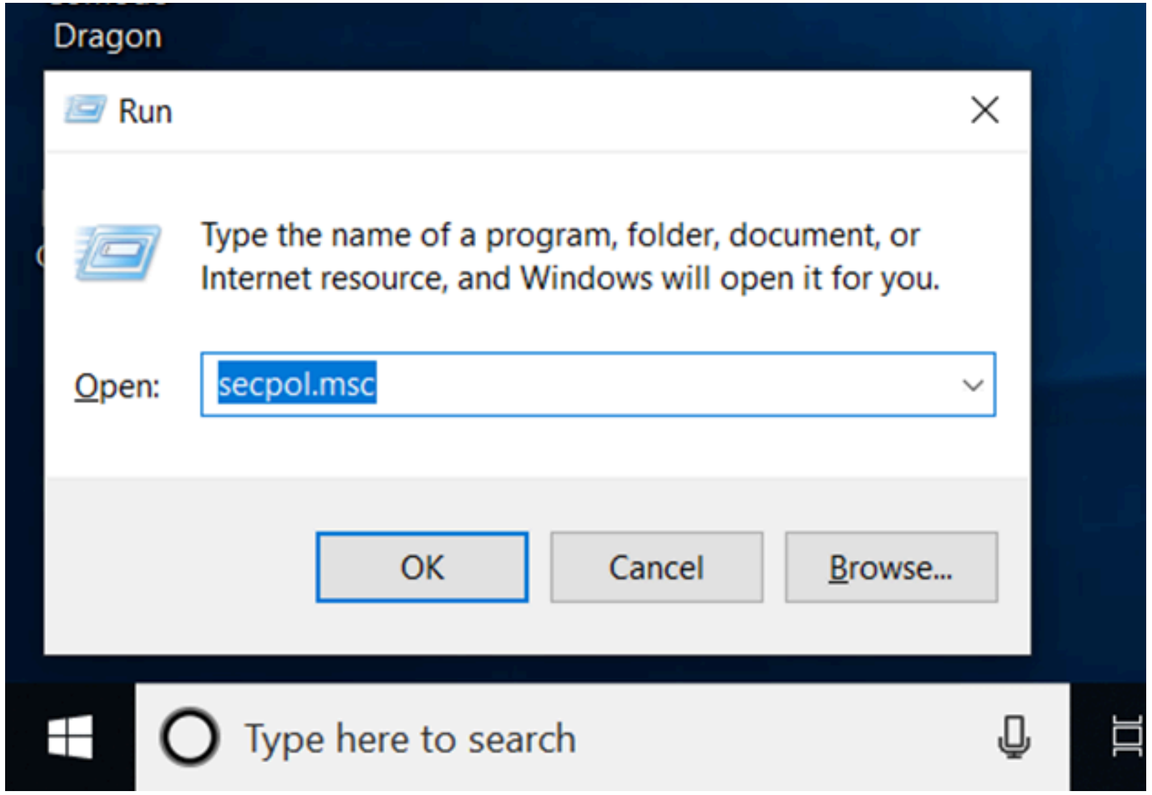
8.Click on the selected boxes,e.g. Block request from pop-up alerts



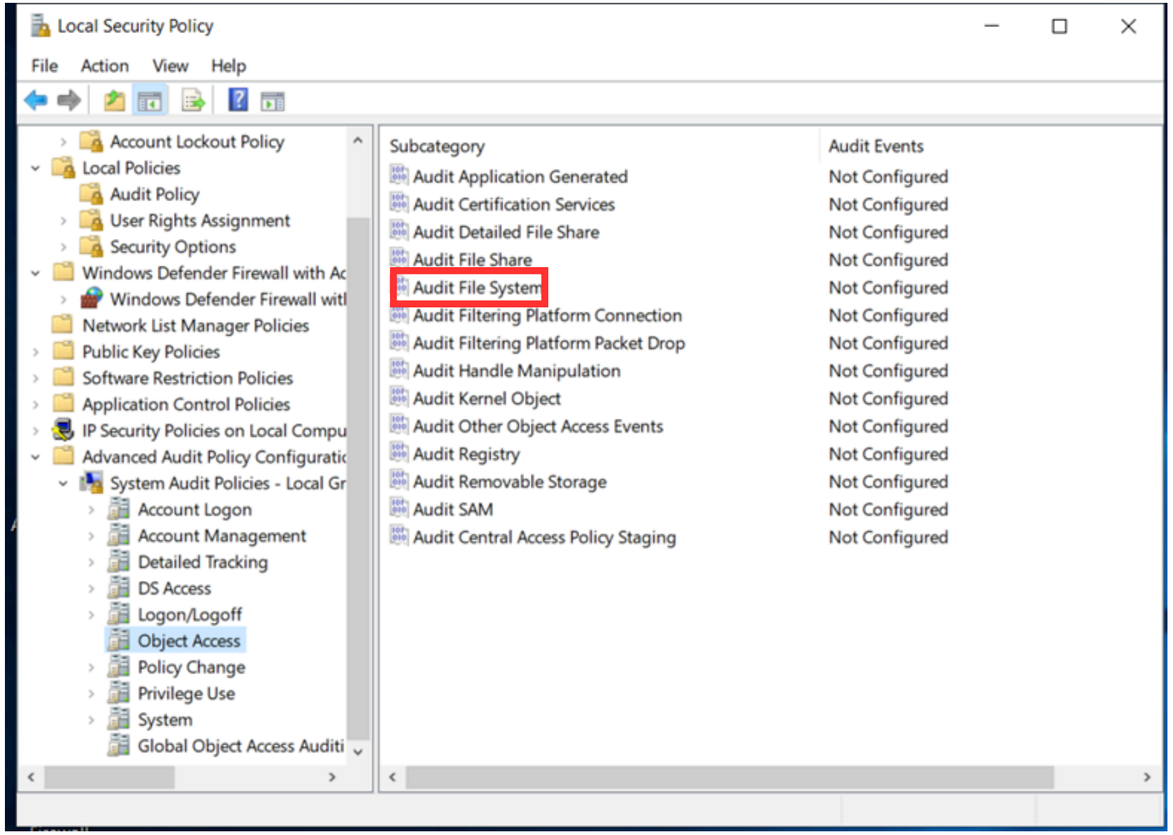
_tasks

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

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

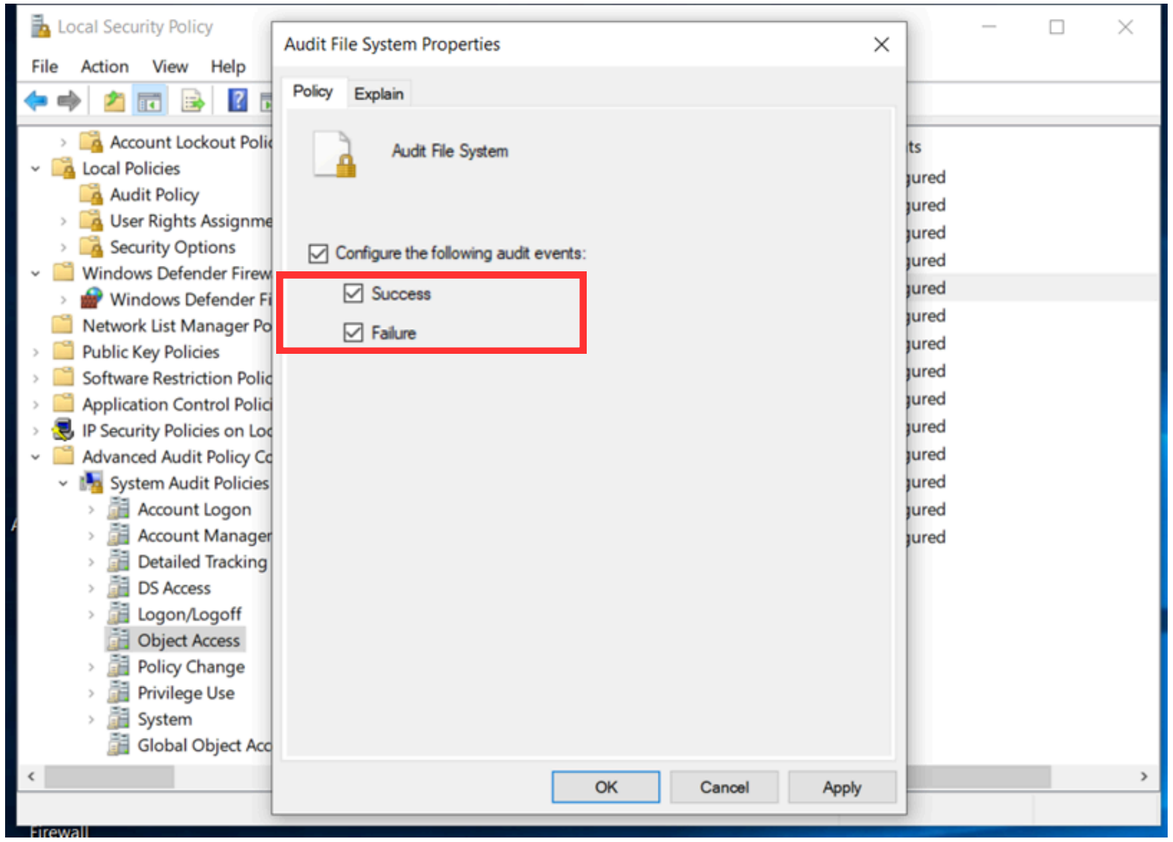


2.Go to Advanced Audit Policy Config > System Audit Policies > Object Access and click on Audit File System

