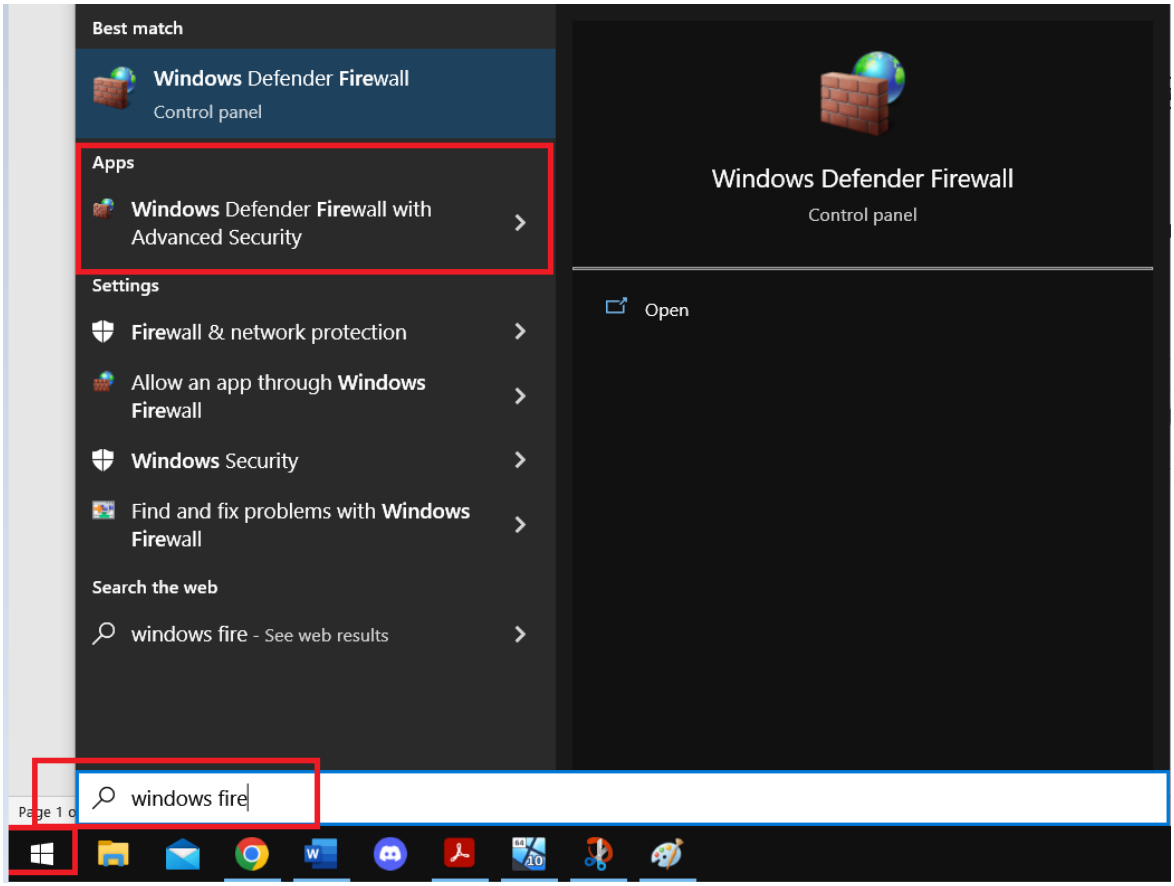
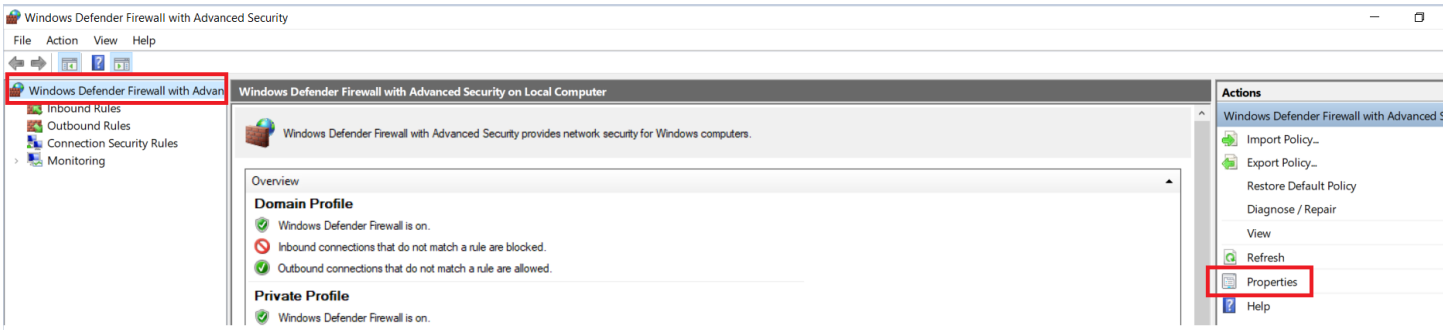
Part 1 – Hardening Windows 10

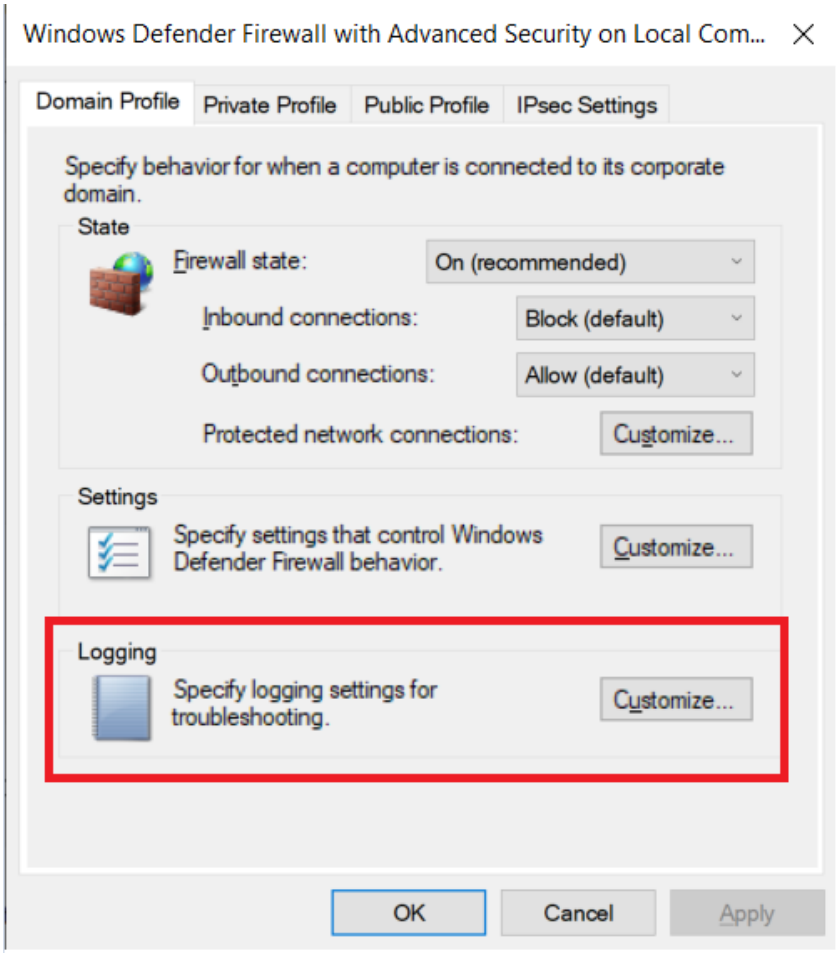
Task #1: Windows Firewall: Logging Dropped Packets

The first task in hardening Windows 10 is to log any dropped packets within our system. To do this, we must do the following: Start ⊞ > type in “windows defender advanced threat protection” (then open it) > Click to target local computer (left column) > Properties (right column)

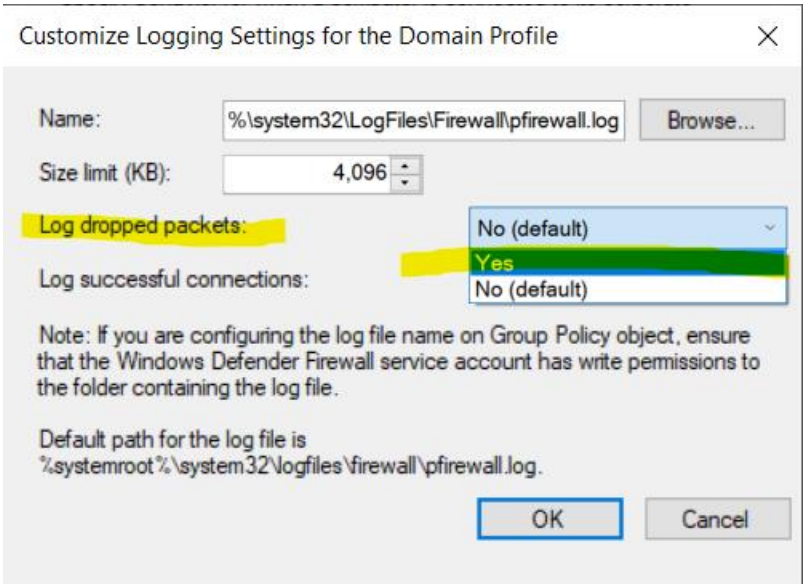




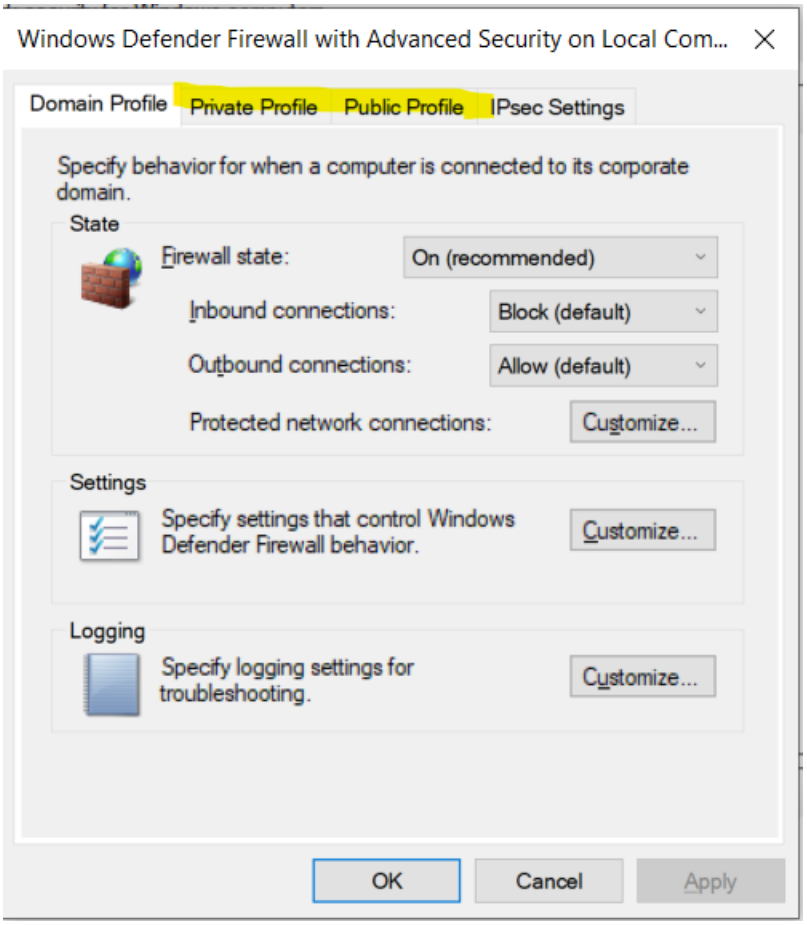
Now under the tab “Domain Profile” look at the subheading “Logging” down below then click “customize”



Finally, change “log dropped packets” from “No” to “Yes”

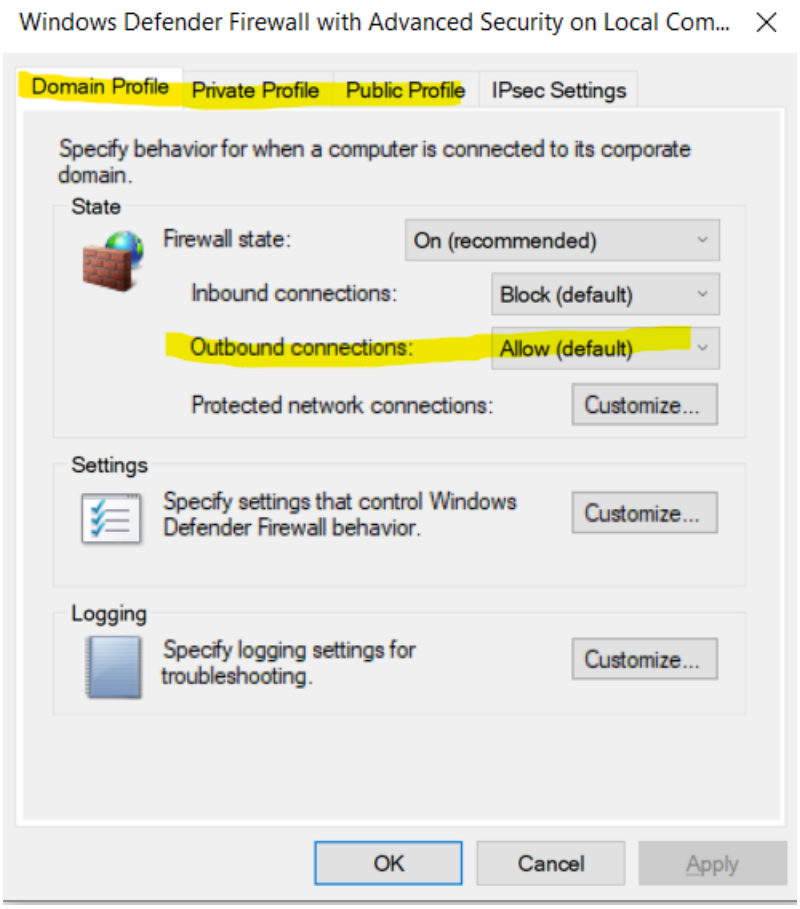


Once completed, do this for the Private and Public Profiles.

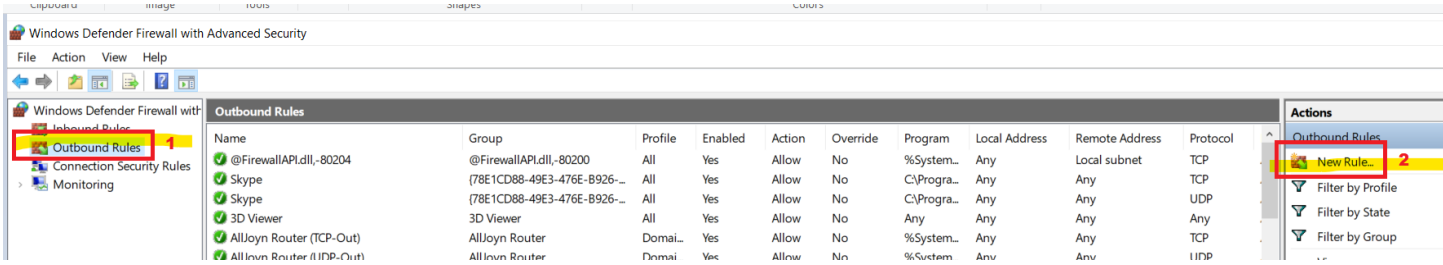


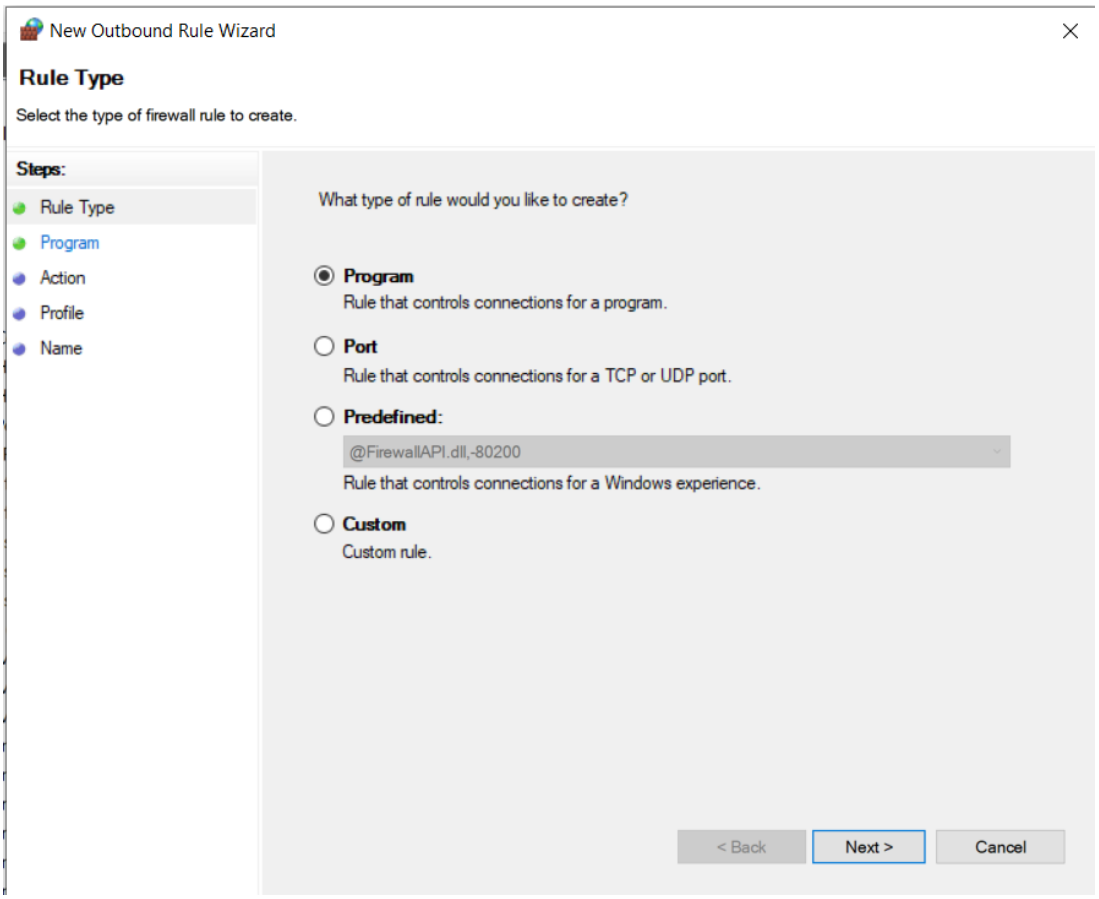
Blocking Outbound Connections

Our next objective is to block any outbound connections as this would enforce a stronger security system especially for office workers. For each profile as aforementioned, change from “Allow” to “Deny”



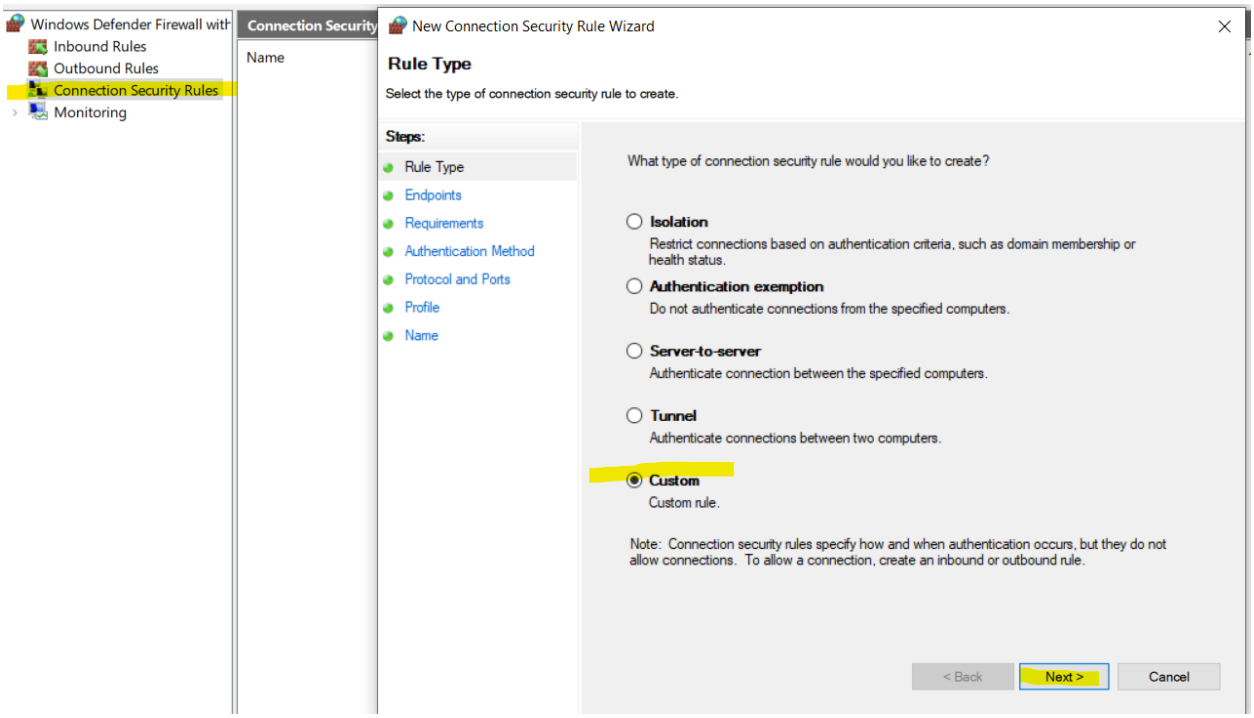
This will block **ALL** outbound connections. In order to allow users to establish a specific connection, we must then add it to the allowlist. This will inherently apply the Principle of least privilege philosophy. To add it back to the allow list we do the following: Outbound Rules (left column) > New Rule (right column) > select the type of rule you want to implement.



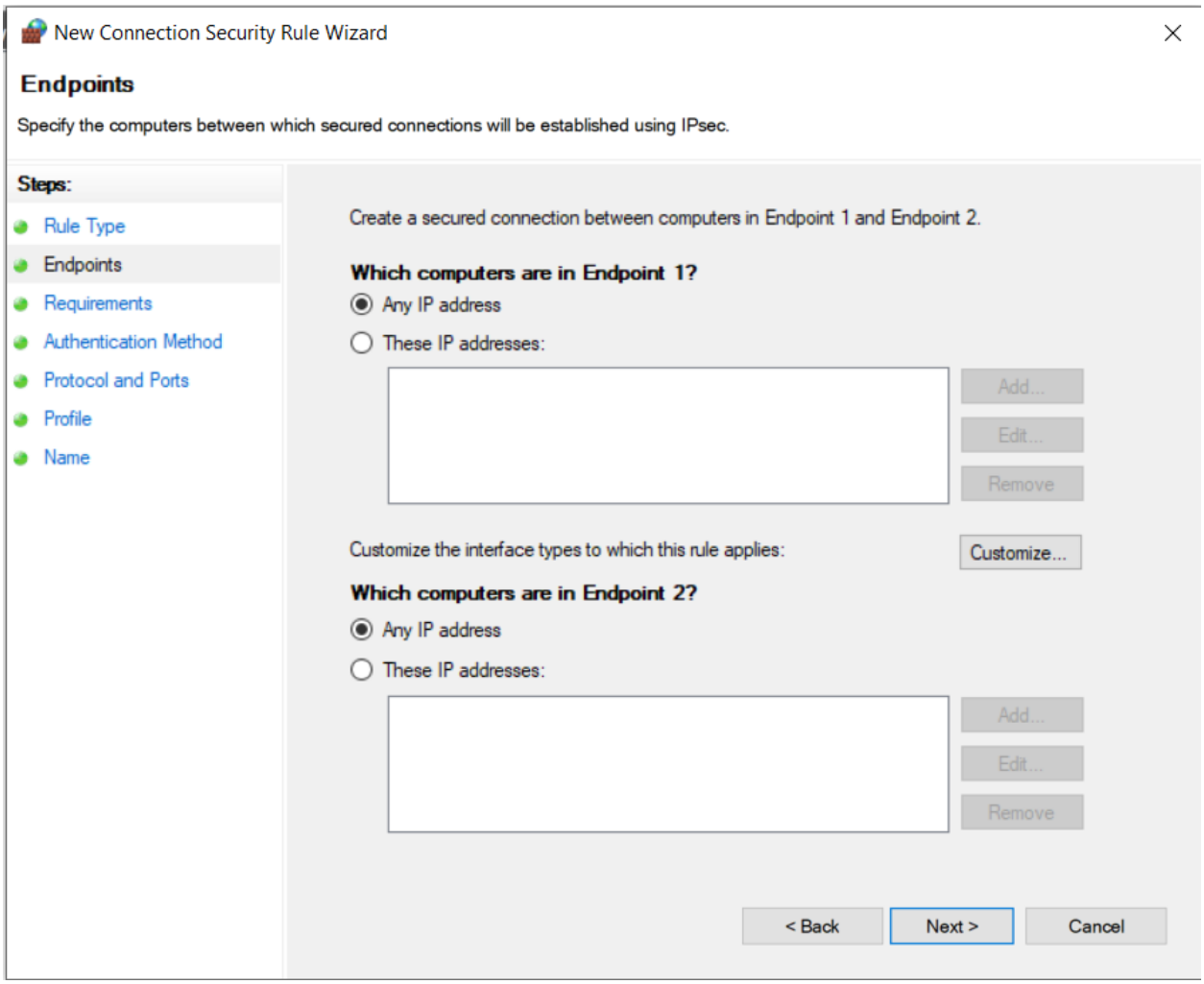


Protecting vulnerable protocols

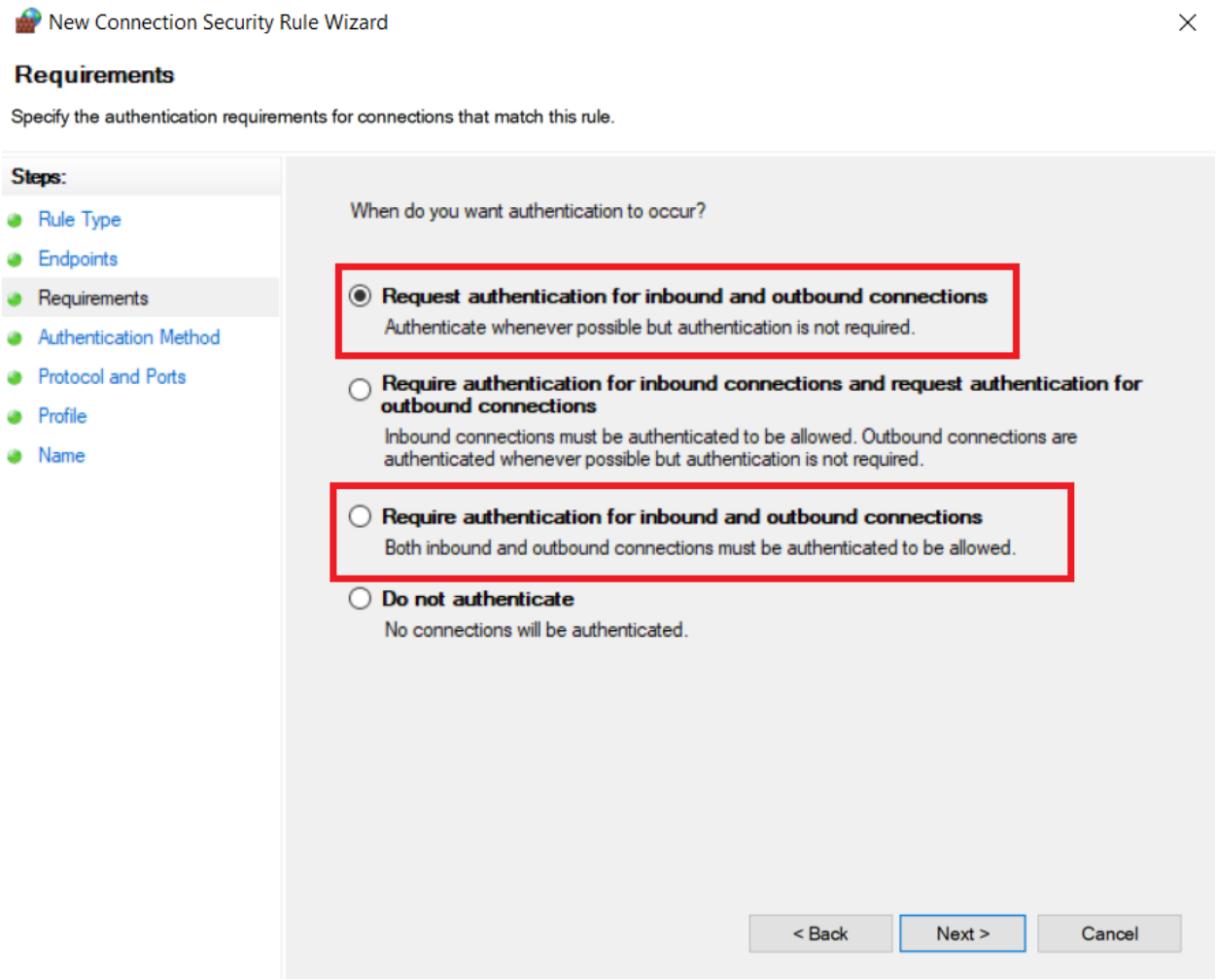
In this section, we will look on how to secure some ports that are vulnerable to attacks such as but not limited to NetBIOS, RDP, WinRM, etc. In order to do this, we do the following:



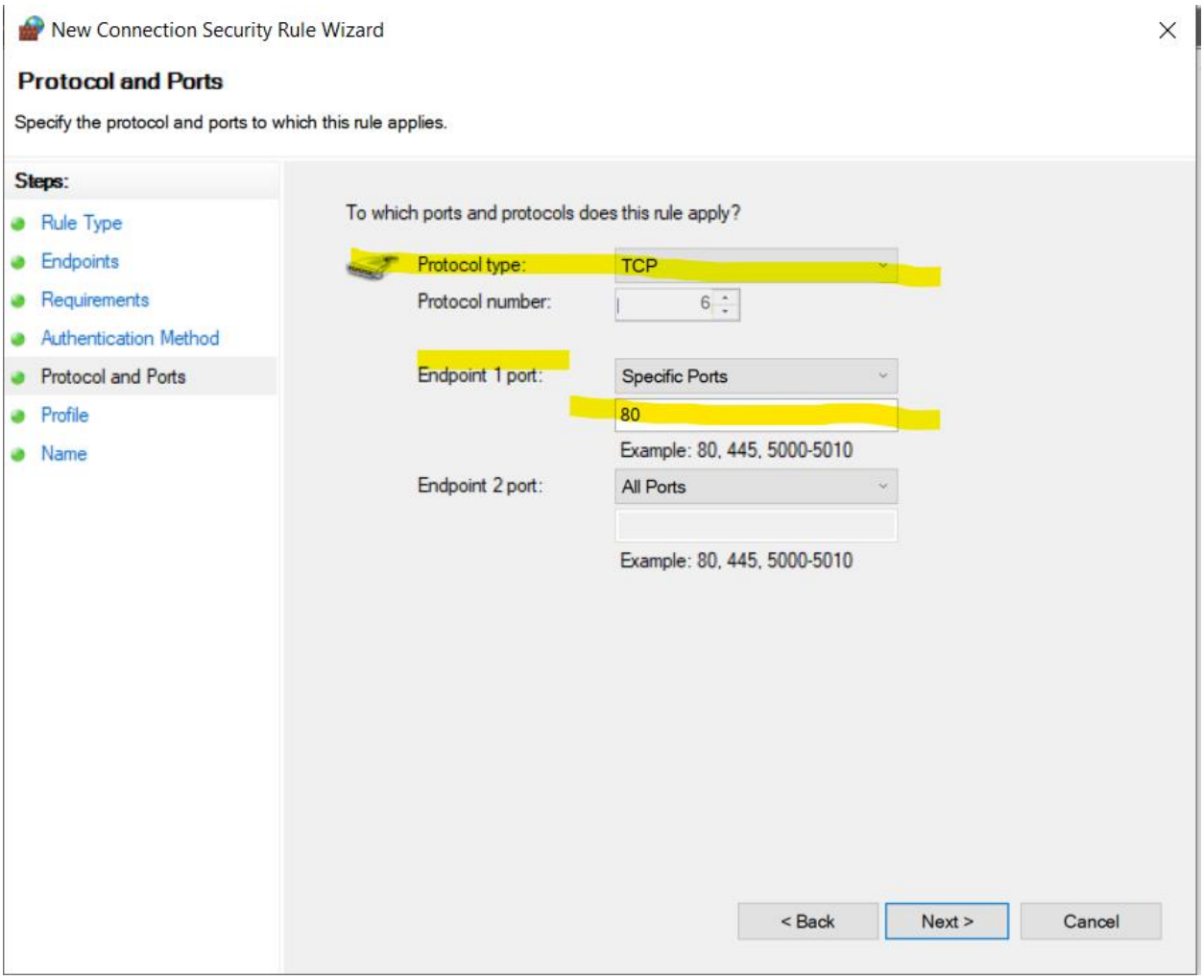
(Connection Security Rules > Custom Rule > Next)



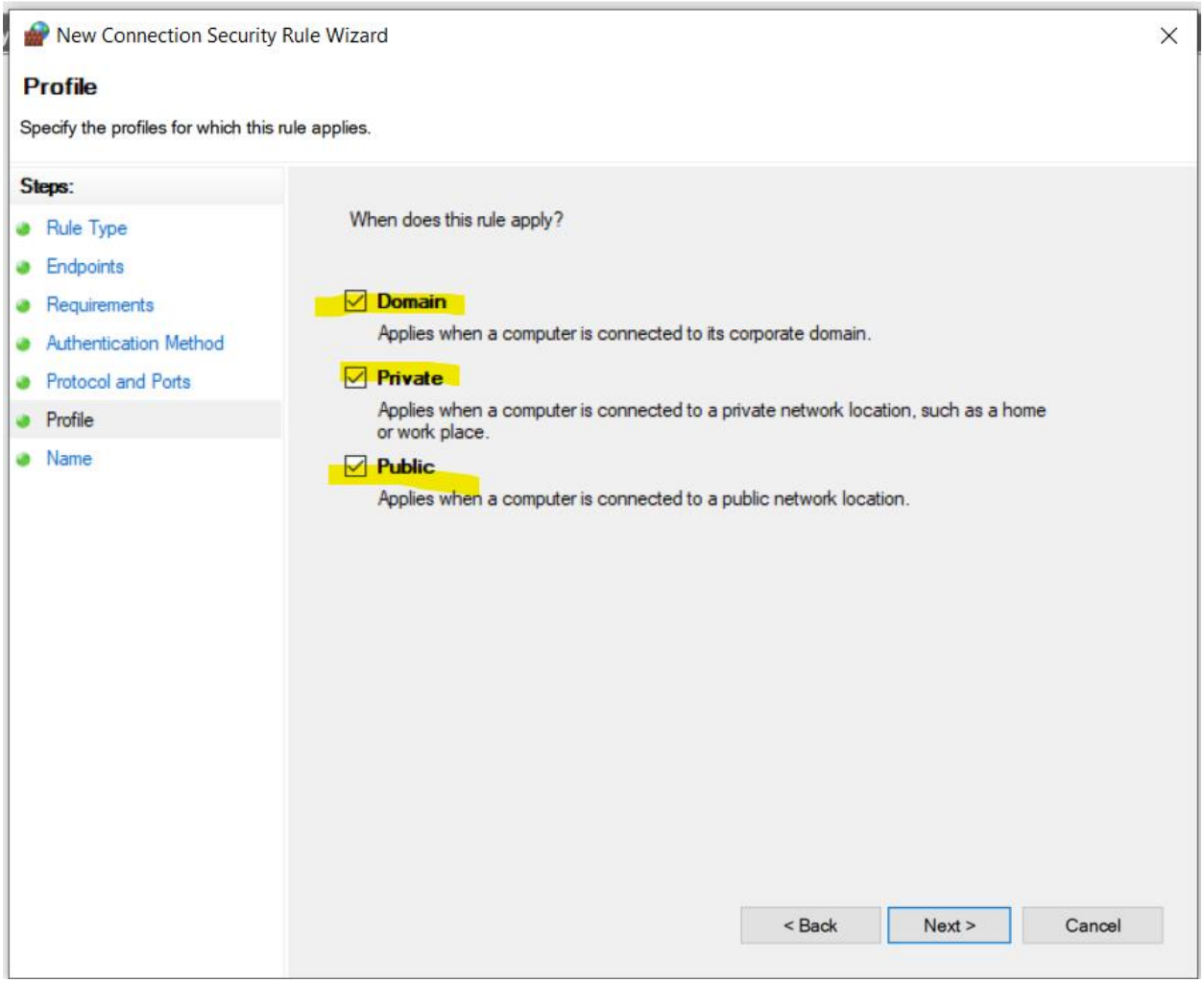
(Select endpoint 1 & endpoint 2 IP address (if there is any))



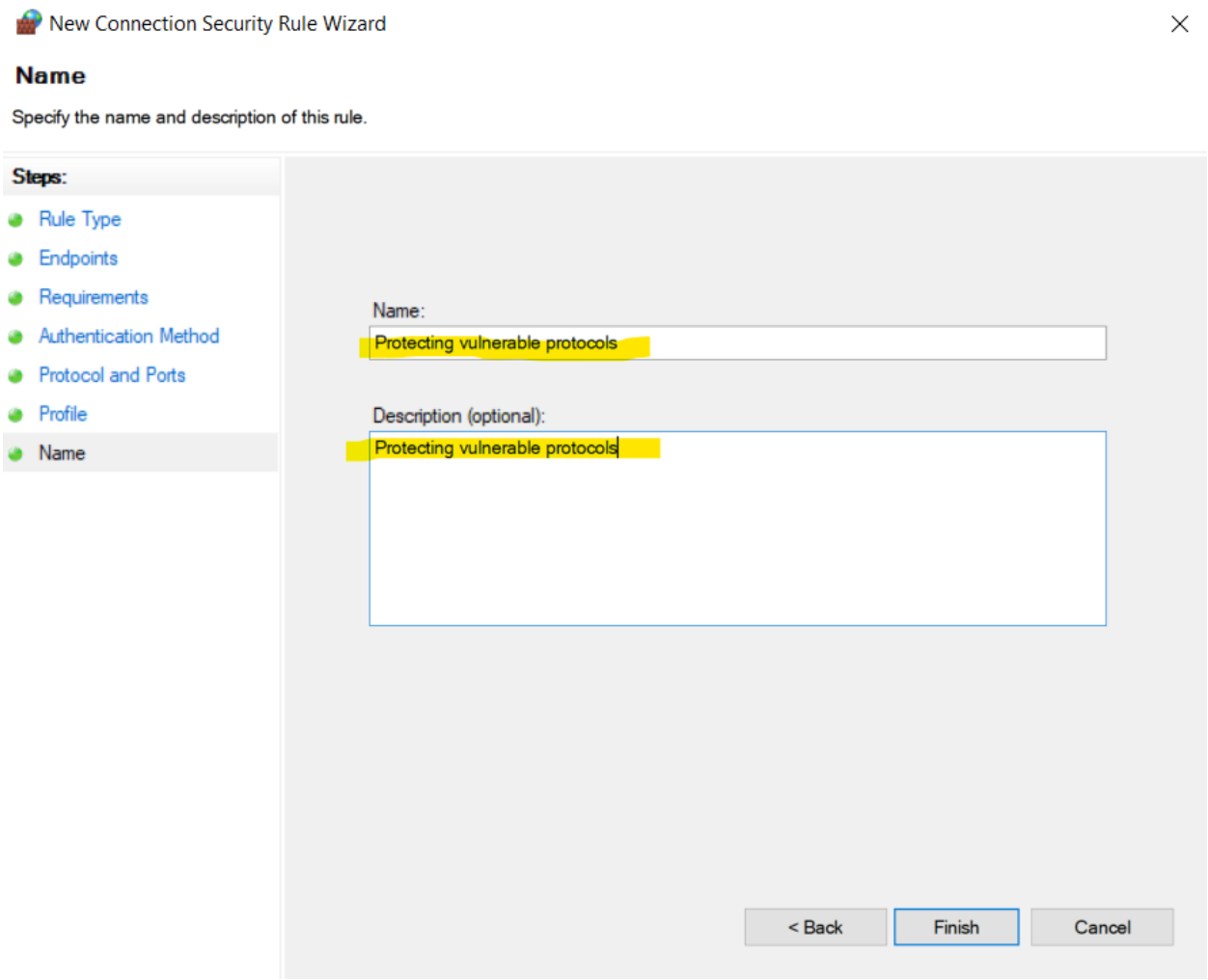
(in requirement section, you can pick either “Request authentication for inbound and outbound connections” or “Require authentication for inbound and outbound connections” as these two are the most secure options Then, select “Computer and User [Kerberos V5] as this restricts connections dependent on user profiles.)