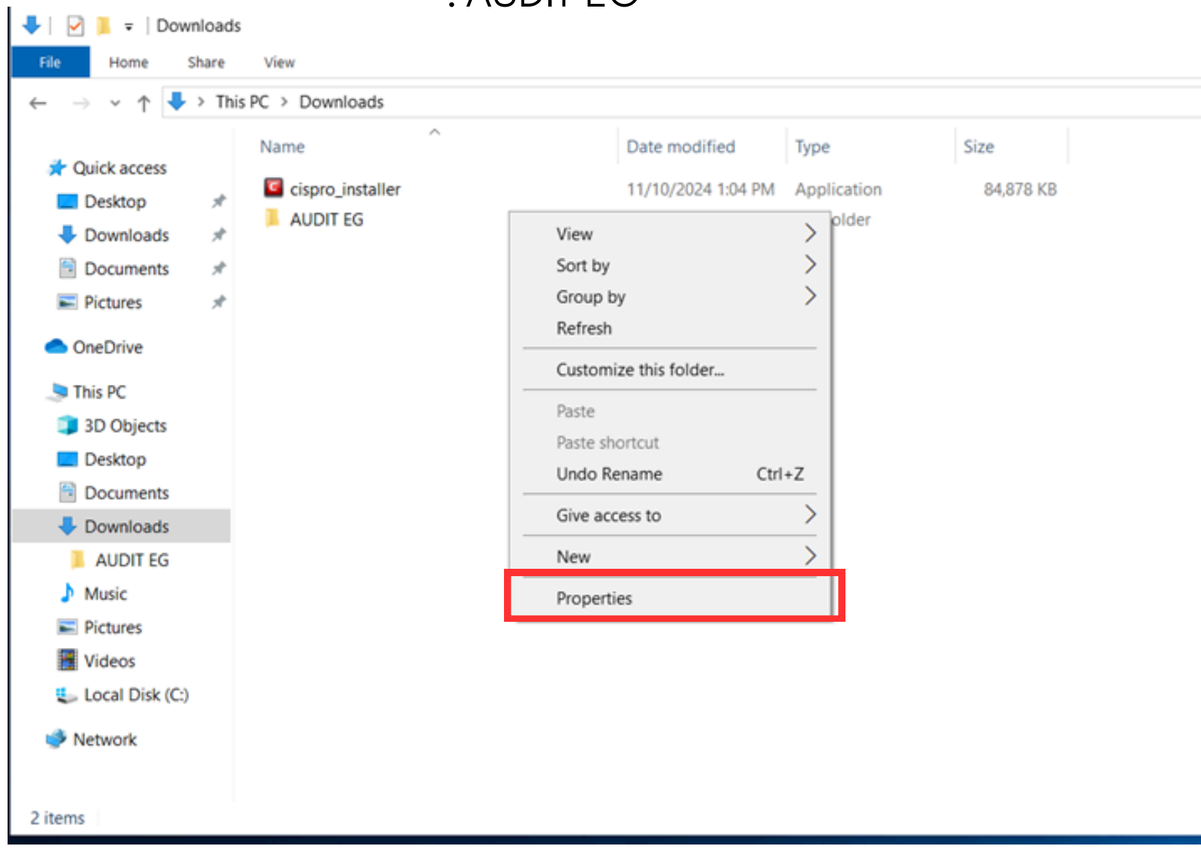


_tasks

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

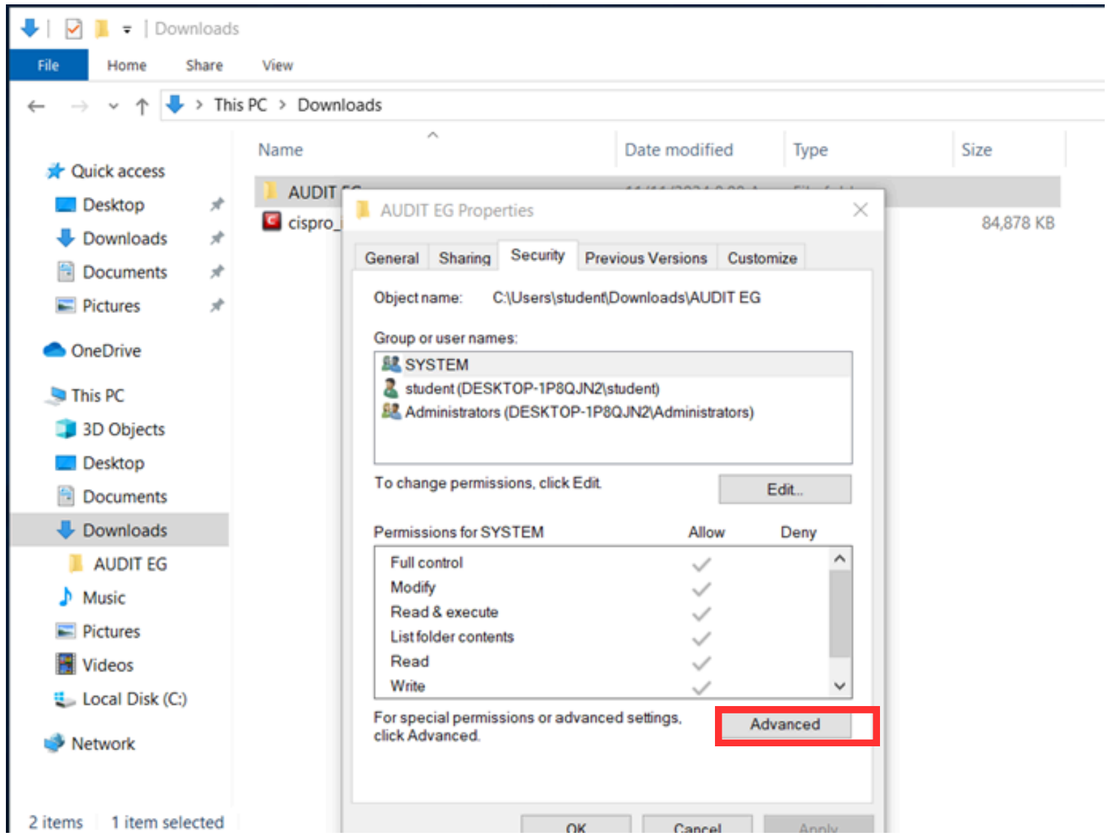


4.On the file you want to audit,right click and select 'Properties' e.g :'AUDIT EG'

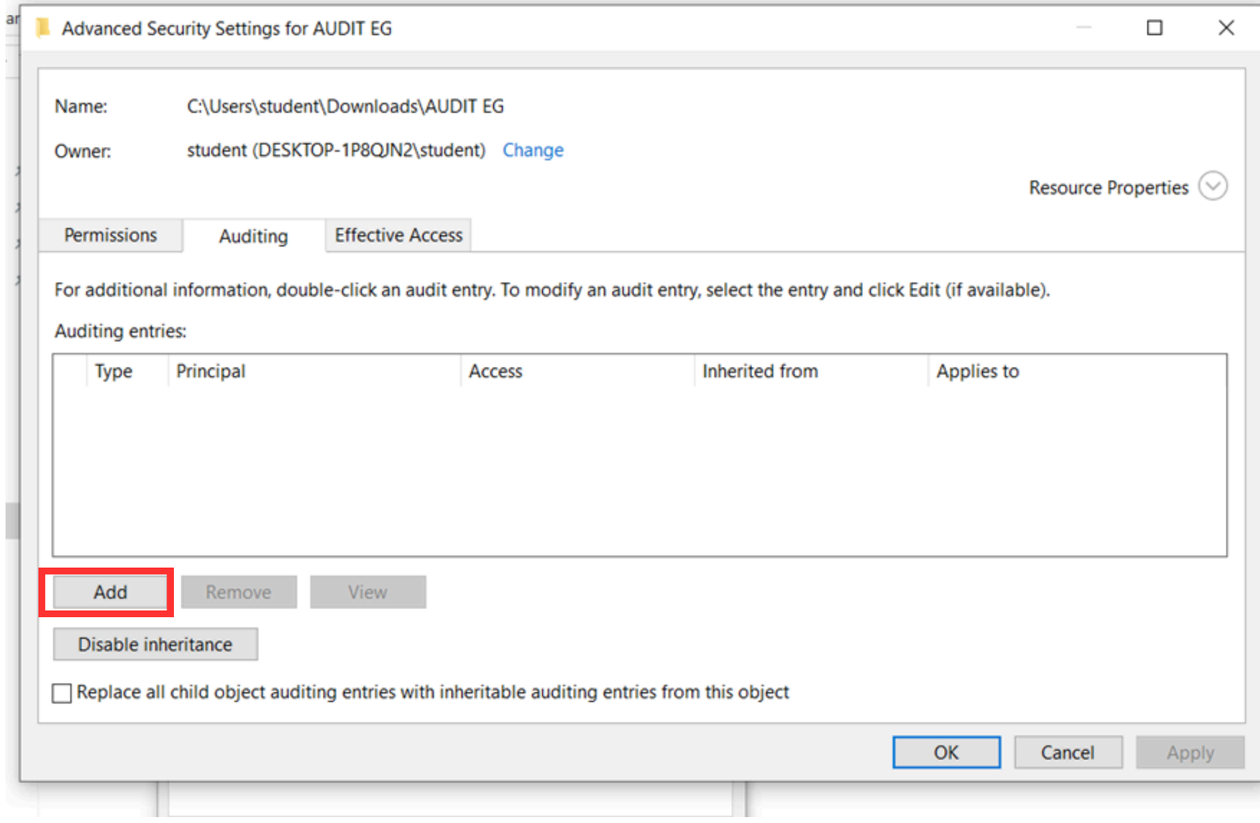


_tasks

5.Go to the Security tab and click ‘Advanced’