(Then select the specific ports you want (In the example, port 80 for TCP is selected).)



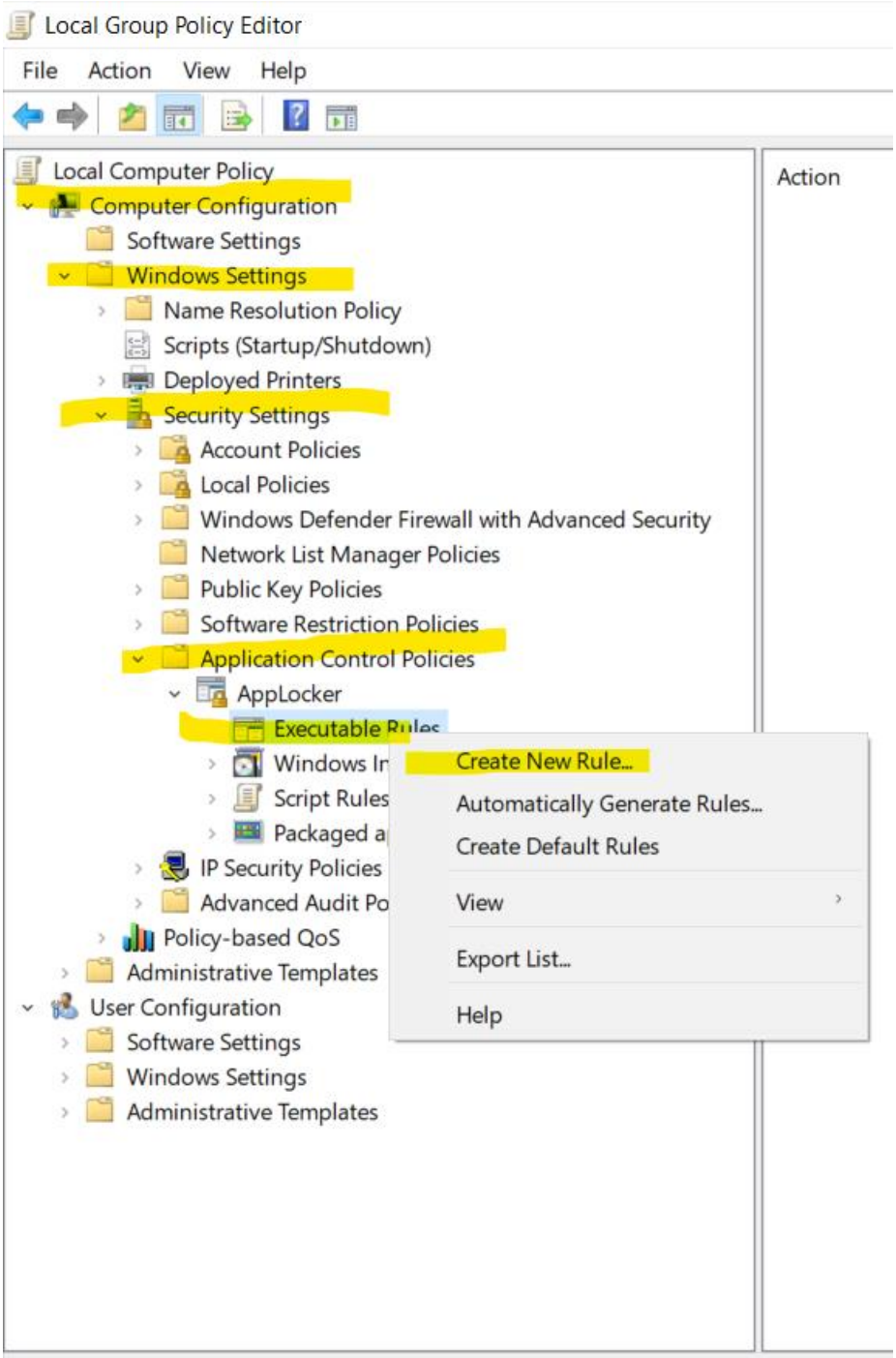
(Finally apply this for all profiles (domain, private, public))



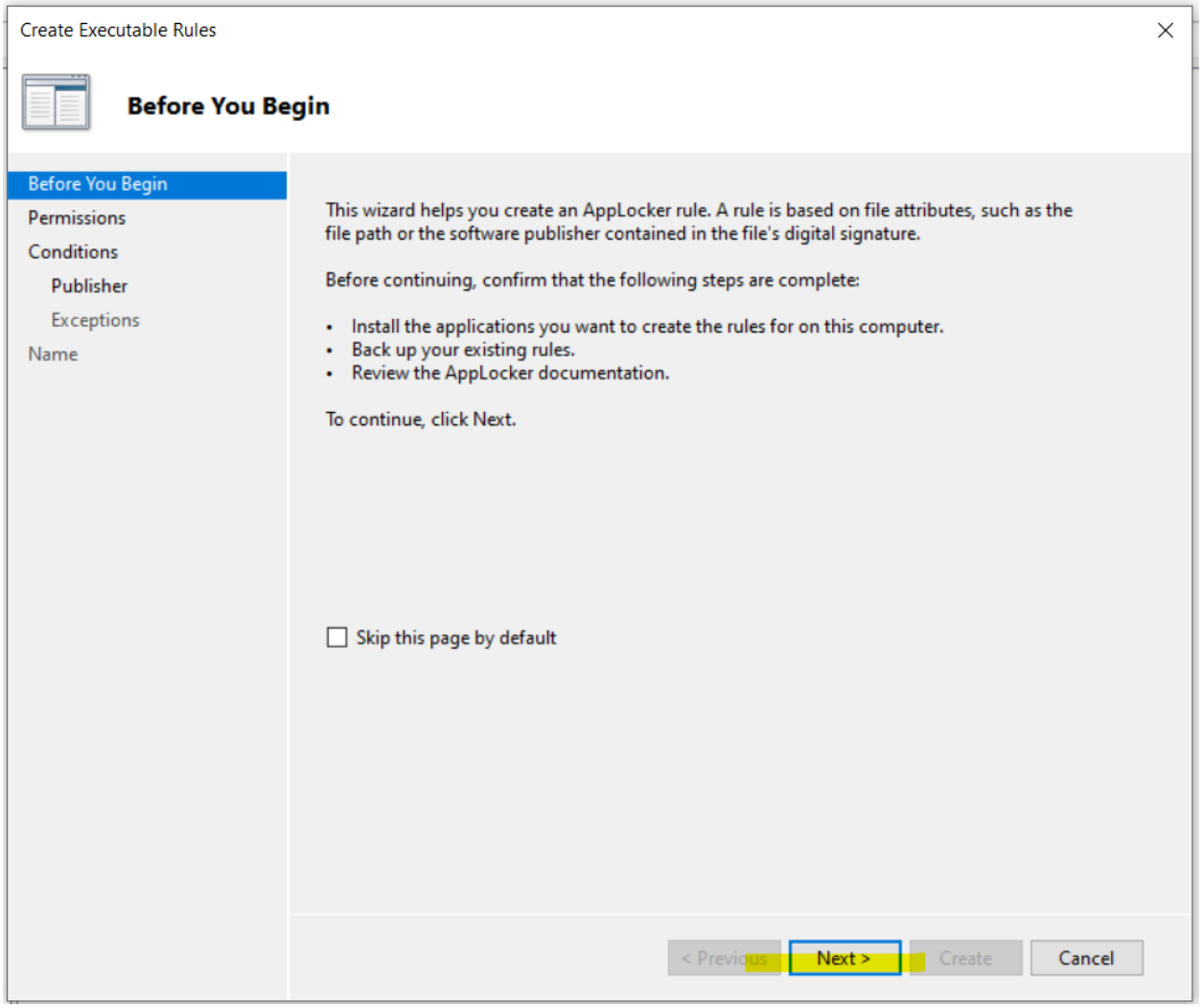
(ame the rule and click “Apply” and “Ok”)

Task #2: Hardening AppLocker

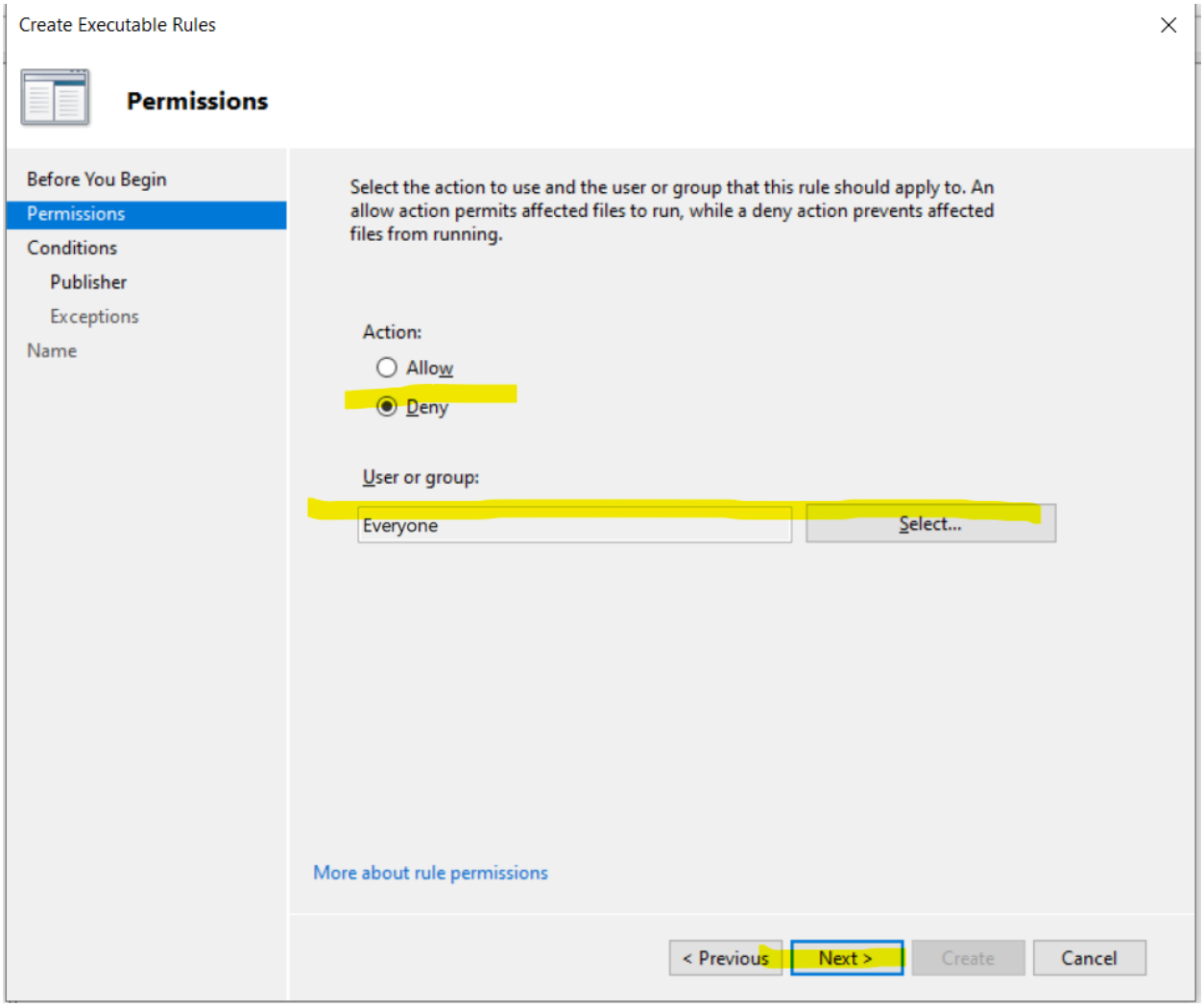
In this section, we will look at hardening the AppLocker and in order to do so, we must block several exe and libraries that are known to bypass AppLocker. To get started we first go to the search bar and type "Edit group policy" then do the following:



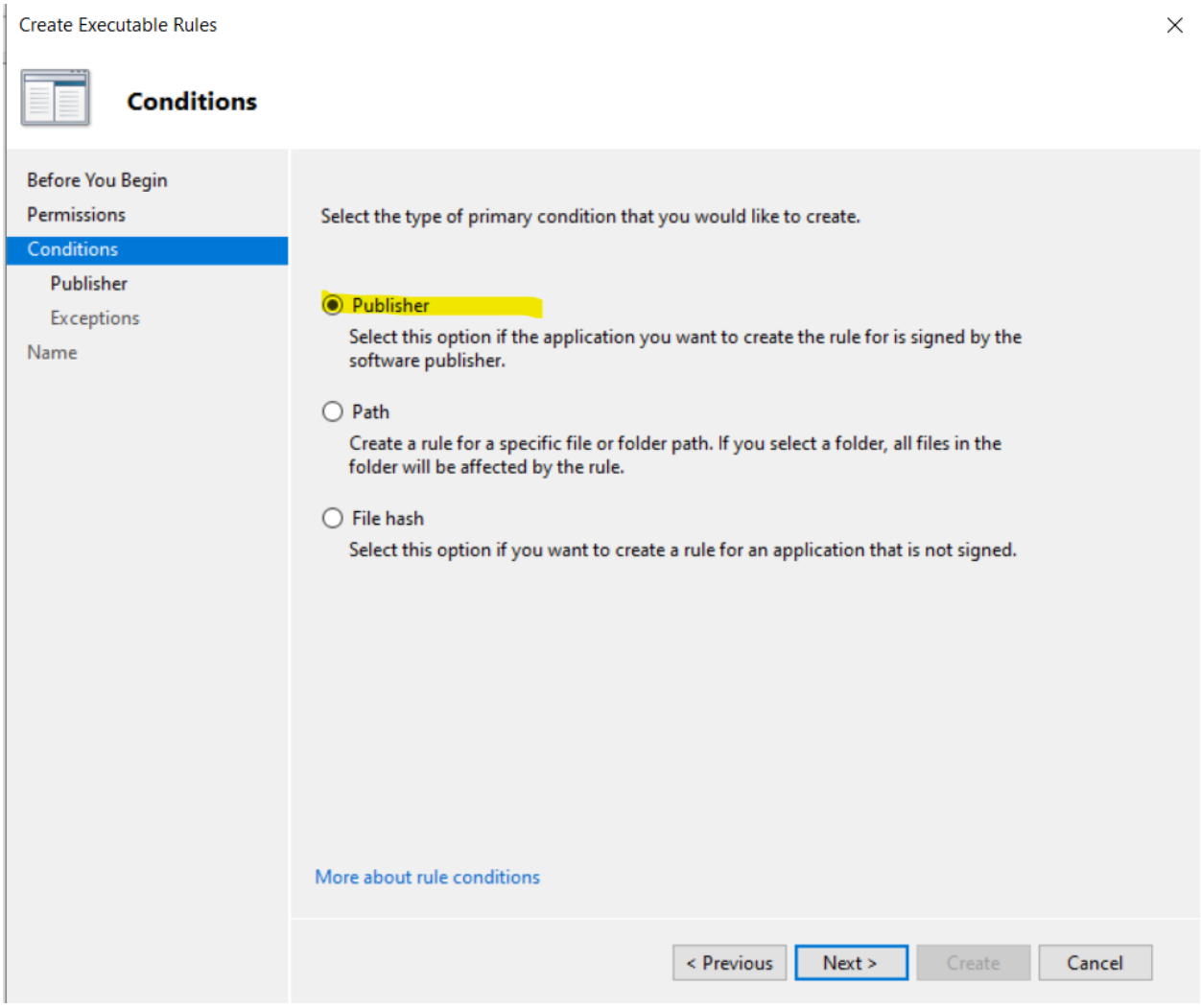
(Go toComputer Configuration > Windows Settings > Security Settings > Application Control Policies > Executable Rules > right click it and then hit "create new rule".)


Create Executable Rules
Before You Begin
Before You Begin
Permissions
Conditions
Publisher
Exceptions
Name
This wizard helps you create an AppLocker rule. A rule is based on file attributes, such as the file path or the software publisher contained in the file's digital signature.
Before continuing, confirm that the following steps are complete:
Install the applications you want to create the rules for on this computer.
Back up your existing rules.
Review the AppLocker documentation.
To continue, click Next.
Skip this page by default
< Previous
Next >
Create
Cancel

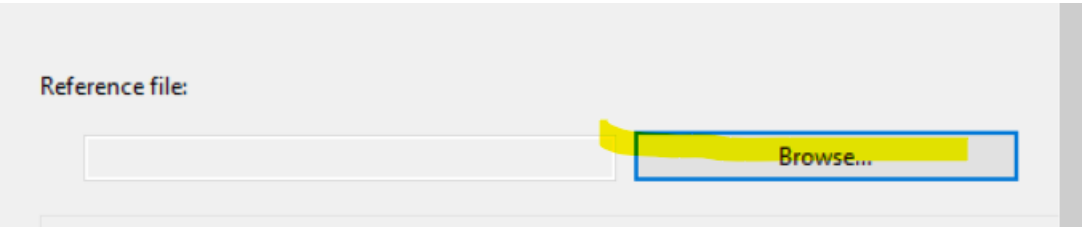
(Click “next”)



(Select action is “deny” > user or group select: “Everyone” > click “next”)



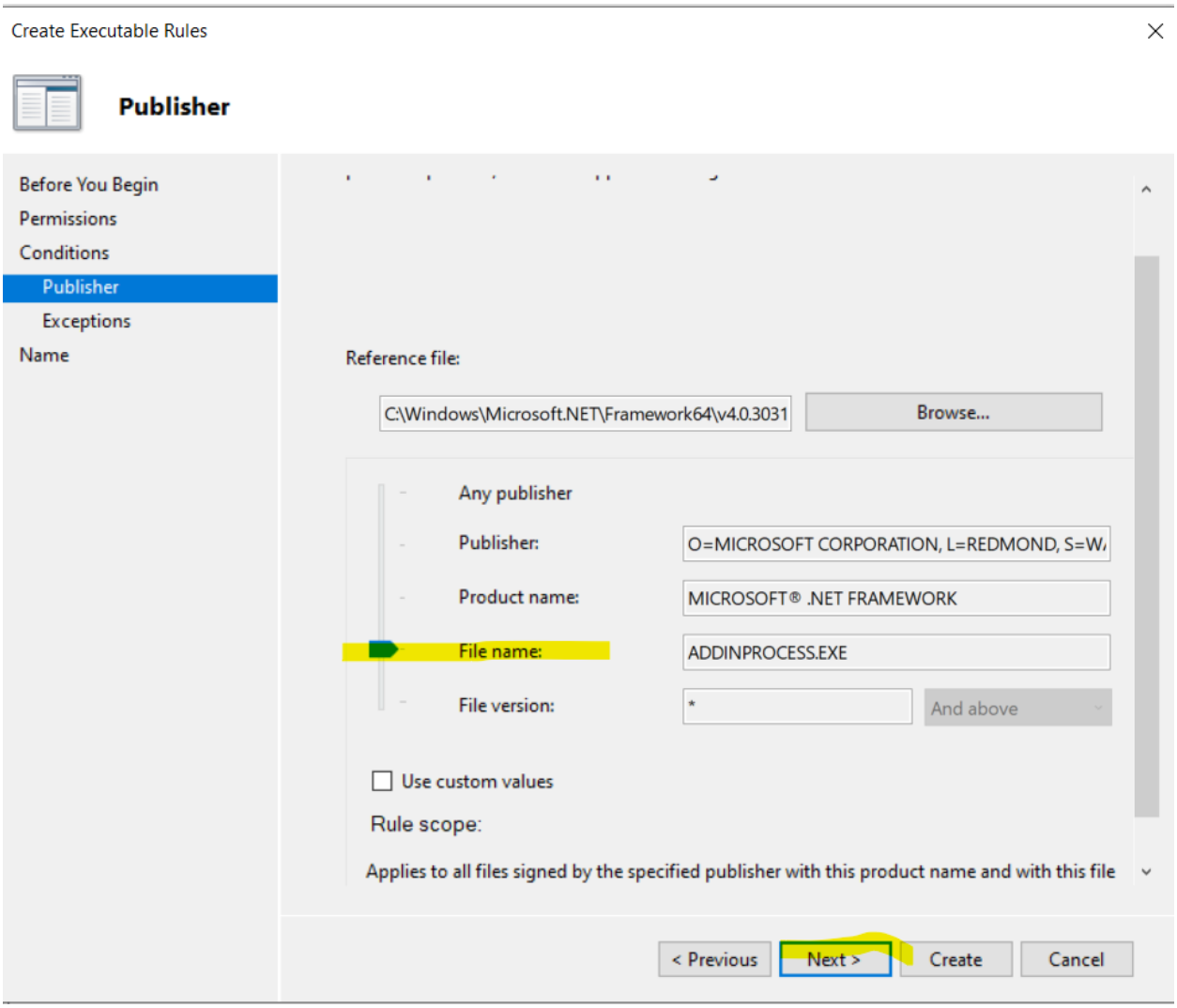
(Select “publisher” > click “next”)



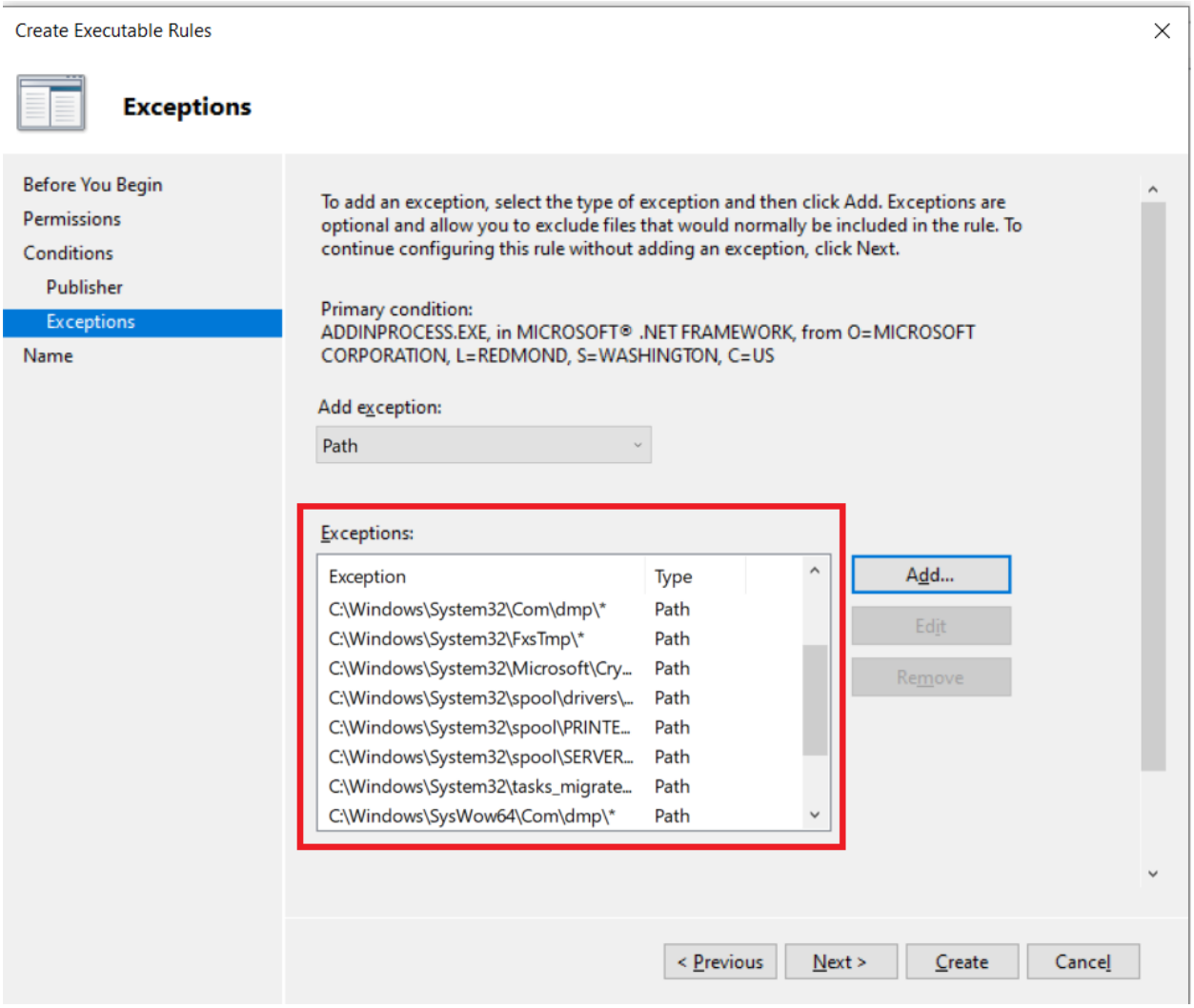
(In here click “Browse” > select the following files listed below in “Figure #1” screenshot)

- *addinprocess.exe*
- *addinprocess32.exe*
- *addinutil.exe*
- *aspnet_compiler.exe*
- *bash.exe*
- *bginfo.exe*
- *cdb.exe*
- *csi.exe*
- *dbghost.exe*
- *dbgsvc.exe*
- *dnx.exe*
- *dotnet.exe*
- *fsi.exe*
- *fsiAnyCpu.exe*
- *infdefaultinstall.exe*
- *kd.exe*
- *kill.exe*
- *lxssmanager.dll*
- *lxrun.exe*
- *Microsoft.Build.dll*
- *Microsoft.Build.Framework.dll*
- *Microsoft.Workflow.Compiler.exe*
- *msbuild.exe2*
- *msbuild.dll*
- *mshta.exe*
- *ntkd.exe*
- *ntsd.exe*
- *powershellcustomhost.exe*
- *rcsi.exe*
- *runscripthelper.exe*
- *texttransform.exe*
- *visualuiaverifynative.exe*
- *system.management.automation.dll*
- *wfc.exe*
- *windbg.exe*
- *wmic.exe*
- *wsl.exe*
- *wslconfig.exe*
- *wslhost.exe*

(Figure #1 above)



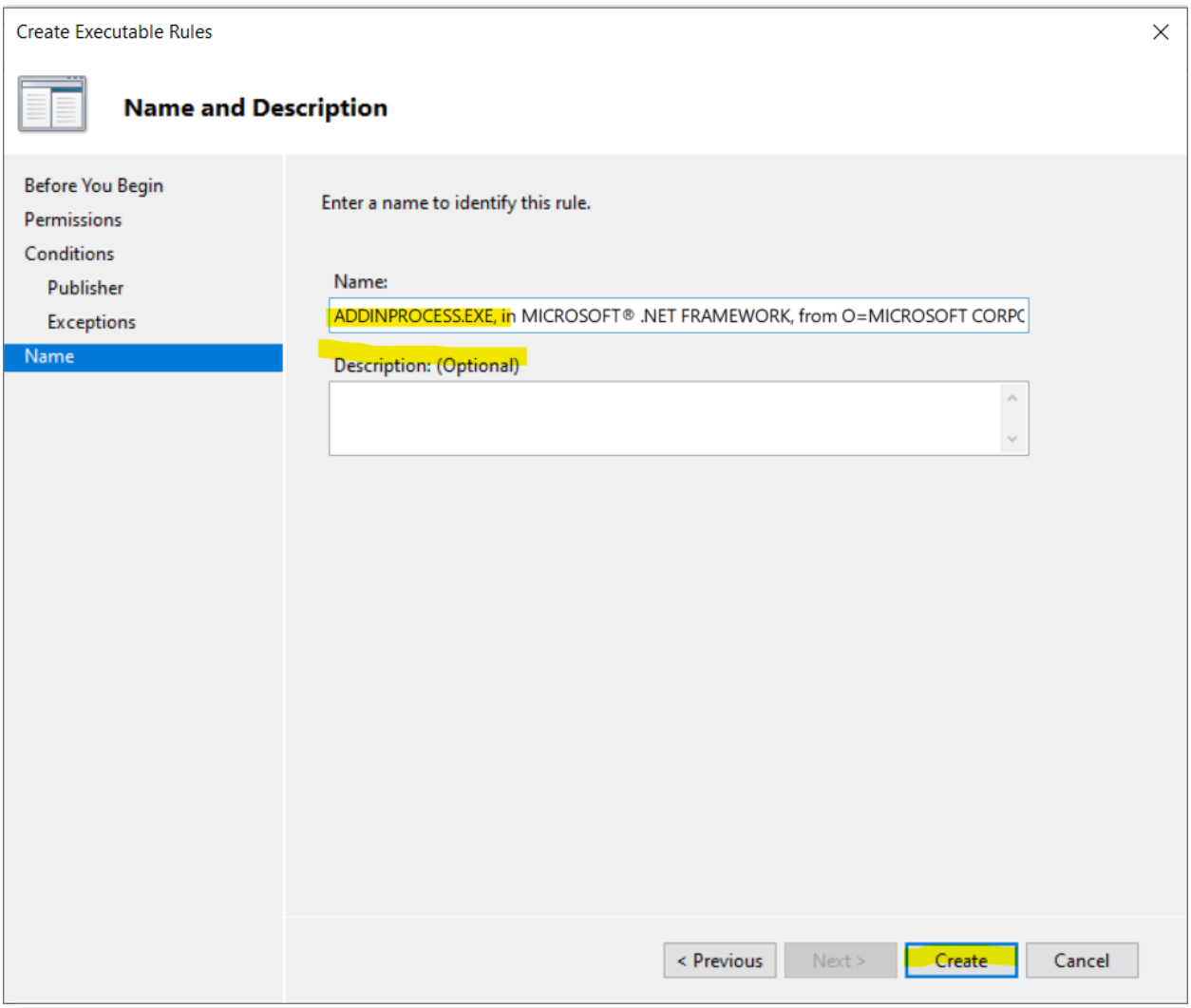
((I picked “addinprocess.exe” as an example) > Select the scroll icon to set it to “file name” option.)



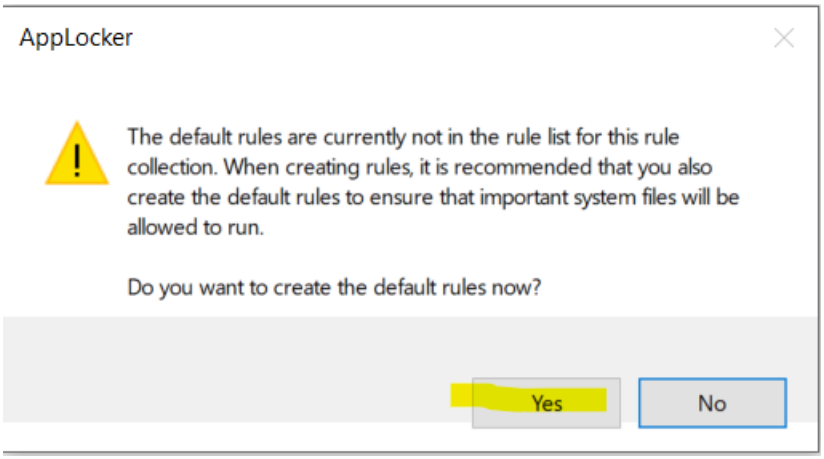
(Next, we must create an exception for these rules with user writeable paths; the rules are listed under "Figure #2".)

Path
*C:\Windows\Tasks**
*C:\Windows\Temp**
*C:\Windows\tracing**
*C:\Windows\System32\Com\dmp**
*C:\Windows\System32\FxsTmp**
*C:\Windows\SysWow64\Com\dmp**
*C:\Windows\SysWow64\FxsTmp**
*C:\Windows\System32\spool\drivers\color**
*C:\Windows\System32\spool\PRINTERS**
*C:\Windows\System32\spool\SERVERS**
*C:\Windows\System32\Microsoft\Crypto\RSA\MachineKeys**
C:\Windows\System32\tasks_migrated\microsoft\windows\pla\system
*C:\Windows\SysWow64\Tasks\microsoft\Windows\pla\system**

(Figure #2 above)



(Finally, give it a name and description before hitting “create” button.)

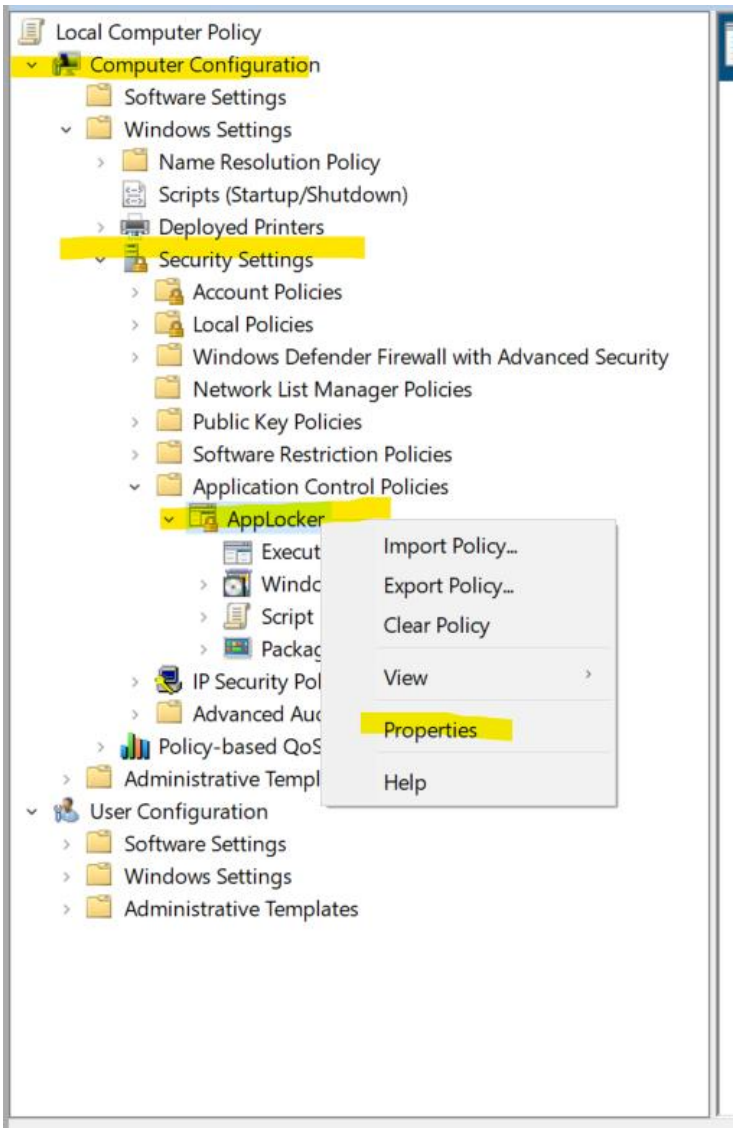


(Click “yes” when the pop-up messages come up and now you will see the newly created rules.)

Action	User	Name	Condition	Exceptions
Allow	Everyone	(Default Rule) All files located in the Pro...	Path	
Allow	Everyone	(Default Rule) All files located in the Win...	Path	
Allow	BUILTIN\Adm...	(Default Rule) All files	Path	
Deny	Everyone	ADDINPROCESS.EXE, in MICROSOFT® .N...	Publisher	Yes

Now, repeat these steps for everything in Figure #1.