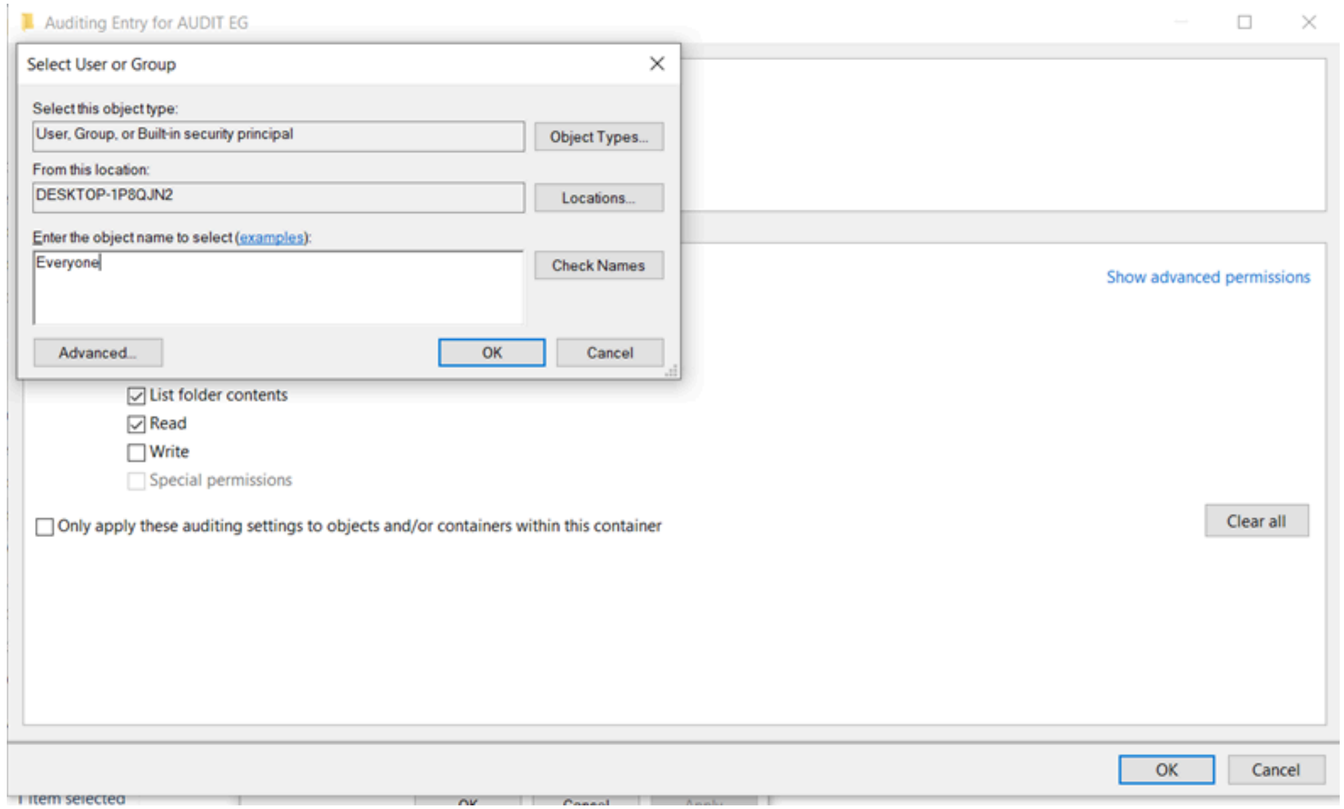


6.Click on Add



_tasks

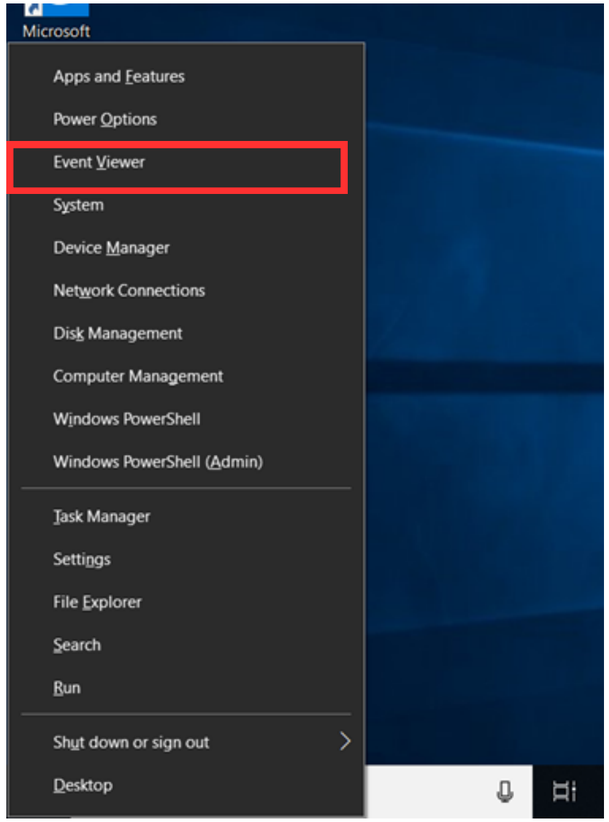
7.Click on ‘Particular groups’,then enter the object as ‘everyone’, click check names, and ok. Tick the boxes you want to audit.E.g-Read, Write and Modify, and Click ok



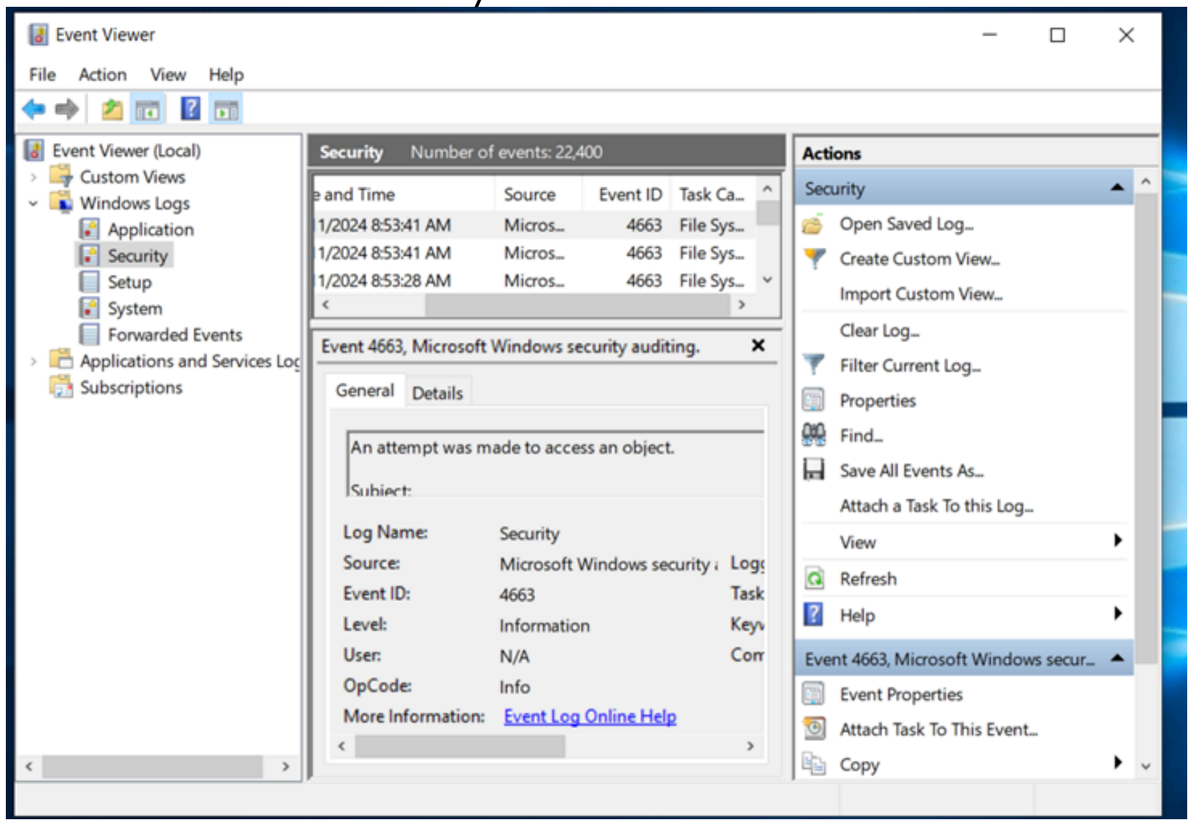
CHECK FOR AUDIT

_tasks

1.Press Win + X and select Event Viewer



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 protecti  n 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

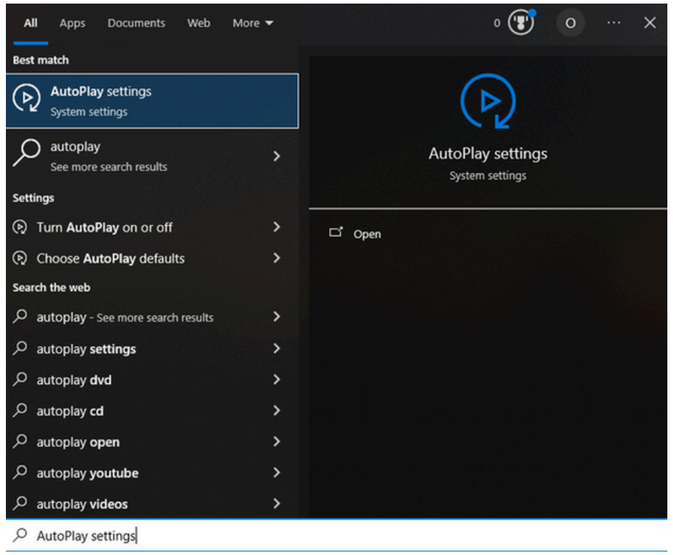
additional tasks

device protection and malware stuff

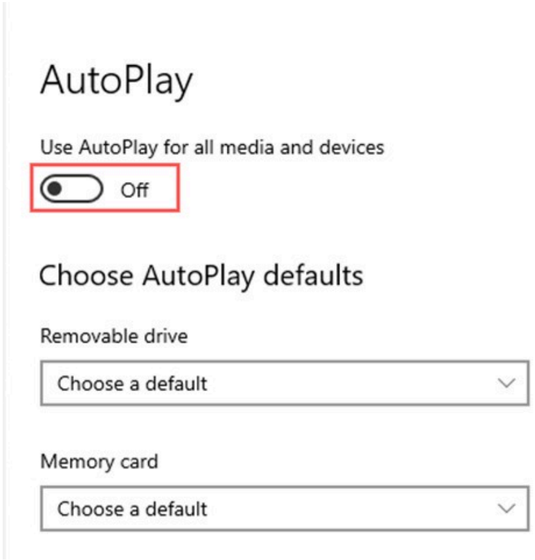
_tasks

(12) Disable Autorun and Boot from USB

1. Search for AutoPlay Settings and press Enter



2. Toggle Off AutoPlay

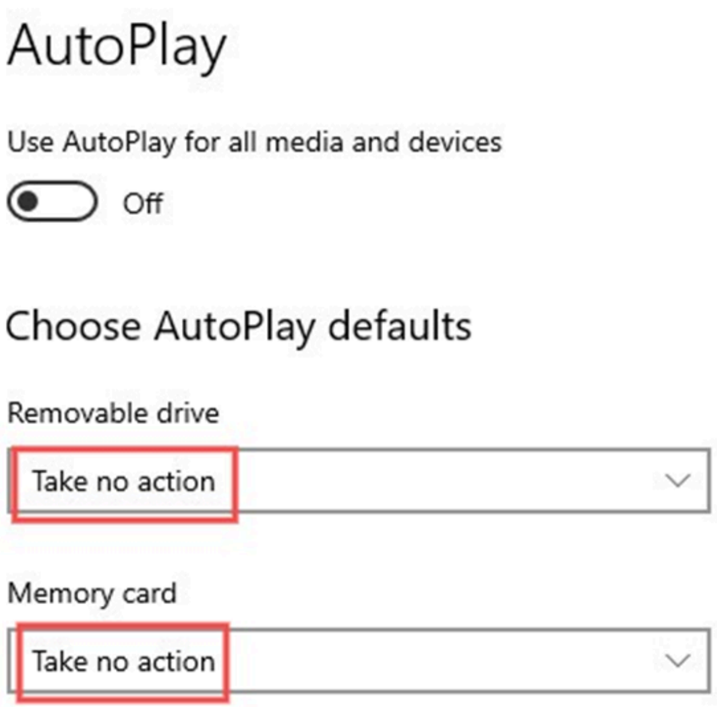


device protection and malware stuff

_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’