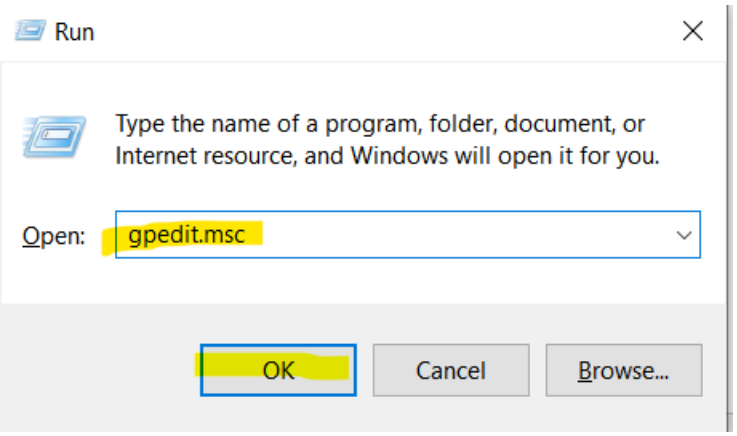
Once everything aforementioned is done, we can turn on enforcement mode for AppLocker. To do this, we must do the following:

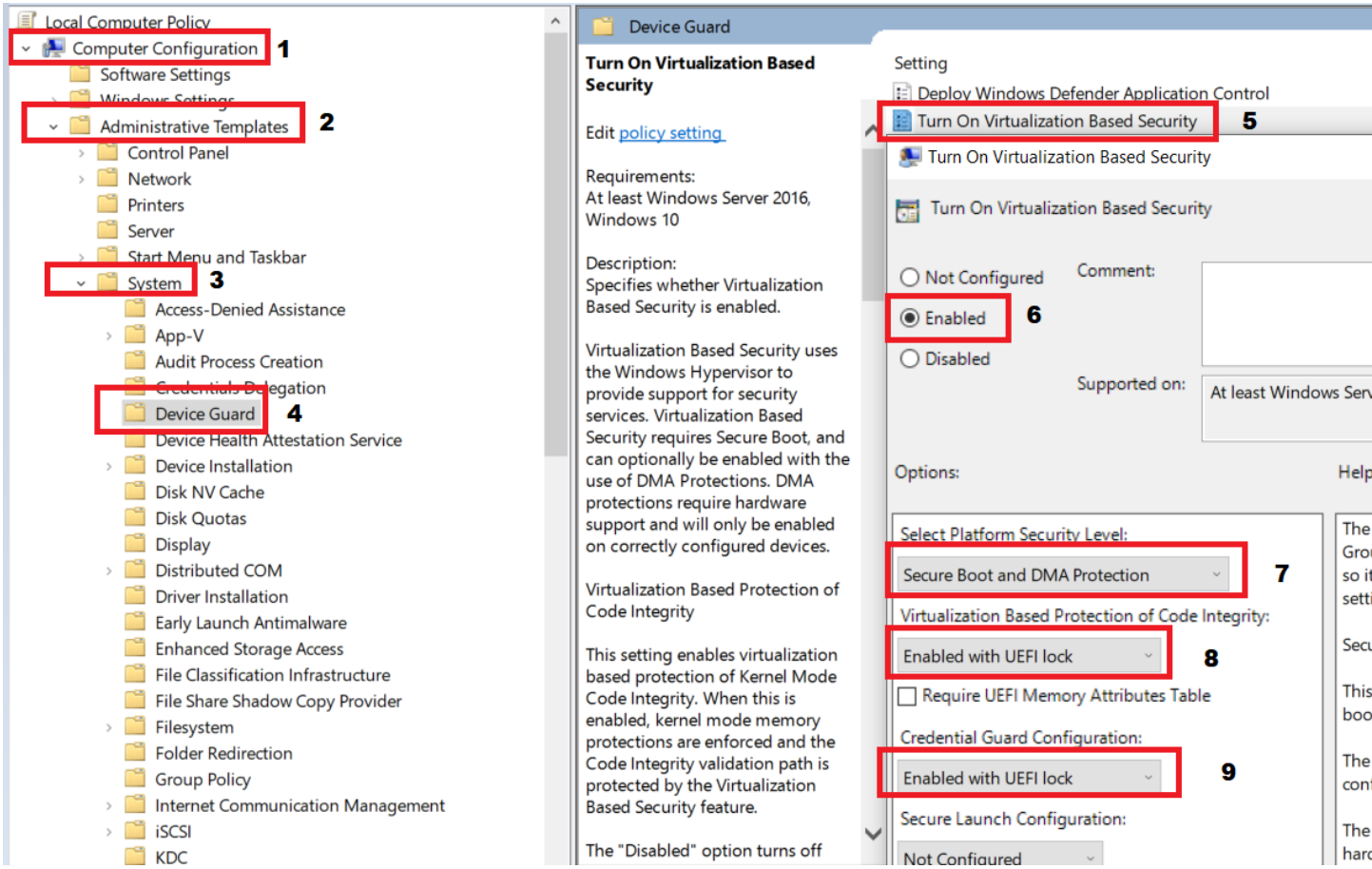


(right click “AppLocker” > Properties > check mark everything on the screen and hit “Ok”)

Task #3: Enhancing Credential Protection

Enabling credential guard is one of the most effective ways to protect user credentials from getting into the wrong hands. Credential Guard essentially isolates them by using Hyper-V hence preventing tools like Mimikatz. In order make the change, do the following: ⊞ + G > type in “gpedit.msc” and hit enter > administrative templates > System > Device Guard > Turn on Virtualization Based Security > Now select “enable” and then select everything in the red rectangle under “options” shown in the screenshot below. Once correctly configured, you will it enabled like in Figure #3. Check screenshots below for pictural chronological steps.



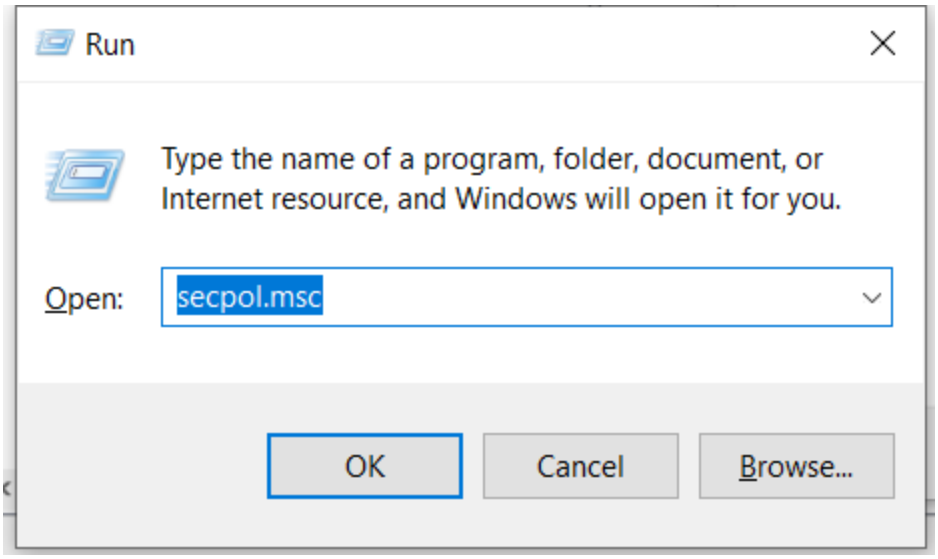


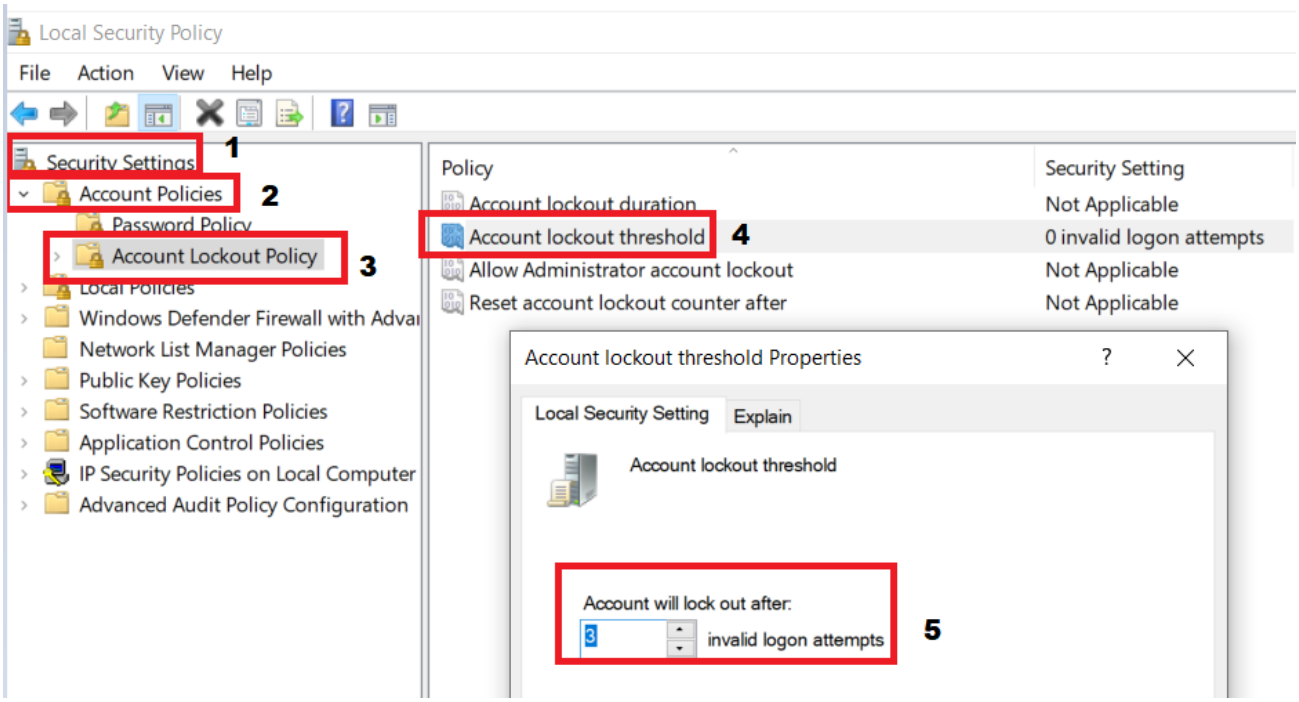
Setting	State	Comment
Deploy Windows Defender Application Control	Not configured	No
Turn On Virtualization Based Security	Enabled	No

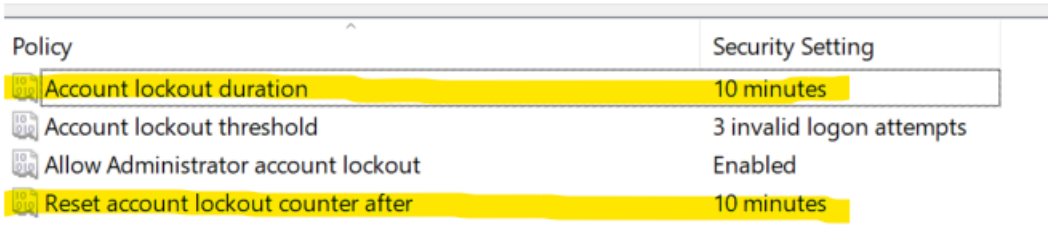
(Figure #3)

Task #4: Enhancing Account Policies

To further enhance users accounts we must adjust the default settings under the account policies with respect to the lockout duration and threshold. In doing so, we prevent any brute force attacks on the credentials. To change these, we do the following: ⊞ + G > type “secpol.msc” then hit “Ok” > Go to “Account Policies” then “Account Lockout Policy” in the left pane of “Local Security Policy” > click on “Account lockout threshold”. Now enter “3” into the box. Hit “Ok”. You can adjust the time of the lockout duration and reset account lockout after timers to 15 minutes by double clicking each in Figure #4. Check screenshots below for pictural chronological steps.



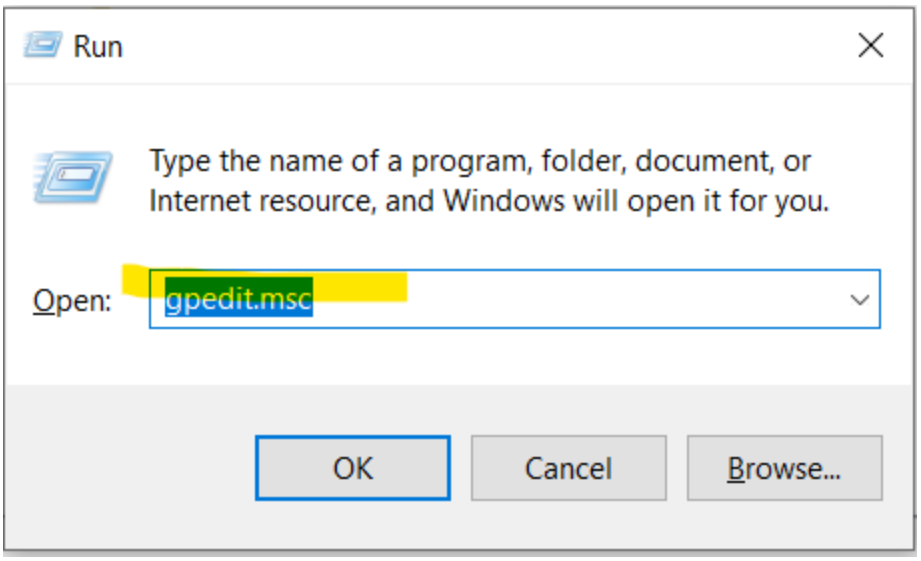


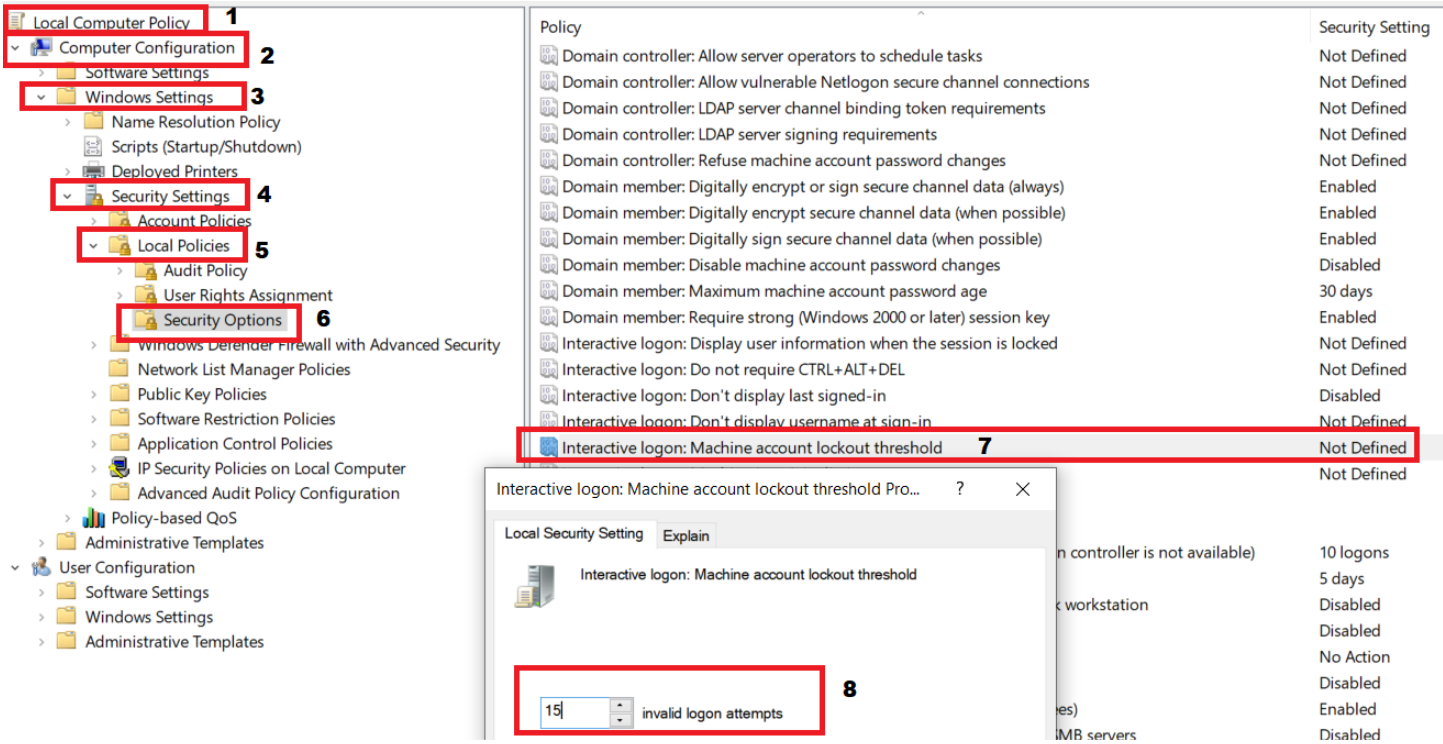


(Figure #4 above)

Task #5: BitLocker & Encrypted Key Lockouts

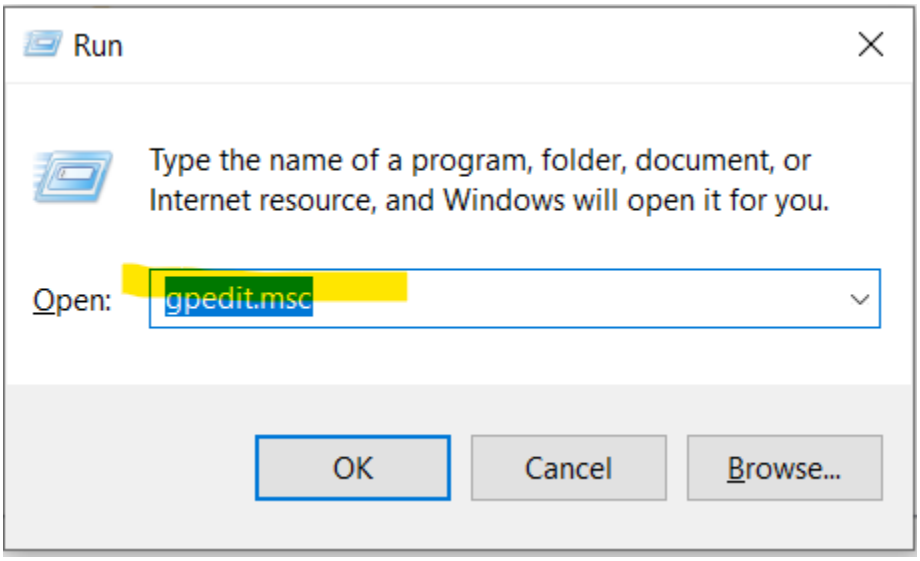
Sometimes, there may be sensitive data on the computer thus it is best practice to delete encrypted keys after many logins attempts by a bad actor. This is necessary for protection against advance types of password attacks such as Credential Stuffing. To enable, we do the following: ⊞ + G > type "gpedit.msc" then hit "Ok" > computer configuration > windows settings > security settings > local policies > security options > in the policy section double click "Interactive logon: Machine account lockout threshold" > set the "invalid logon attempts" to 15 > click "apply" then "ok". After 15 attempts, the user would have to go through BitLocker recovery in order to recover their PC. Check screenshots below for pictural chronological steps.

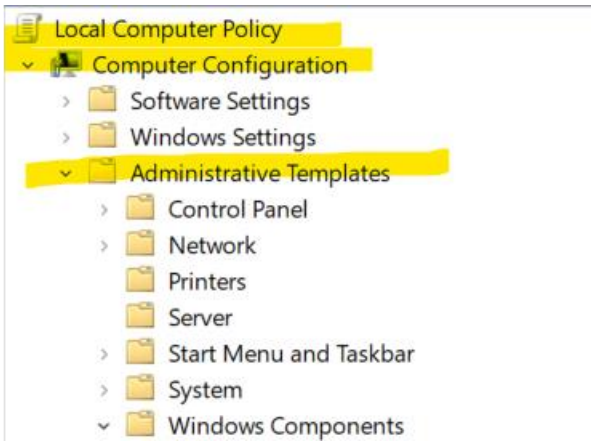

Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
gpedit.msc
OK
Cancel
Browse...