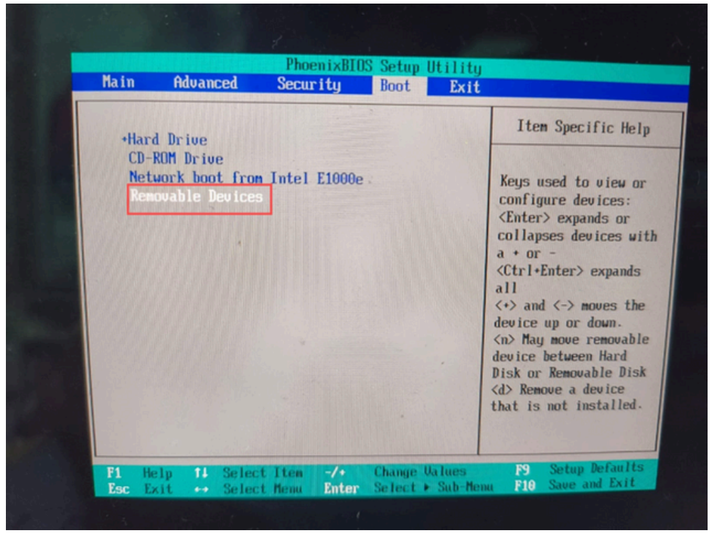


device protection and malware stuff

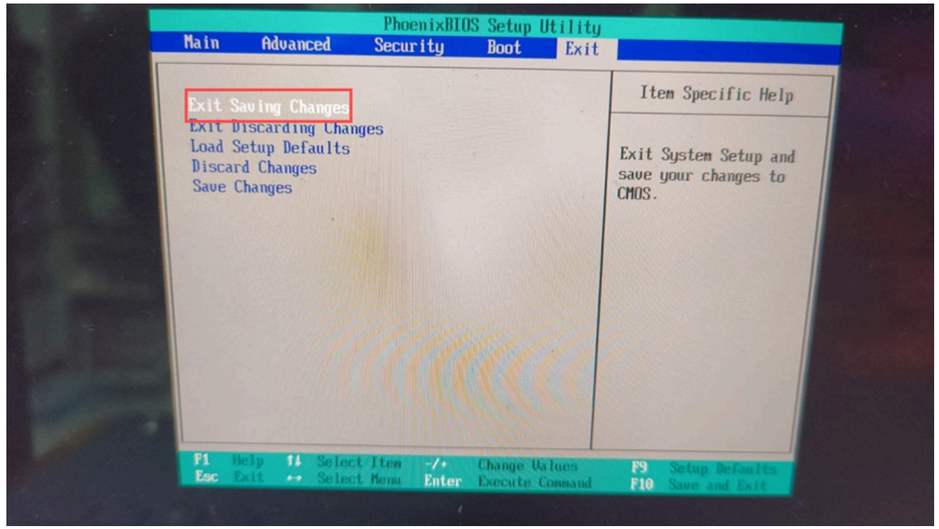
_tasks

(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

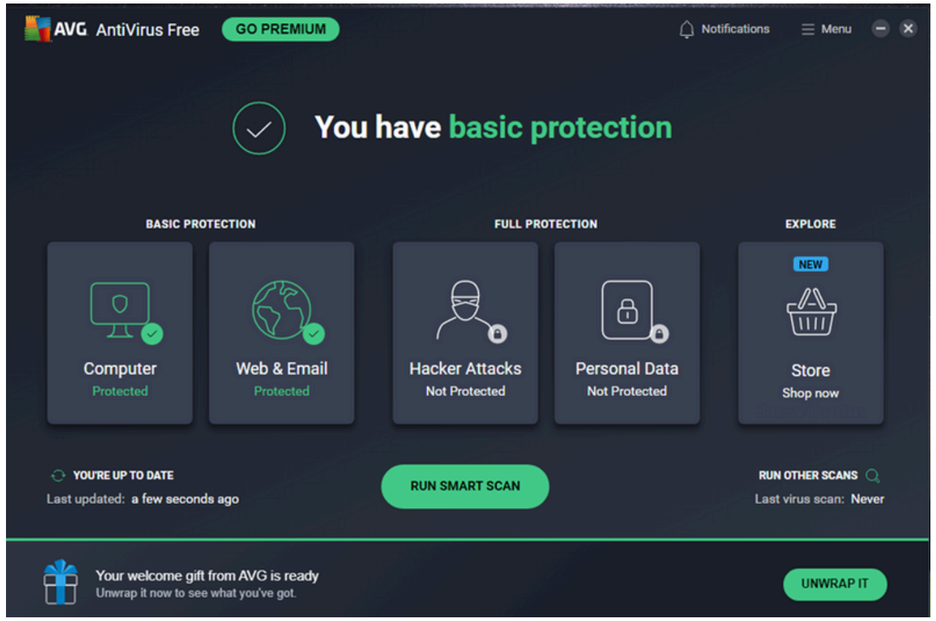
_tasks

(13) Install antivirus software and updates

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

device protection and malware stuff

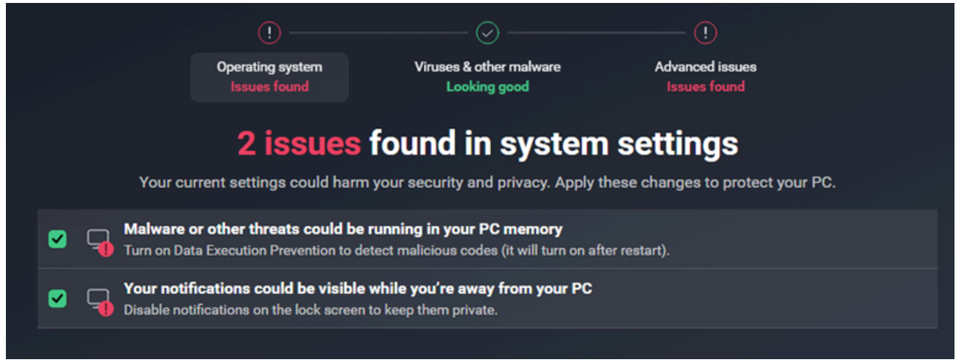
2. Launch AVG > follow through with the initial setup > Run a Smart Scan



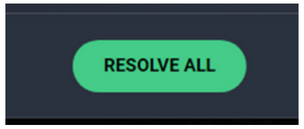
_tasks

(13) Install antivirus software and updates

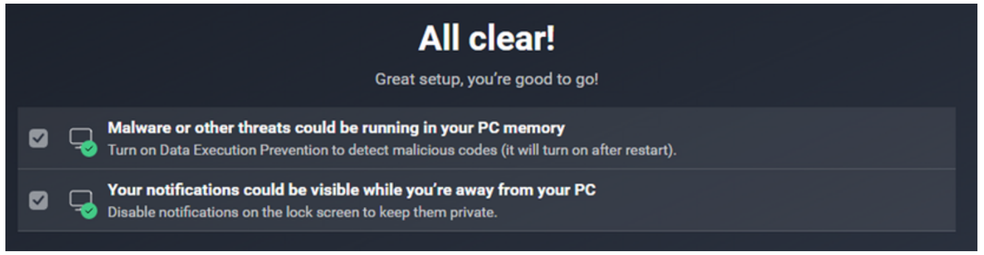
3. If there are issues found with your system
 > Review them to check if needed



Click Resolve All to fix the detected issues



Once okay, you will see the following message:

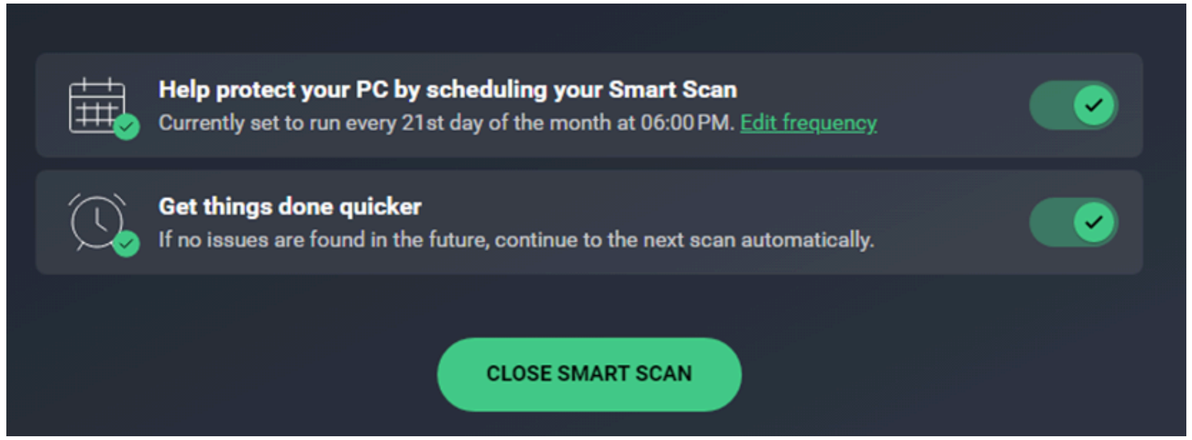


device protection and malware stuff

_tasks

(13) Install antivirus software and updates

Here are some additional settings to enable if automation is preferred

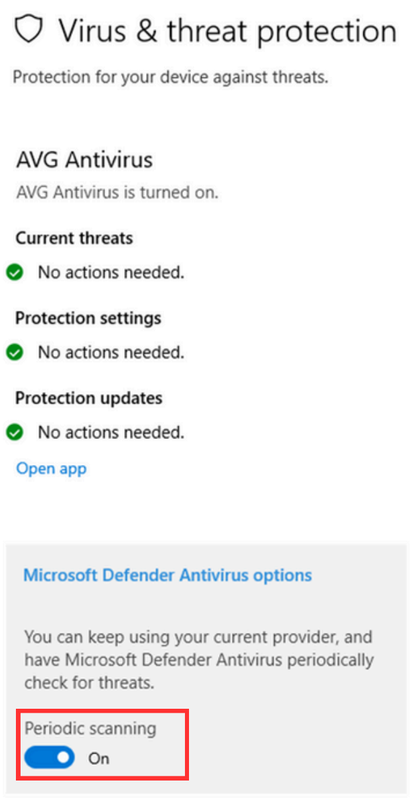


device protection and malware stuff

_tasks

(13) Install antivirus software and updates

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

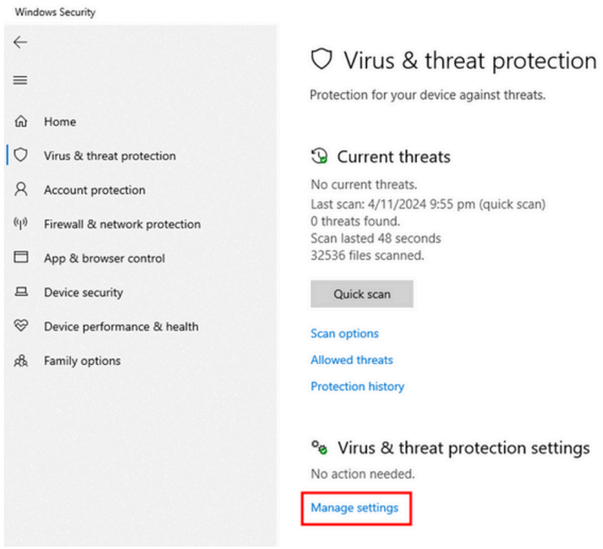


device protection and malware stuff

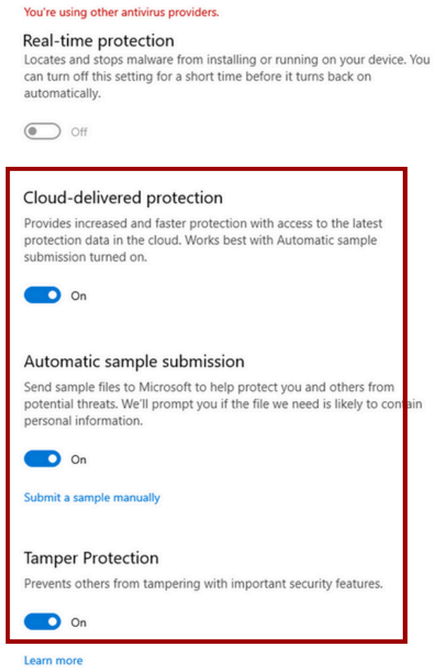
_tasks

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

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



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

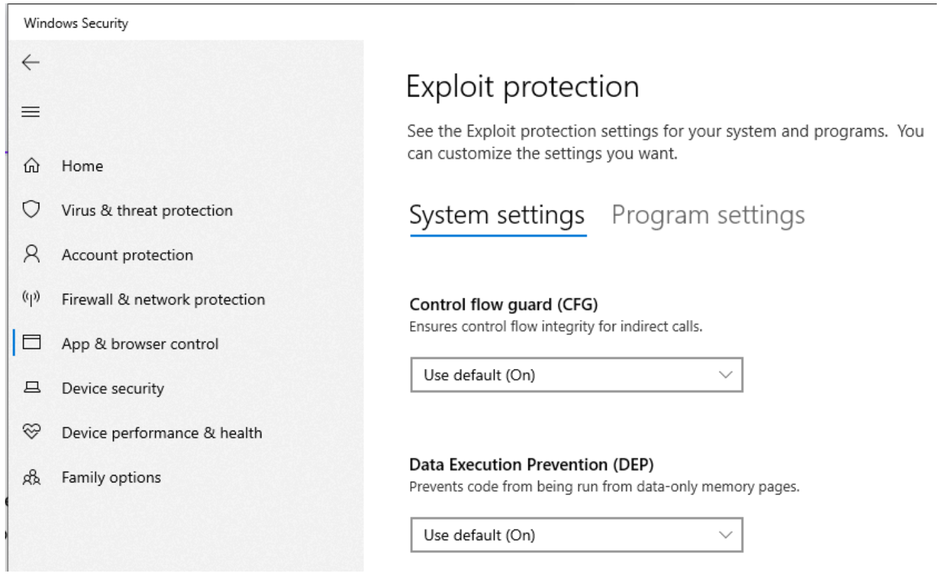


device protection and malware stuff

_tasks

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

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

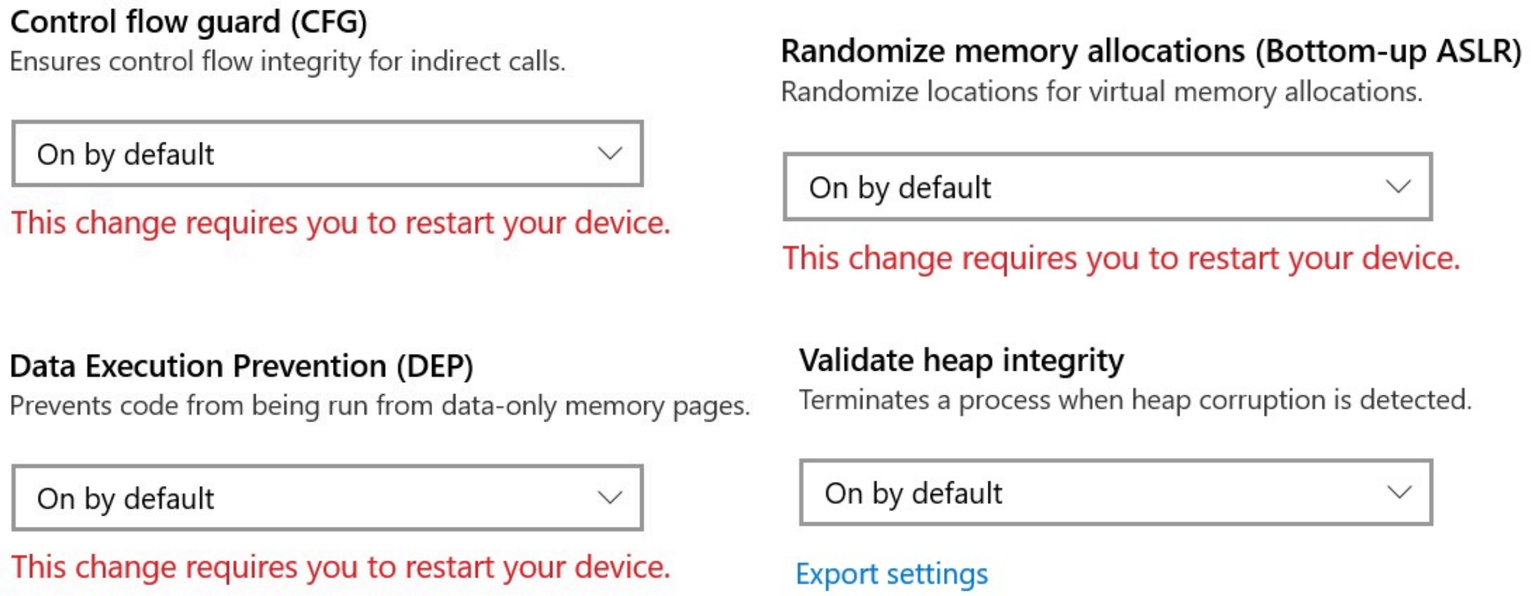


device protection and malware stuff

_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



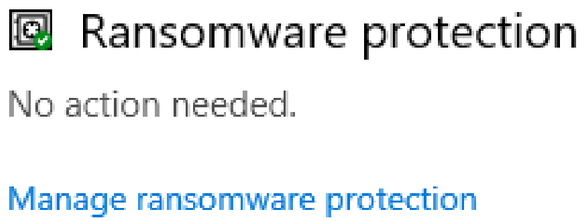
device protection and malware stuff

_tasks

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

,

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