Local Computer Policy
1
Computer Configuration
2
Software Settings
Windows Settings
3
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
4
Account Policies
Local Policies
5
Audit Policy
User Rights Assignment
Security Options
6
Windows Defender Firewall with Advanced Security
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Computer
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates
User Configuration
Software Settings
Windows Settings
Administrative Templates
Policy
Security Setting
Domain controller: Allow server operators to schedule tasks
Not Defined
Domain controller: Allow vulnerable Netlogon secure channel connections
Not Defined
Domain controller: LDAP server channel binding token requirements
Not Defined
Domain controller: LDAP server signing requirements
Not Defined
Domain controller: Refuse machine account password changes
Not Defined
Domain member: Digitally encrypt or sign secure channel data (always)
Enabled
Domain member: Digitally encrypt secure channel data (when possible)
Enabled
Domain member: Digitally sign secure channel data (when possible)
Enabled
Domain member: Disable machine account password changes
Disabled
Domain member: Maximum machine account password age
30 days
Domain member: Require strong (Windows 2000 or later) session key
Enabled
Interactive logon: Display user information when the session is locked
Not Defined
Interactive logon: Do not require CTRL+ALT+DEL
Not Defined
Interactive logon: Don't display last signed-in
Disabled
Interactive logon: Don't display username at sign-in
Not Defined
Interactive logon: Machine account lockout threshold
7
Not Defined
Interactive logon: Machine account lockout threshold Pro...
Local Security Setting
Explain
Interactive logon: Machine account lockout threshold
15
invalid logon attempts
8

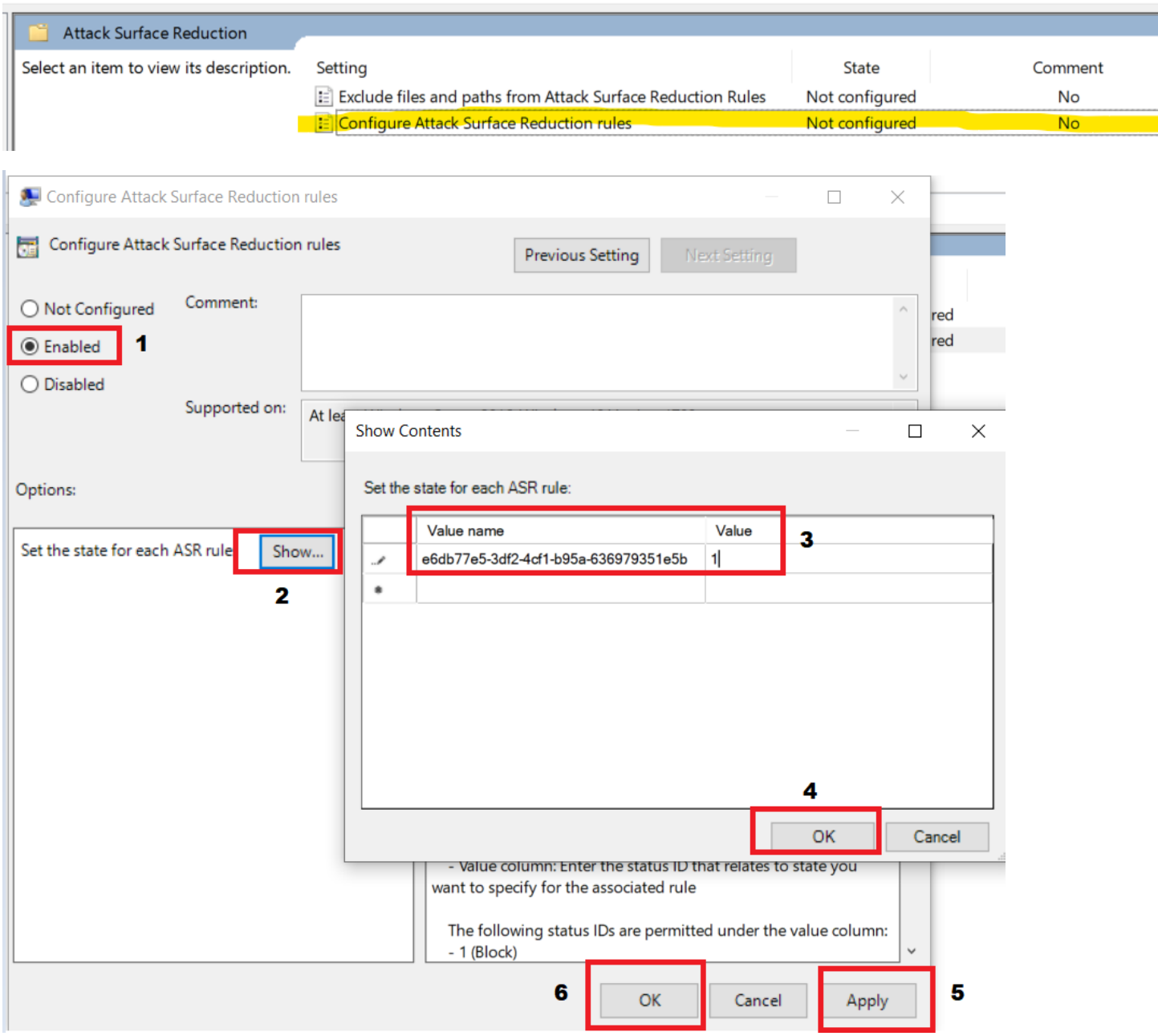
Task #6: WMI Event Subscription Persistence Attacks

WMI Subscription Persistence is a very common way for malware to establish a foothold within a system and start execution of arbitrary code through the trigger of a system event (e.g., user loging, computer's uptime, etc.). To prevent such an issue from occurring, we will have to block any code execution through WMI events. Here are the following steps to do this: ⊞ + G > type “gpedit.msc” then hit “Ok” > computer configuration > windows component > Microsoft Defender Exploit Guard > Attack Surface Reduction > Configure Attack Surface Reduction rule (center panel item) > click enable then add the following rule ID and value: ID = e6db77e5-3df2-4cf1-b95a-636979351e5b | value = 1. Check screenshots below for pictural chronological steps.



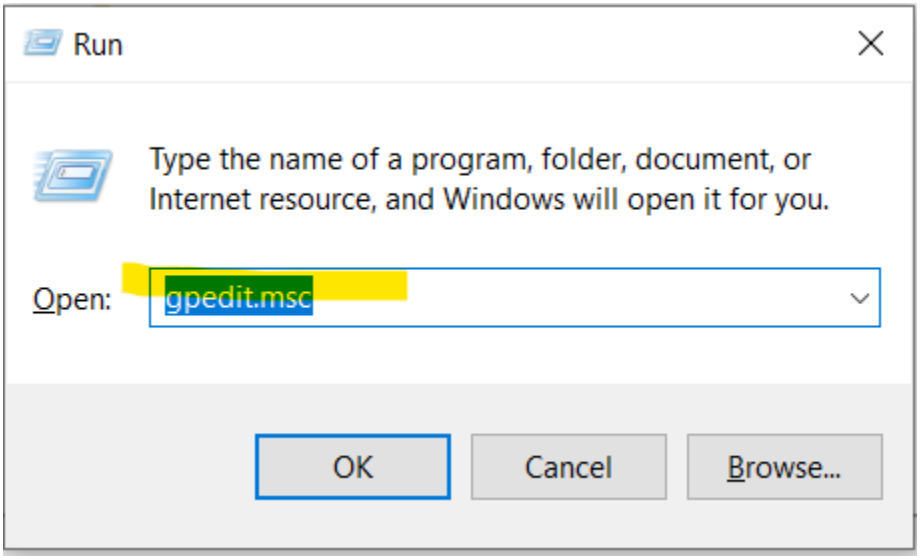


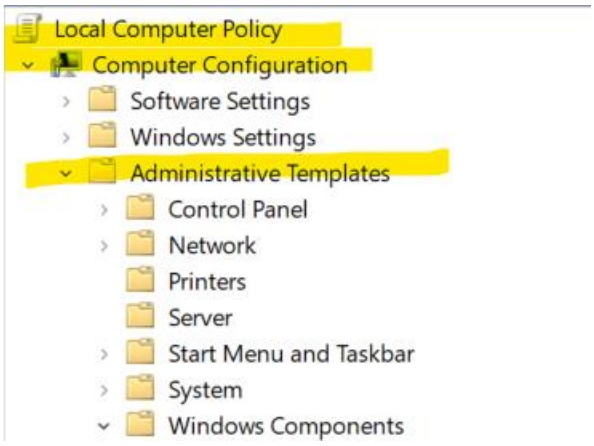
Microsoft account
Microsoft Defender Antivirus
Client Interface
Device Control
Exclusions
MAPS
Microsoft Defender Exploit Guard
Attack Surface Reduction
Controlled Folder Access
Network Protection


Attack Surface Reduction
Select an item to view its description.
Setting
State
Comment
Exclude files and paths from Attack Surface Reduction Rules
Not configured
No
Configure Attack Surface Reduction rules
Not configured
No
Configure Attack Surface Reduction rules
Configure Attack Surface Reduction rules
Previous Setting
Next Setting
Not Configured
Enabled
1
Disabled
Comment:
Supported on:
Options:
Set the state for each ASR rule
Show...
2
Show Contents
Set the state for each ASR rule:
Value name
Value
e6db77e5-3df2-4cf1-b95a-636979351e5b
1
3
4
OK
Cancel
- Value column: Enter the status ID that relates to state you want to specify for the associated rule
The following status IDs are permitted under the value column:
- 1 (Block)
6
OK
Cancel
Apply
5

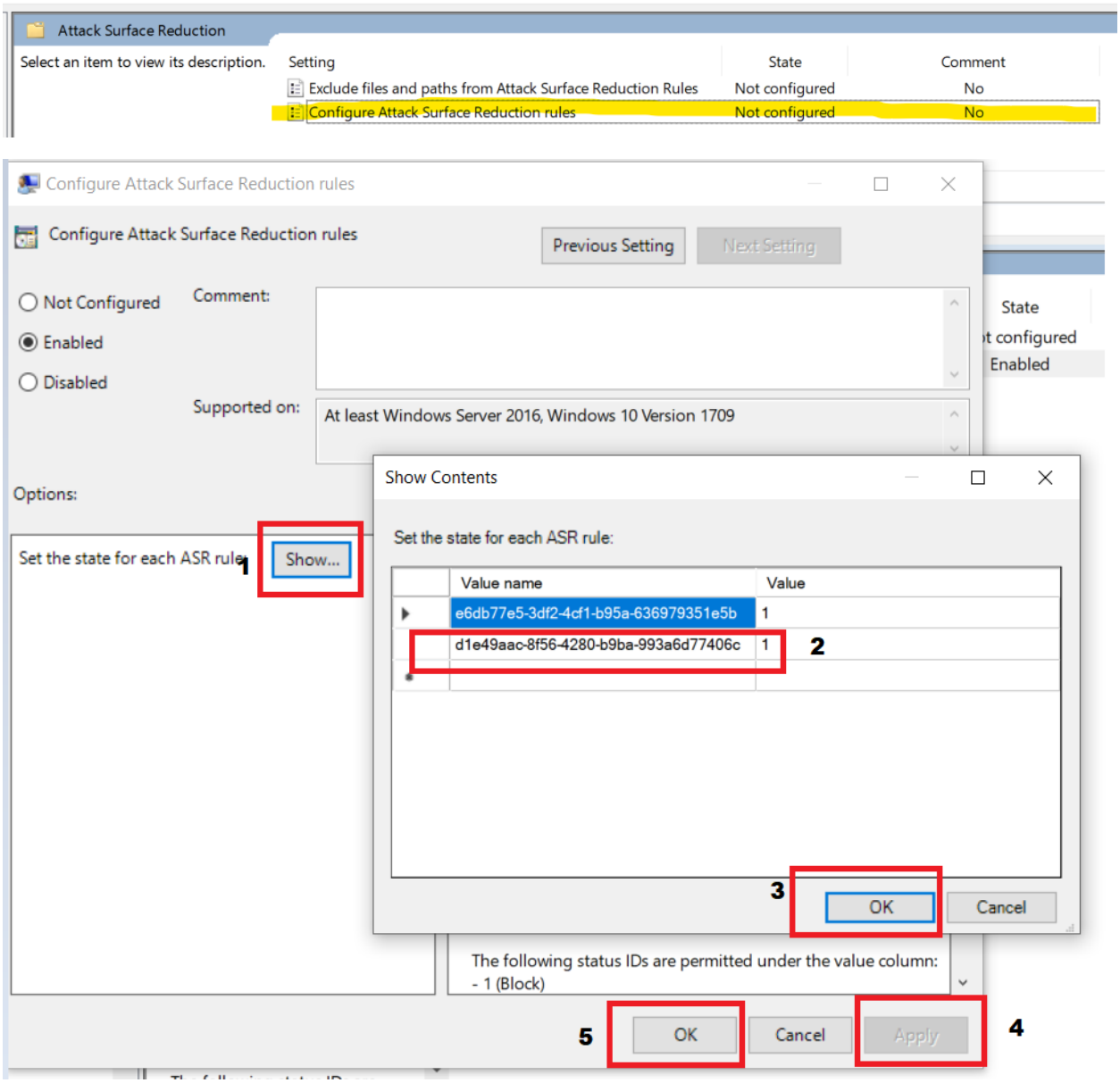
Blocking Arbitrary Code execution through WMI & PSExec

Remote commands can be used to run arbitrary code by malware or APT groups through WMI and PSExec. In order to prevent this from happening, we must ensure that remote execution is disabled. To perform this, we do the following: ⊞ + G > type “gpedit.msc” then hit “Ok” > computer configuration > Administrative Templates > Windows Components > Microsoft Defender Antivirus > Microsoft Defender Exploit Guard > Attack Surface Reduction > Under the items section, click “Configure Attack Surface Reduction rules” > click “show” > enter the ID = d1e49aac-8f56-4280-b9ba-993a6d77406c | value = 1 > hit “ok” > click “apply” > click “ok”. Check screenshots below for pictural chronological steps.



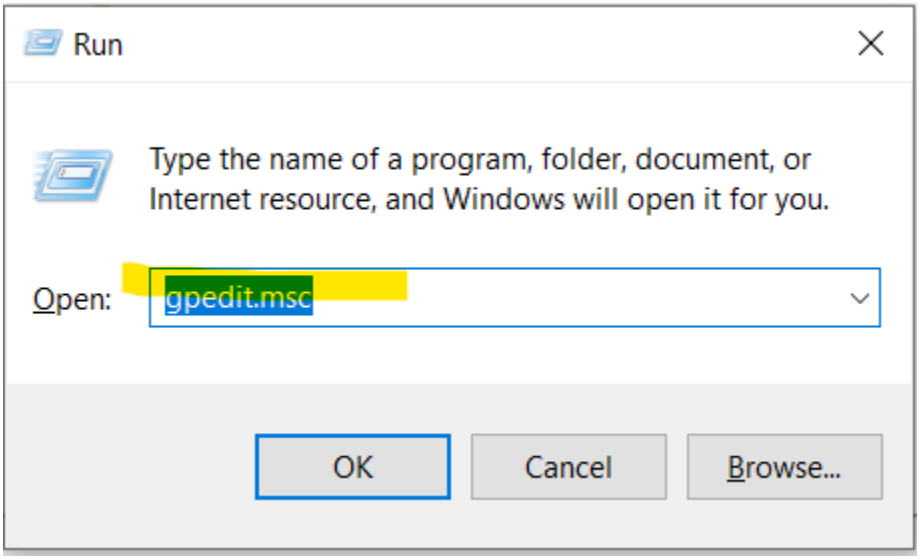


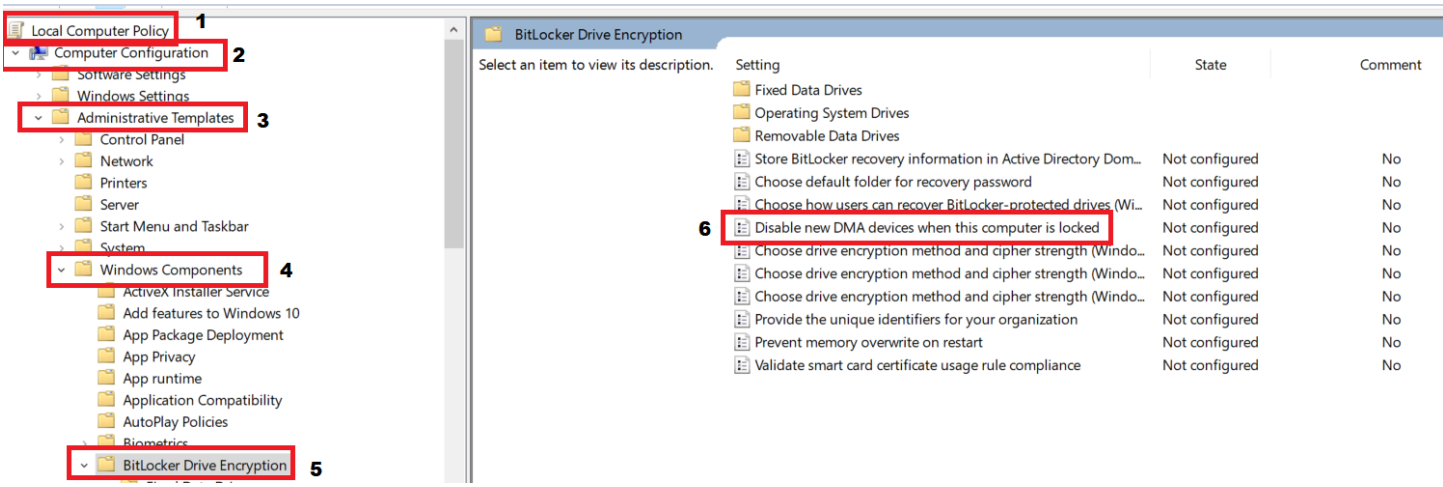
Microsoft account
Microsoft Defender Antivirus
Client Interface
Device Control
Exclusions
MAPS
Microsoft Defender Exploit Guard
Attack Surface Reduction
Controlled Folder Access
Network Protection

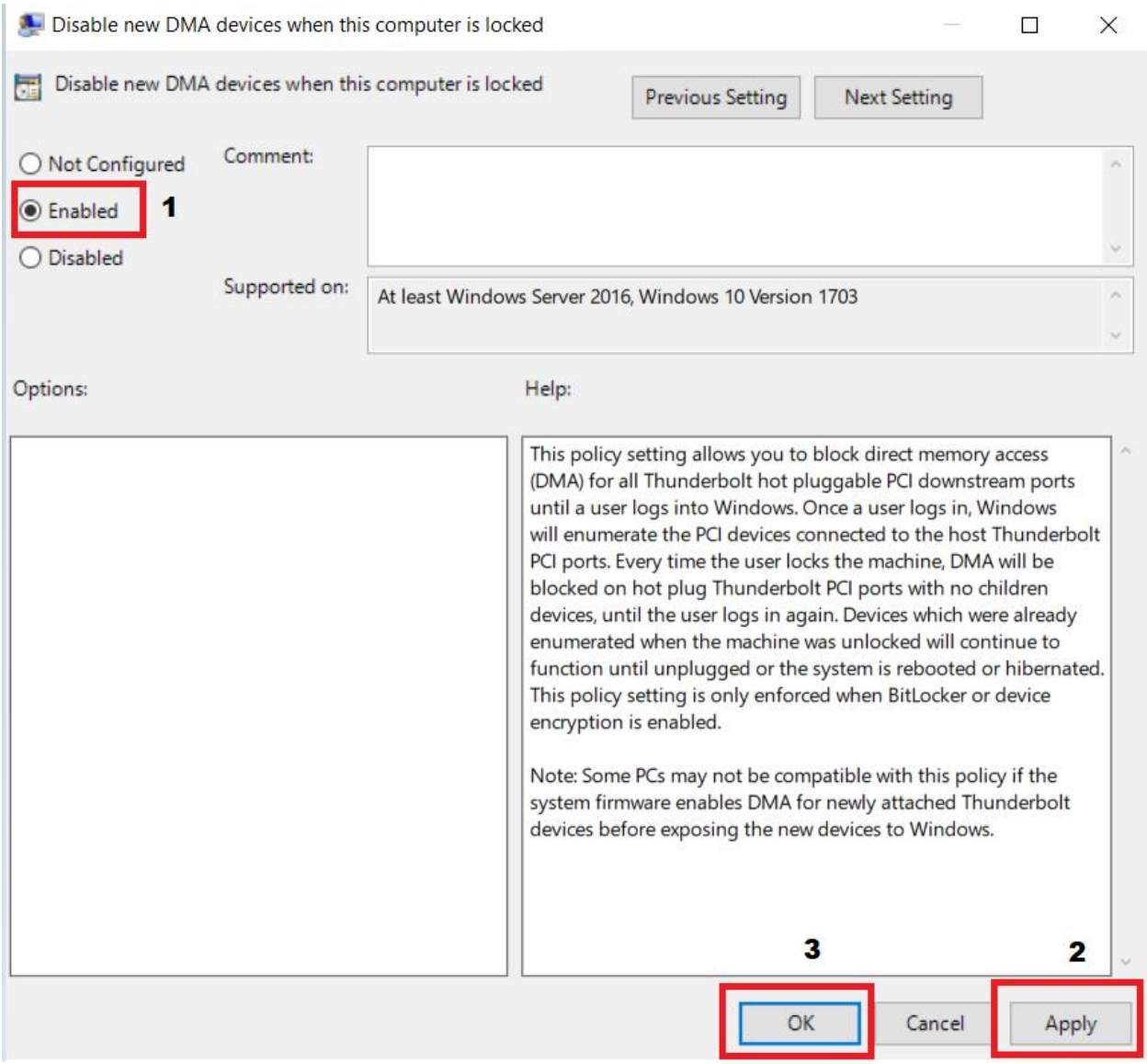

Attack Surface Reduction
Select an item to view its description.
Setting
State
Comment
Exclude files and paths from Attack Surface Reduction Rules
Not configured
No
Configure Attack Surface Reduction rules
Not configured
No
Configure Attack Surface Reduction rules
Configure Attack Surface Reduction rules
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
At least Windows Server 2016, Windows 10 Version 1709
Options:
Set the state for each ASR rule
1
Show...
Show Contents
Set the state for each ASR rule:
Value name
Value
e6db77e5-3df2-4cf1-b95a-636979351e5b
1
d1e49aac-8f56-4280-b9ba-993a6d77406c
1
2
3
OK
Cancel
The following status IDs are permitted under the value column:
- 1 (Block)
5
OK
Cancel
Apply
4

Task #7: Preventing DMA Attacks

Kernel DMA Protection is a great way to mitigate DMA side-channel attacks on in-memory encryption keys. When properly configure, this will prevent adding new DMA devices on the lock screen. To do this, we must harden BitLocker by doing the following: ⊞ + G > type “gpedit.msc” then hit “Ok” > computer configuration > Administrative Templates > Windows Components > BitLocker Drive Encryption (double click to open > click “enable” > hit “apply” > hit “OK”. Check screenshots below for pictural chronological steps.

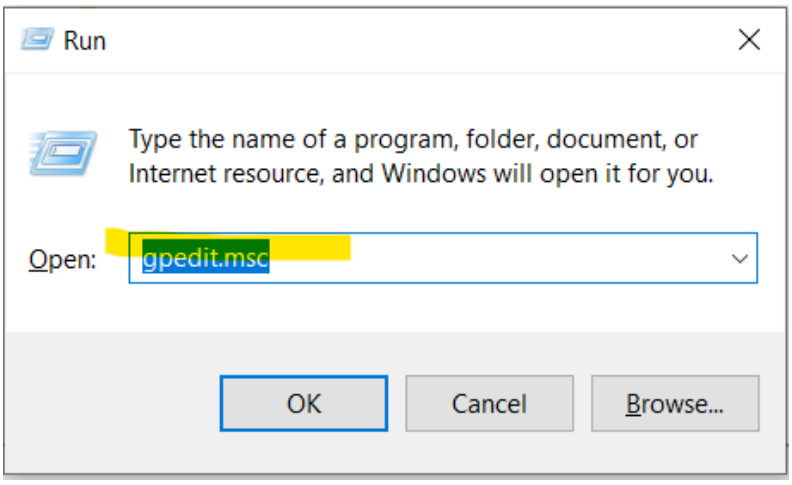


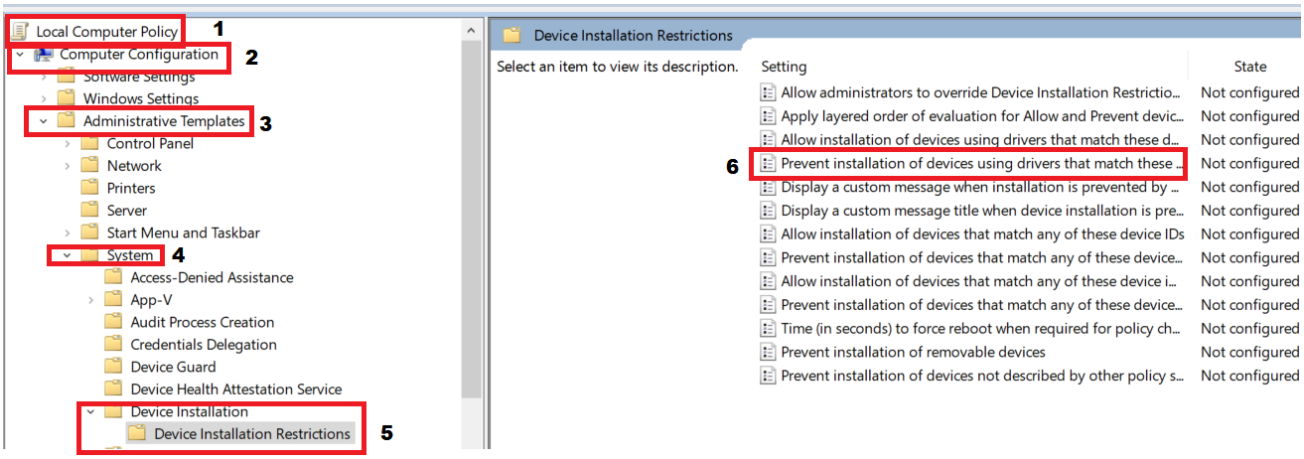


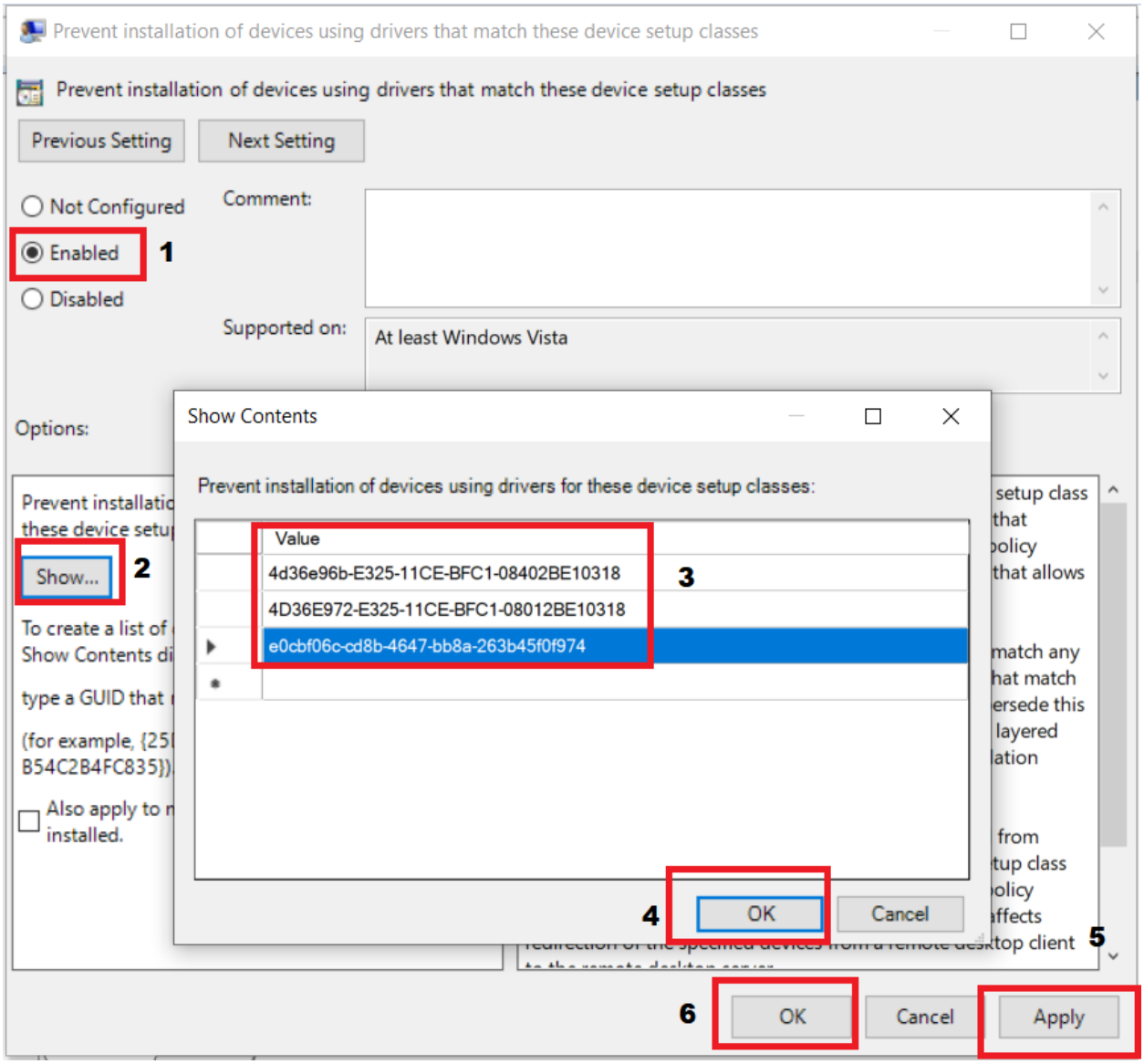


Task #8: Preventing BadUSB Attacks

A BadUSB attack is when a bad actor inserts a modify USB to perform malicious activities on the targeted device. These attacks are generally hard to detect as the computer cannot differentiate between a "malicious" USB devices vs "good" USB devices. The only way to negate these attacks is to prevent any addition of USB devices (this includes new mouse, network adapters, keyboards, etc.) from being added to the PC. We will do the following steps: ⊞ + G > type "gpedit.msc" then hit "Ok" > computer configuration > Administrative Templates > System > Device Installation > Device Installation Restrictions > double click on "Prevent installation of devices using drivers that match these device setup classes" > Click "enable" > click "show" > enter the following values shown in Figure #5 > click "ok" > click "apply > click "ok". Check screenshots below for pictural chronological steps.


Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
gpedit.msc
OK
Cancel
Browse...


Local Computer Policy
1
Computer Configuration
2
Software Settings
Windows Settings
Administrative Templates
3
Control Panel
Network
Printers
Server
Start Menu and Taskbar
System
4
Access-Denied Assistance
App-V
Audit Process Creation
Credentials Delegation
Device Guard
Device Health Attestation Service
Device Installation
Device Installation Restrictions
5
Device Installation Restrictions
Select an item to view its description.
Setting
State
Allow administrators to override Device Installation Restrictio... Not configured
Apply layered order of evaluation for Allow and Prevent devic... Not configured
Allow installation of devices using drivers that match these d... Not configured
6
Prevent installation of devices using drivers that match these ... Not configured
Display a custom message when installation is prevented by ... Not configured
Display a custom message title when device installation is pre... Not configured
Allow installation of devices that match any of these device IDs Not configured
Prevent installation of devices that match any of these device... Not configured
Allow installation of devices that match any of these device i... Not configured
Prevent installation of devices that match any of these device... Not configured
Time (in seconds) to force reboot when required for policy ch... Not configured
Prevent installation of removable devices Not configured
Prevent installation of devices not described by other policy s... Not configured



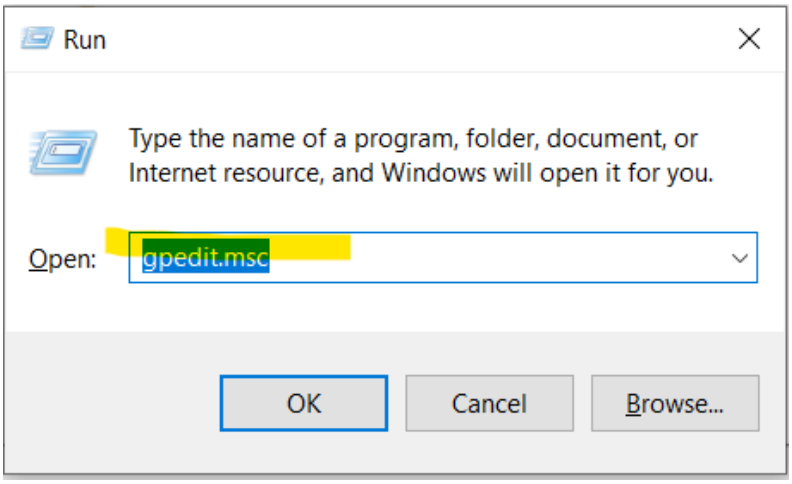
GUID	Description
4d36e96b-E325-11CE-BFC1-08402BE10318	USB Keyboards
4D36E972-E325-11CE-BFC1-08012BE10318	Network interface controllers
e0cbf06c-cd8b-4647-bb8a-263b45f0f974	Bluetooth adapters

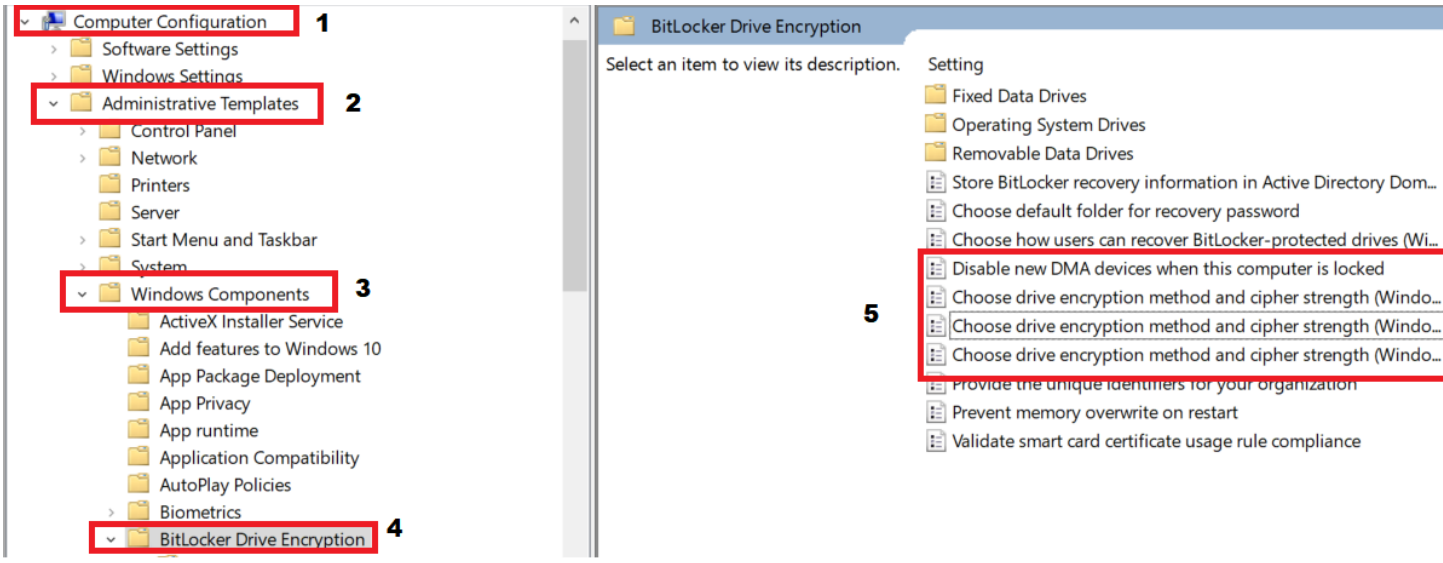
(Figure #5 above)

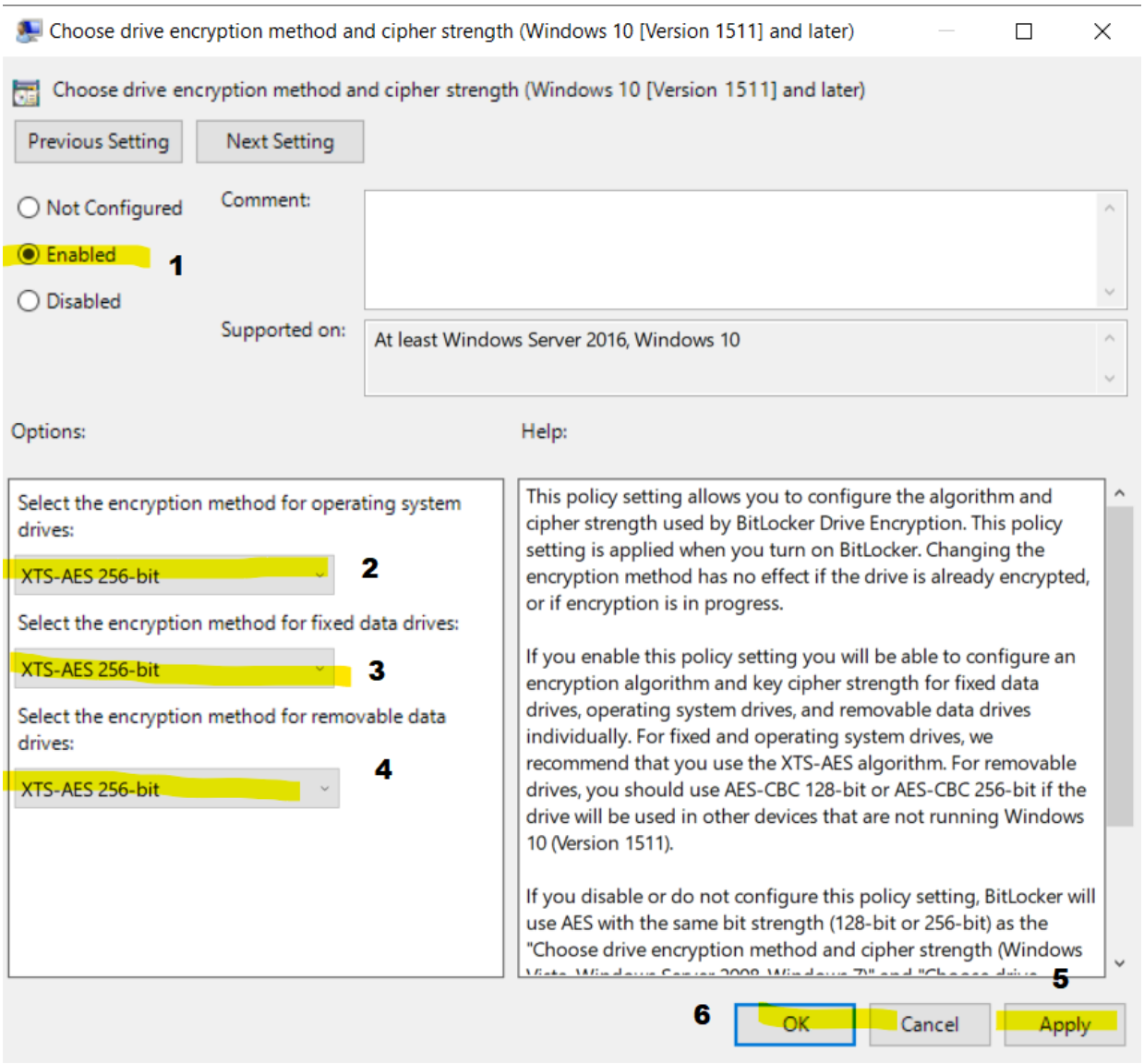
Task #9: Improve encryption mechanism on OS system, fixed data drives, and removable data drives

In order to further secure ones data, we will use a 256-bit AES encryption by BitLocker instead of using the default 128-bit AES encryption mode. By imposing this onto our system, it will strengthen our encryption algorithm with no performance lost. To do this we do the following: ⊞ + G > type

“gpedit.msc” then hit “Ok” > computer configuration > Administrative Templates > Windows Components > click “BitLocker Drive Encryption” > click “Choose drive encryption method and cipher strength (Windows 10 [Version 1511] and later)” > click “enable” > Select the encryption method for “operating system drives” as “XTS-AES 256-bit” > select the “encryption method for fixed data drives” as “XTS-AES 256-bit” > select the “encryption method for removable data drives” as “XTS-AES 256-bit” > click “ok” > click “apply” > click “ok”. Do this for all 4 options in <u>step #5</u> as shown in the screenshot below. Check screenshots below for pictural chronological steps.