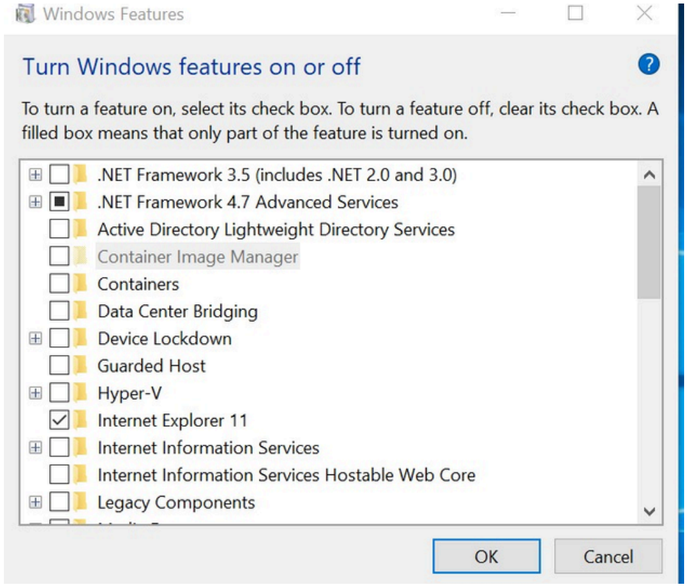
4. Turn on ‘Controlled folder access

device protection and malware stuff

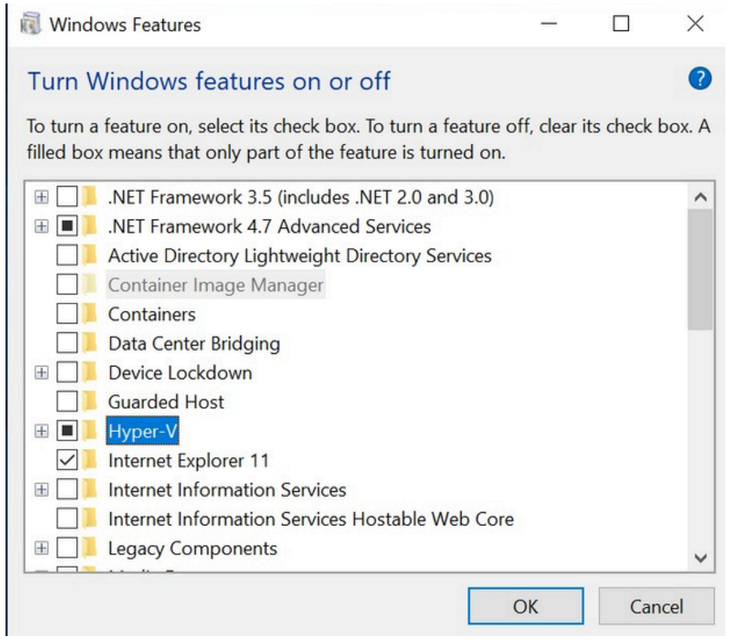
_tasks

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

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



2. Tick the checkbox next to Hyper-V

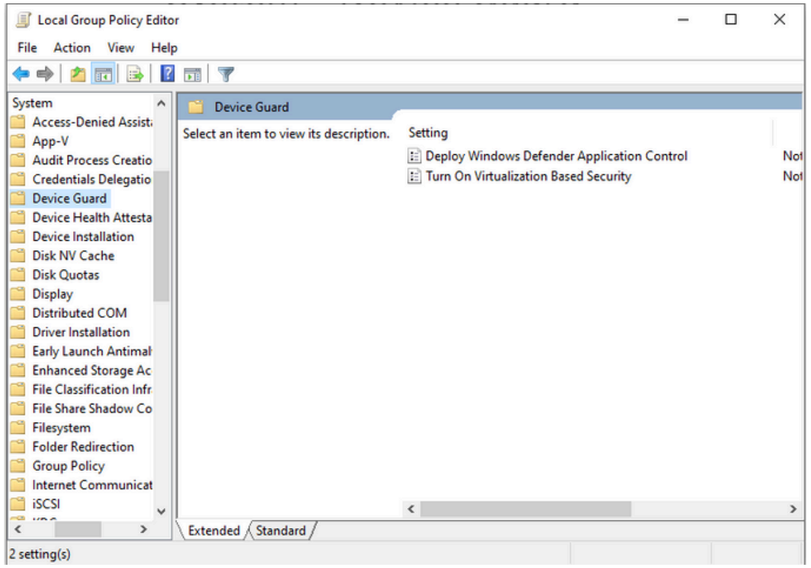


device protection and malware stuff

_tasks

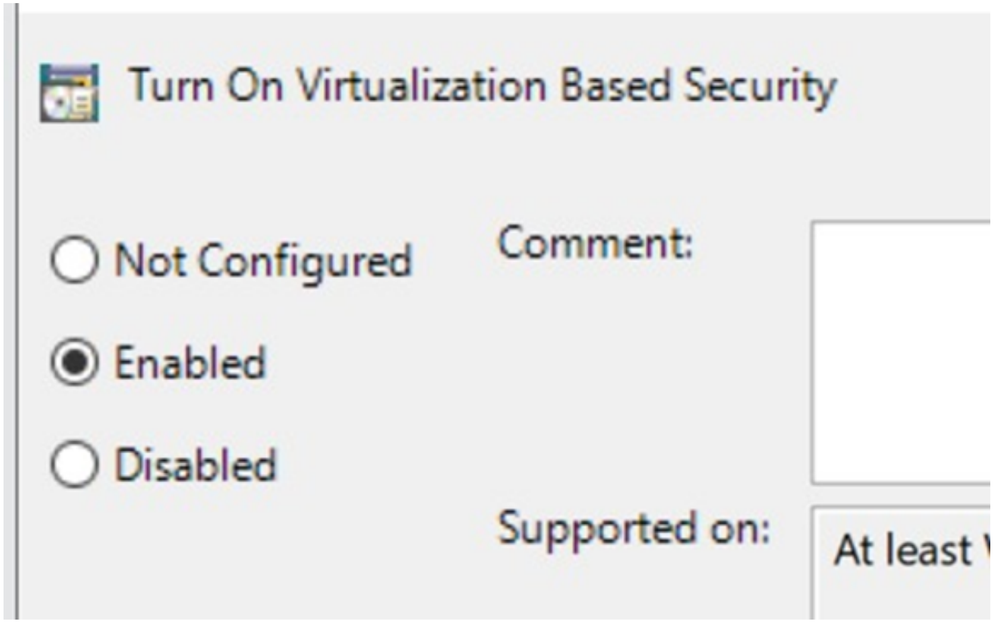
(20) Maximize or Enhance Windows Defender Features (Credential Guard)

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



device protection and malware stuff

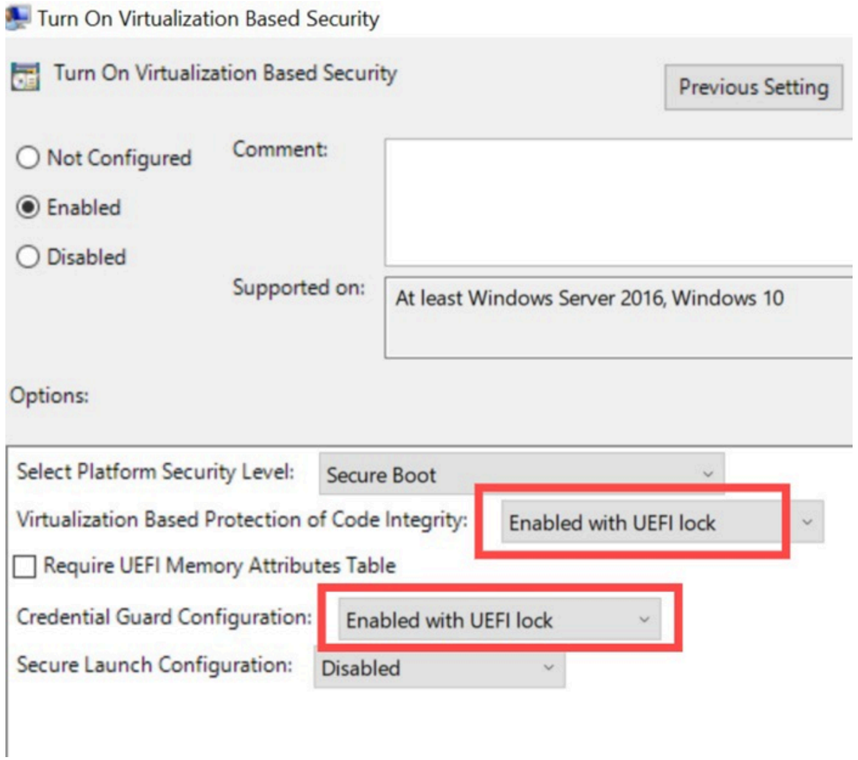
2. Double Click ‘Turn On Virtualization Based Security’ and set it to enabled



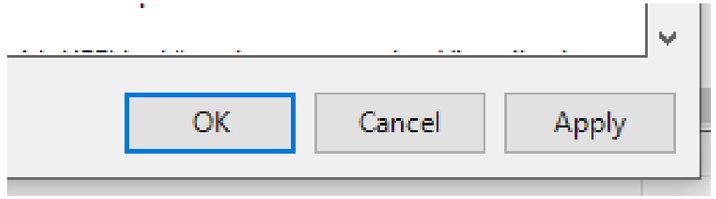
_tasks

(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



Press Apply then OK



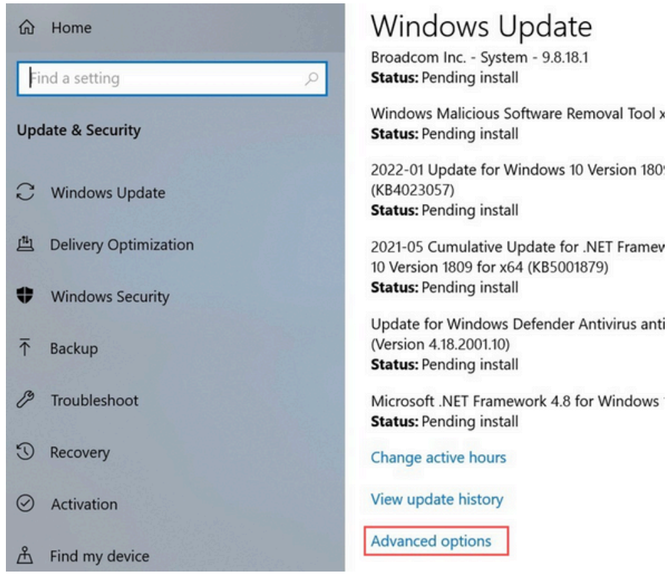
Then Restart for it to take action

device protection and malware stuff

_tasks

(17) Enable Auto Updates

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



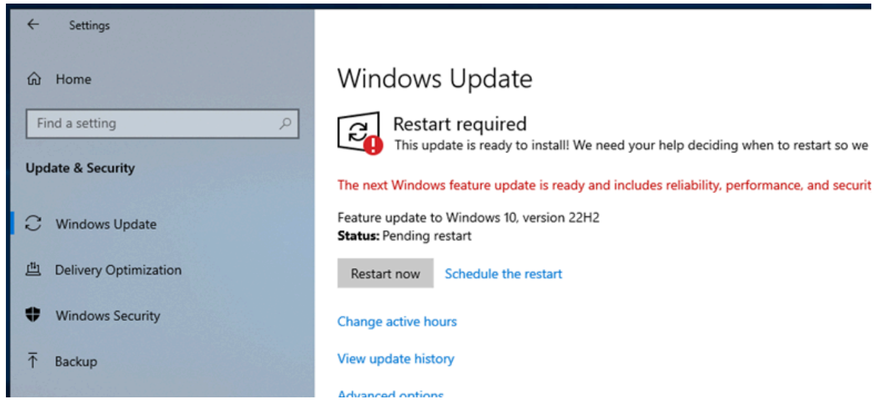
2. Toggle on ‘Give me updates’ and ‘Automatically download updates’

device protection and malware stuff

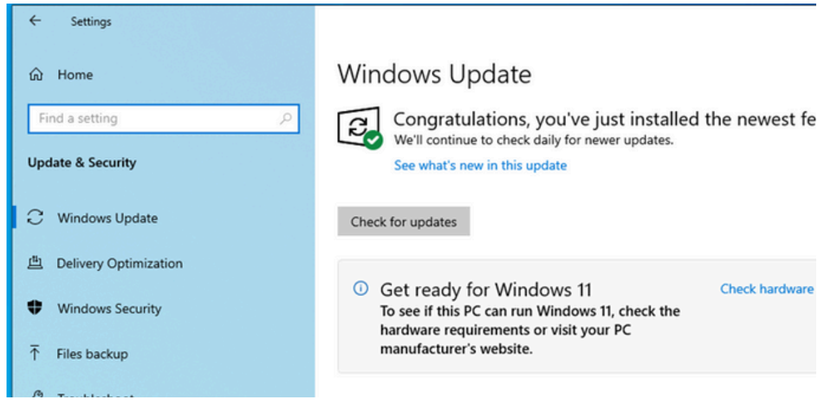
_tasks

(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

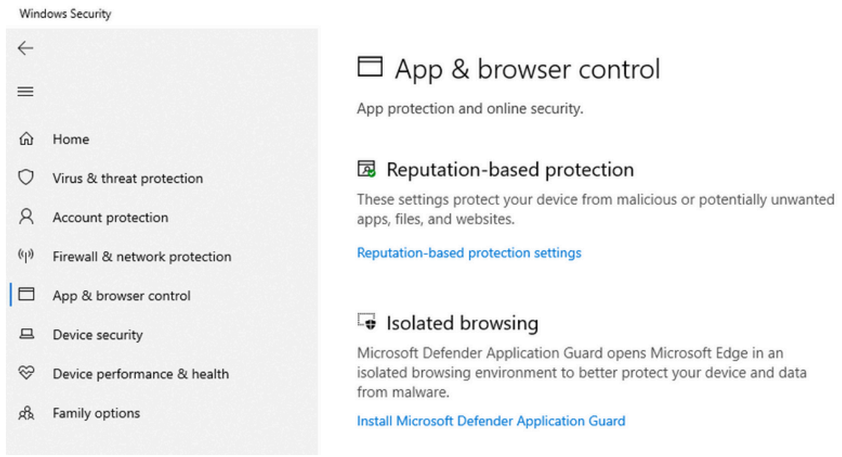


device protection and malware stuff

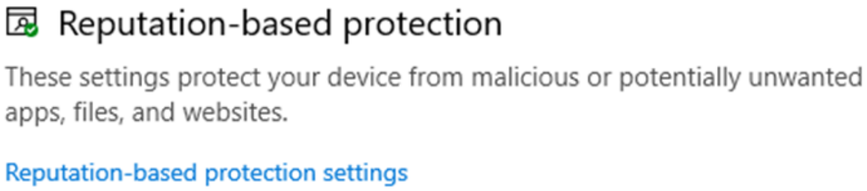
_tasks

(21) Enable Microsoft SmartScreen

1. Visit Windows Security > App & browser control



2. Click on Reputation-based protection settings

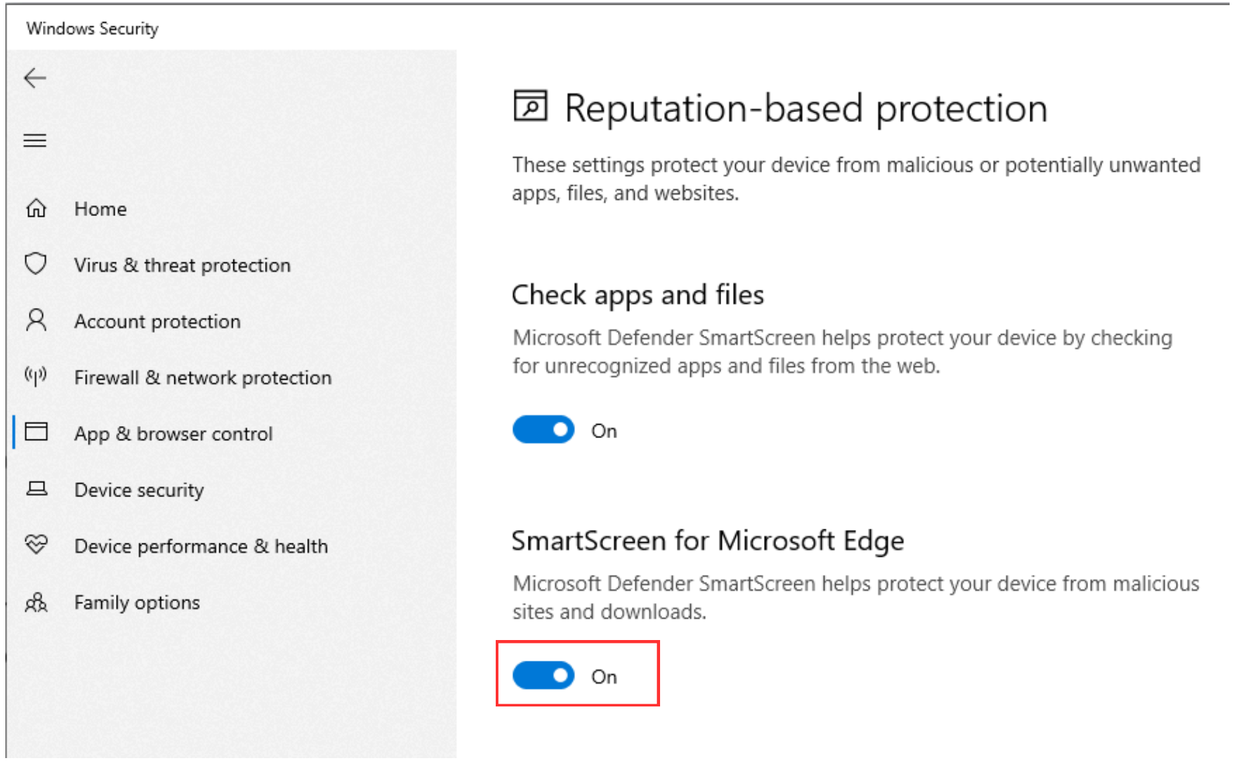


device protection and malware stuff

_tasks

(21) Enable Microsoft SmartScreen

3. Make sure SmartScreen for Microsoft Edge is enabled

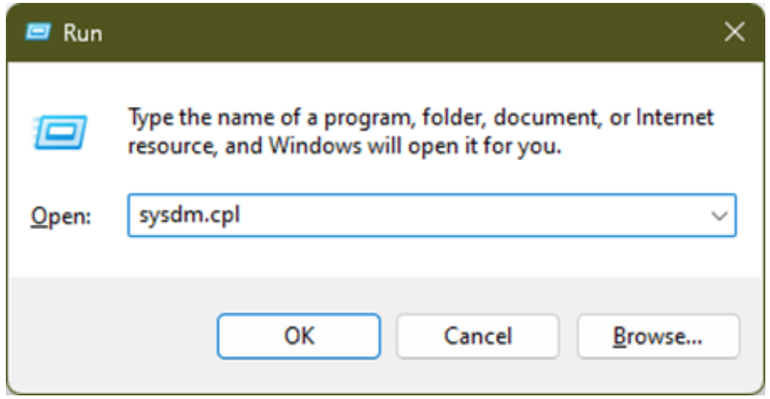


device protection and malware stuff

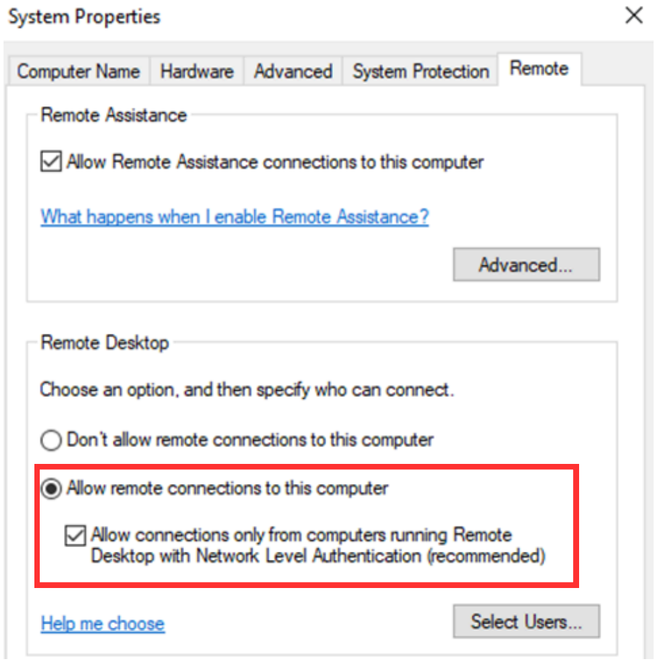
_tasks

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

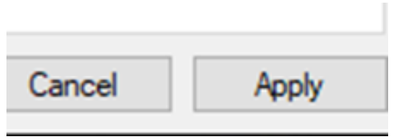
1. Open System Properties, Win + R > sysdm.cpl > OK



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



Press Apply to save changes

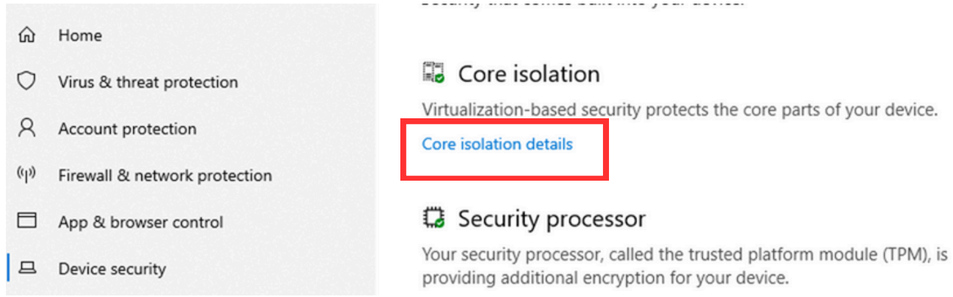


device protection and malware stuff

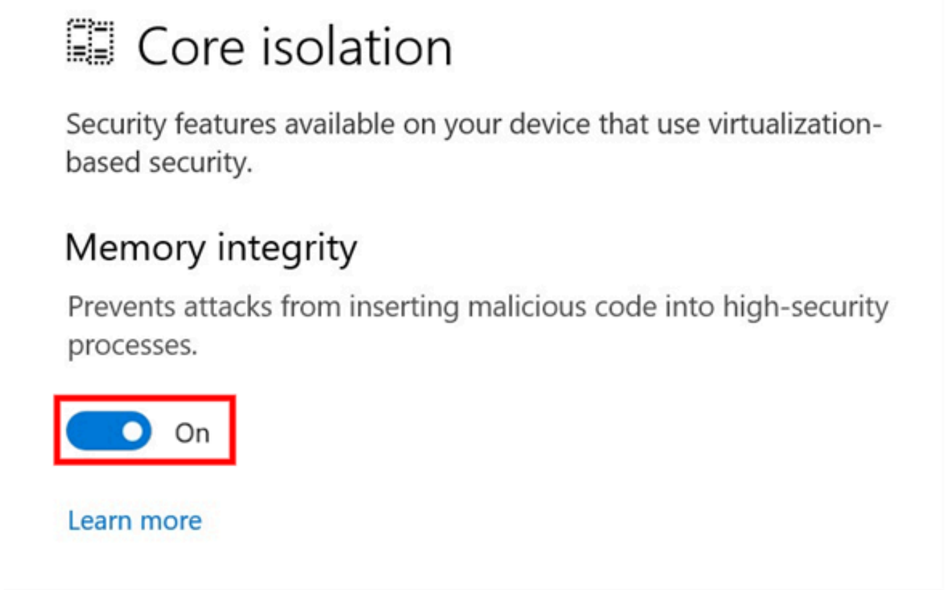
_tasks

(37) Enabling Memory Integrity

1. Windows Security > Device Security > Core Isolation Details



2. Switch on ‘Memory integrity’ then restart.

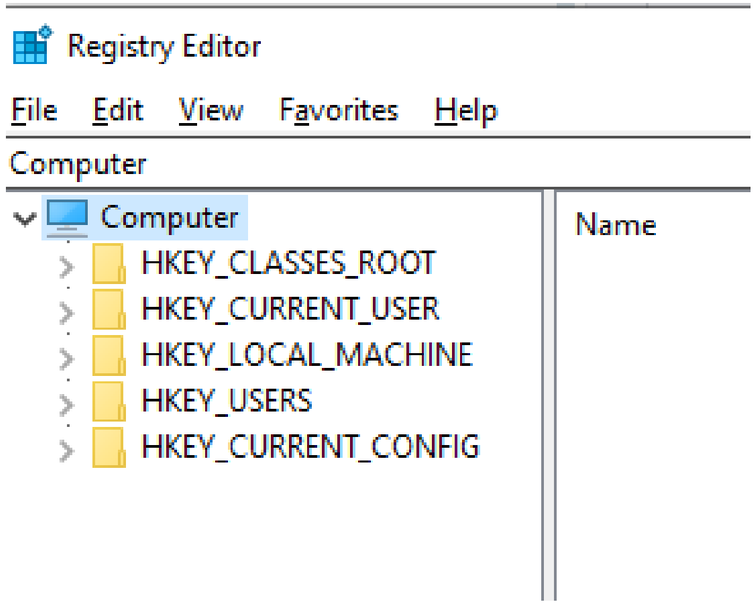


device protection and malware stuff

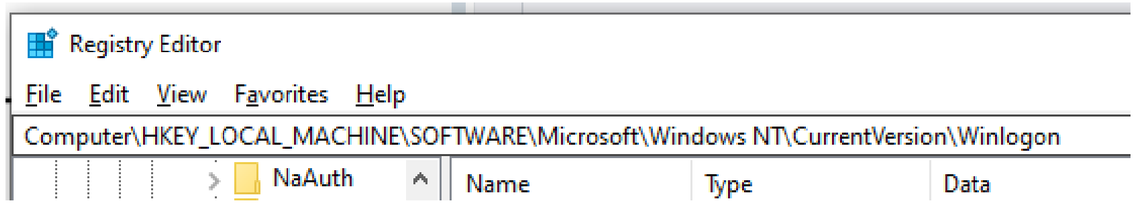
_tasks

(38) Disabling automatic login

1. Open Registry Editor



2. Navigate to this path:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

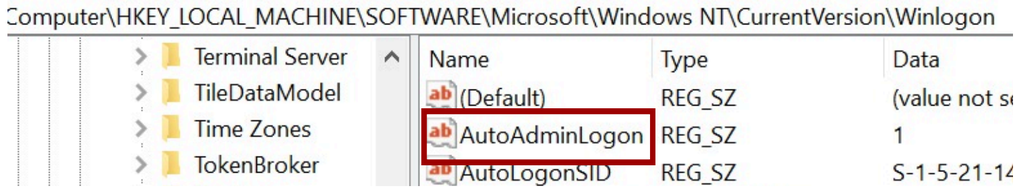


device protection and malware stuff

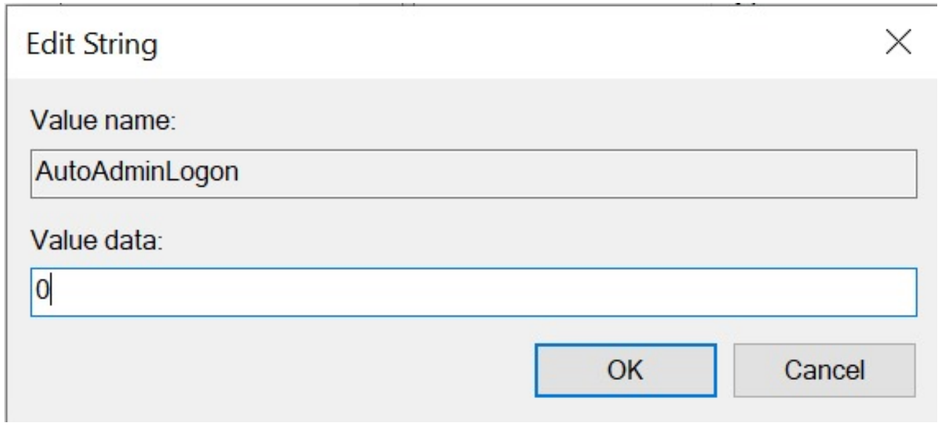
_tasks

(38) Disabling automatic login

3. Double Click on AutoAdminLogon



4. Change the value to 0

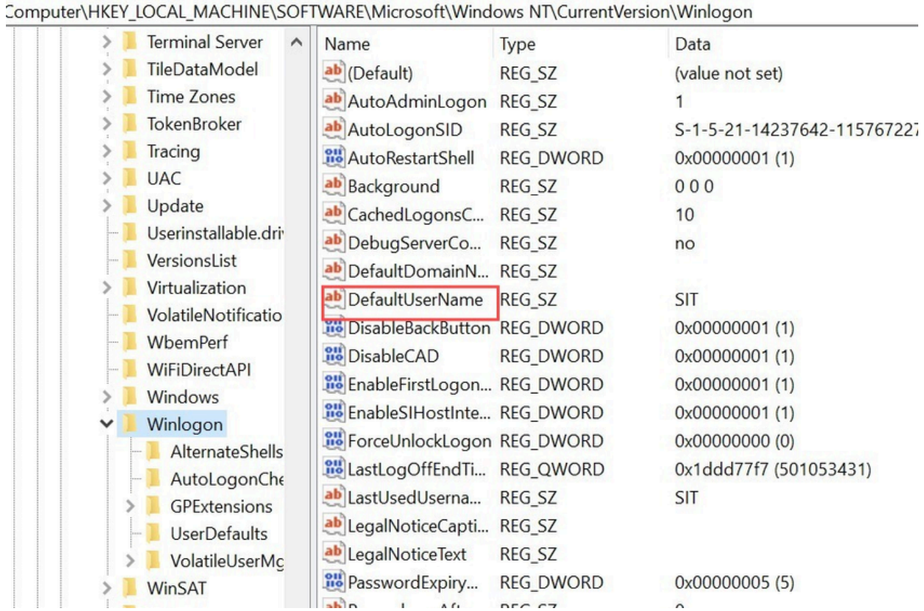


device protection and malware stuff

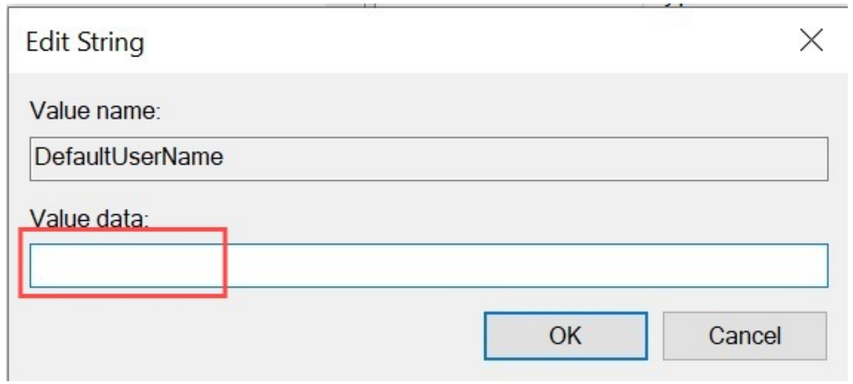
_tasks

(38) Disabling automatic login

5. Double Click on DefaultUserName



6. Clear the value data so that it is blank

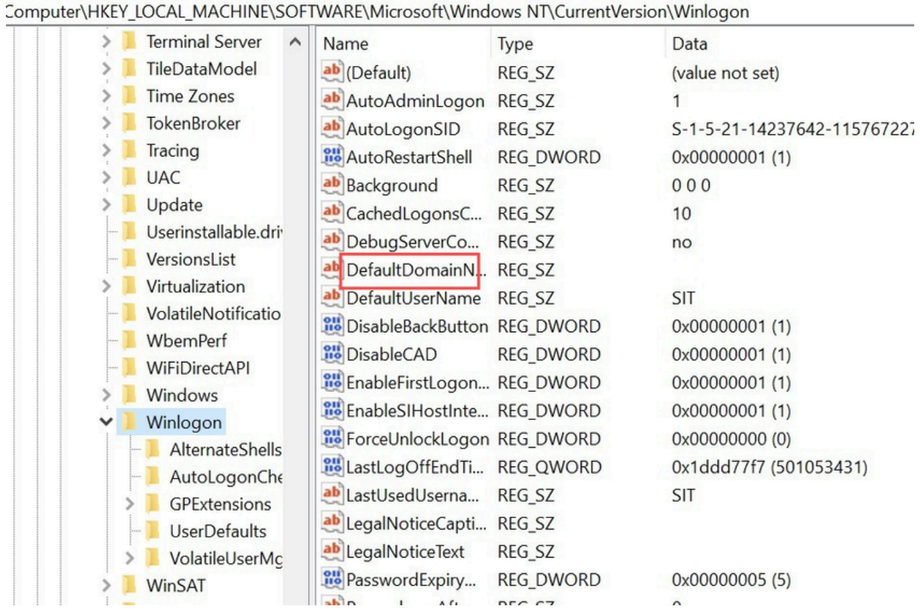


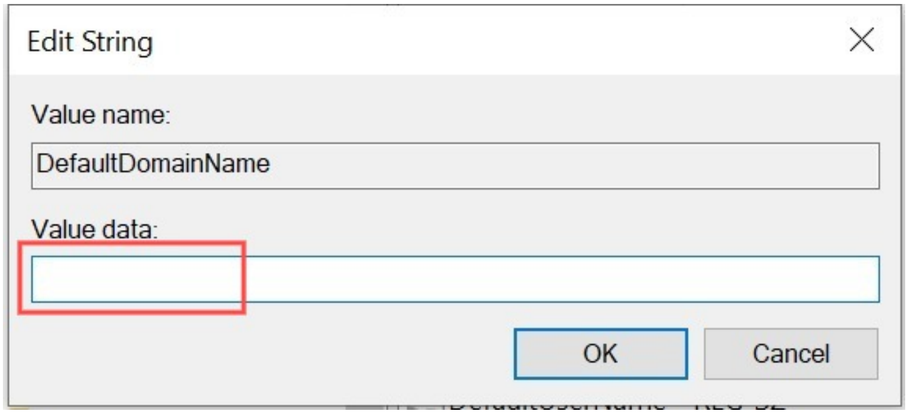
device protection and malware stuff

_tasks

(38) Disabling automatic login

7. Repeat steps 5 & 6 on DefaultDomainName





device protection and malware stuff

_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