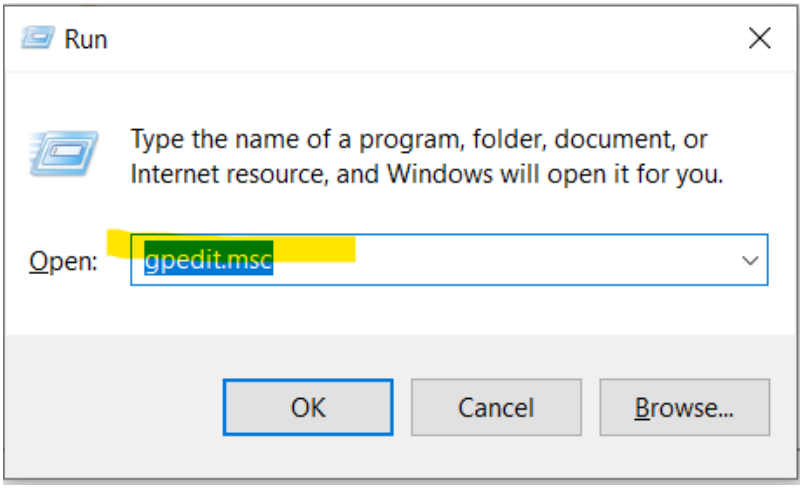


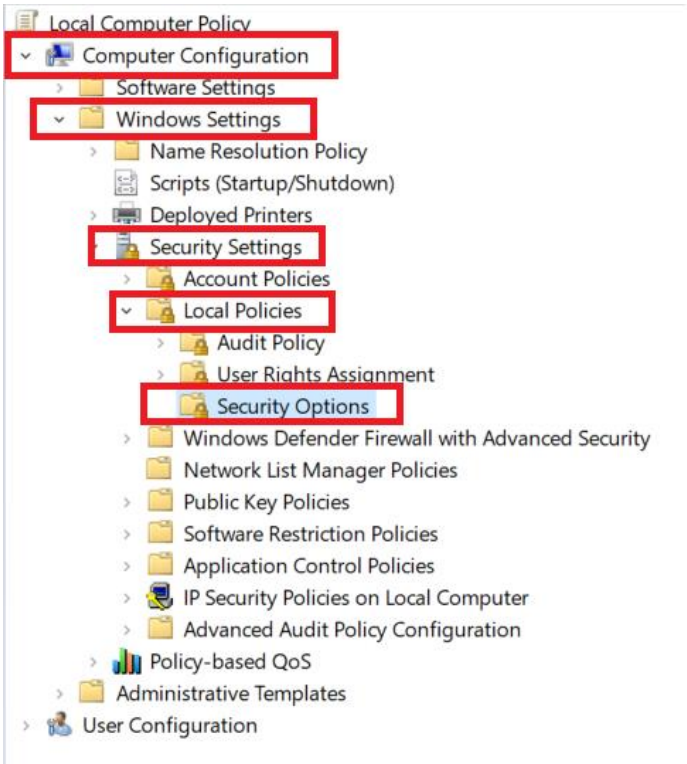


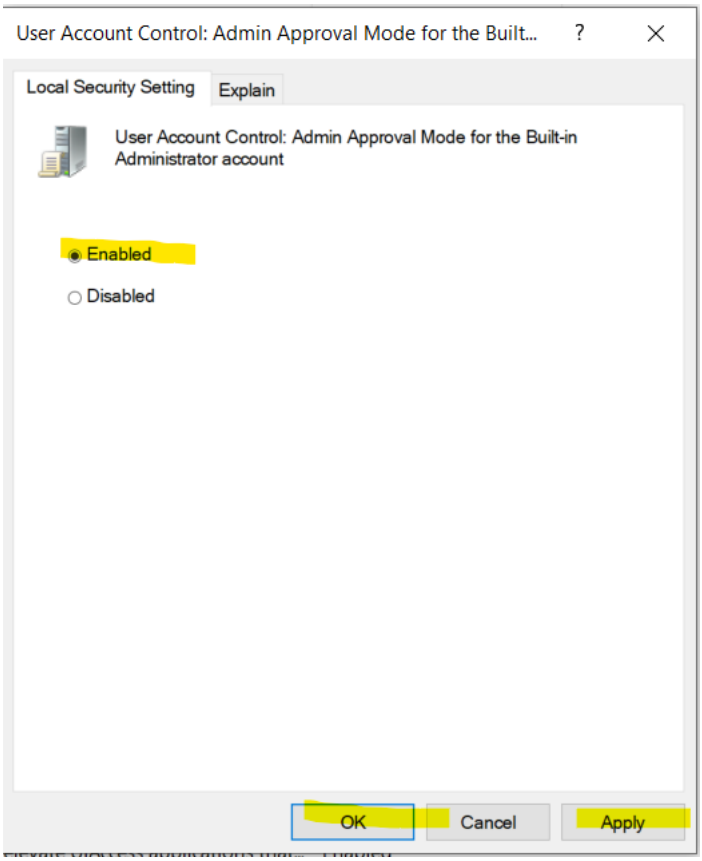
Task #10: Configuring User Access Control (UAC) & Enabling BitLocker

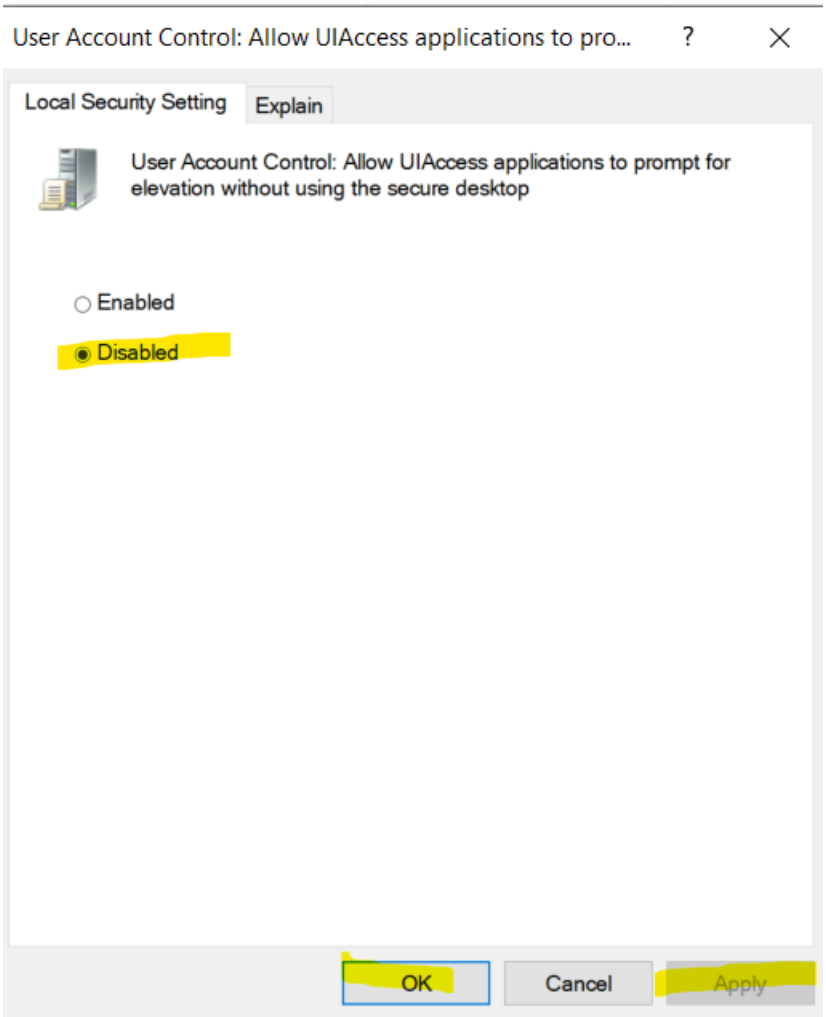
The final task is to properly configure UAC and enable BitLocker protection. UAC by default allows privileged users to perform actions without entering any credentials to verify the legitimacy of the user. Hence, we can see where the problem lies, if the account was compromised by an bad actor, then certain restricted actions are now able to be performed by the bad actor. To correct such issue, we must configure UAC to be more rigorous. This can be performed by the following steps: ⊞ + G > type "gpedit.msc" then hit "Ok" > computer configuration > Windows Settings > Security Settings > Local Policies > Security Options > click "User Account Control: Admin Approval Mode for the Built-in Administrator account" and then "enable" that and hit "apply" then "ok"> click "User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop" and then "disable" that and hit "apply" then "ok" > click "User Account Control: Behavior of the elevation prompt for standard users" and then click "Automatically deny elevation requests" and hit "apply" then "ok" >

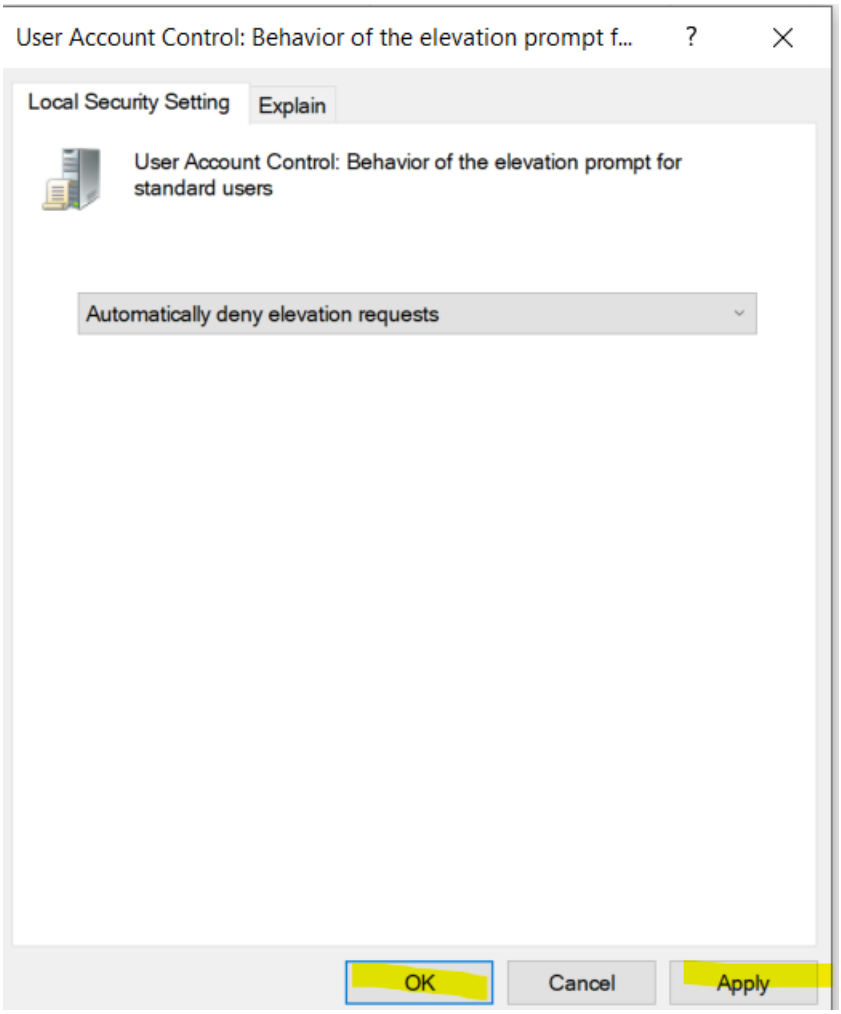
click “User Account Control: Detect application installations and prompt for elevation” and then “enable” that and hit “apply” then “ok” > click “User Account Control: Only elevate UIAccess applications that are installed in secure locations” and then “enable” that and hit “apply” then “ok” > click “User Account Control: Run all administrators in Admin Approval Mode” and then “enable” that and hit “apply” then “ok” > click “User Account Control: Switch to the secure desktop when prompting for elevation” and then “enable” that and hit “apply” then “ok” > click “User Account Control: Virtualize file and registry write failures to per-user locations” and then “enable” that and hit “apply” then “ok”. Check screenshots below for pictural chronological steps.

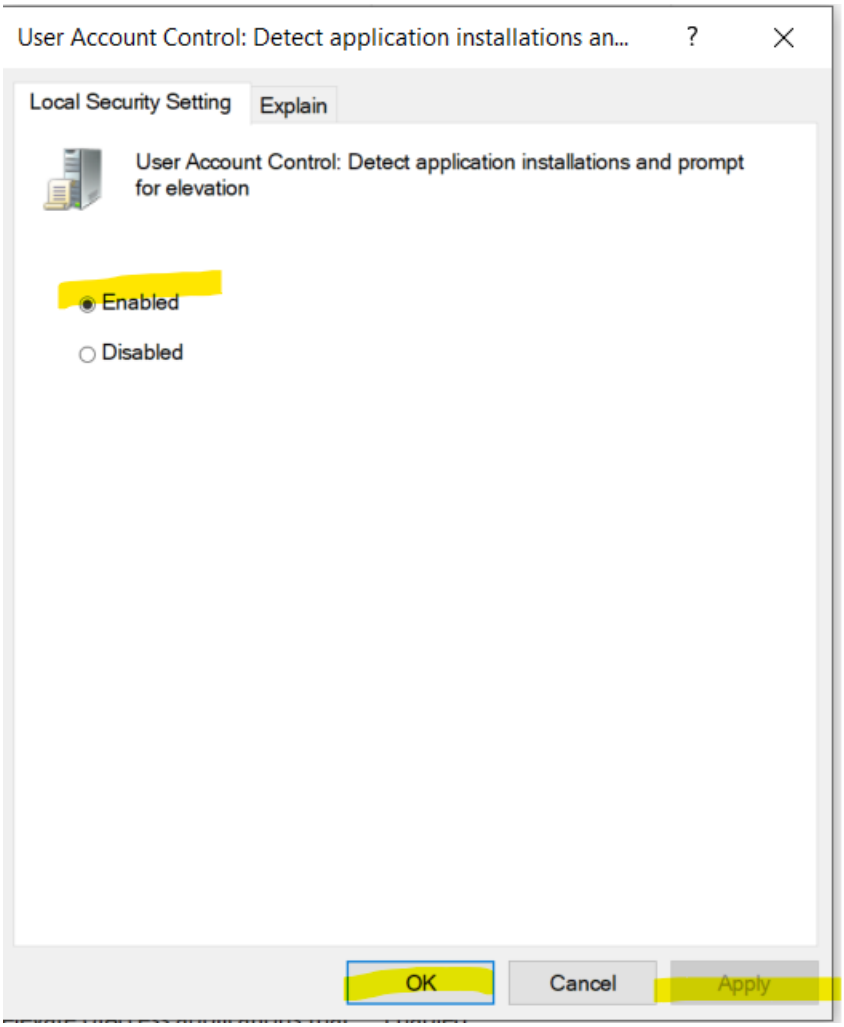


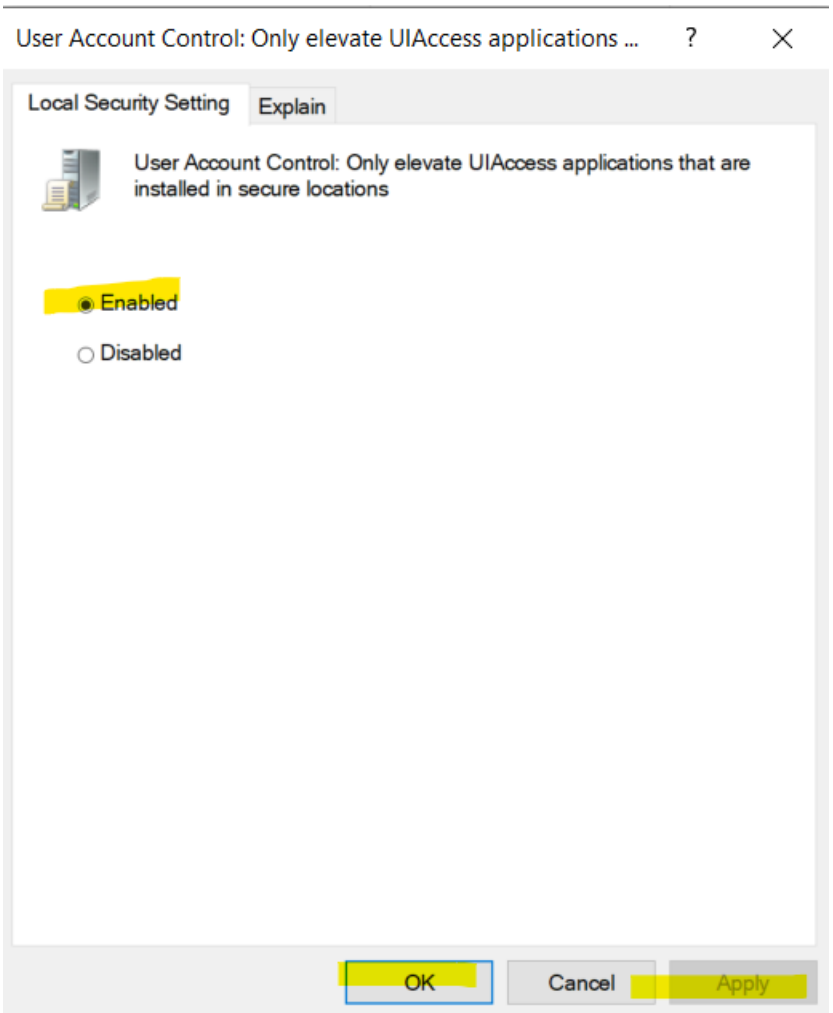


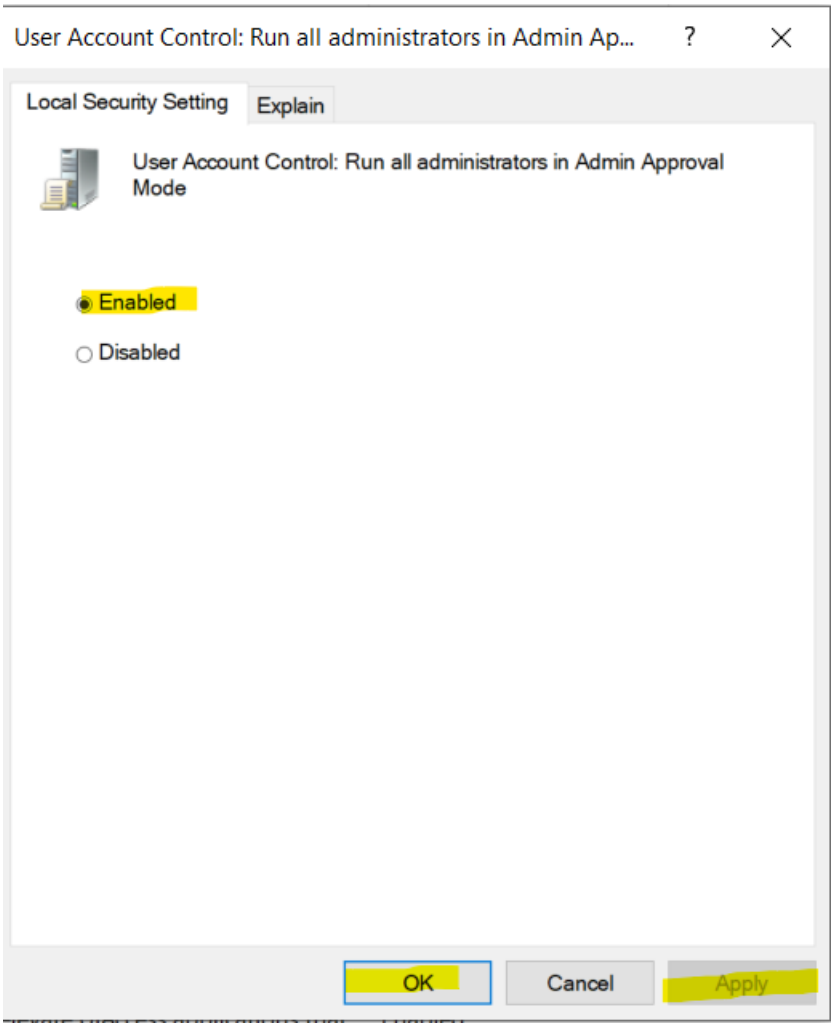

User Account Control: Admin Approval Mode for the Built...
Local Security Setting
Explain
User Account Control: Admin Approval Mode for the Built-in Administrator account
Enabled
Disabled
OK
Cancel
Apply

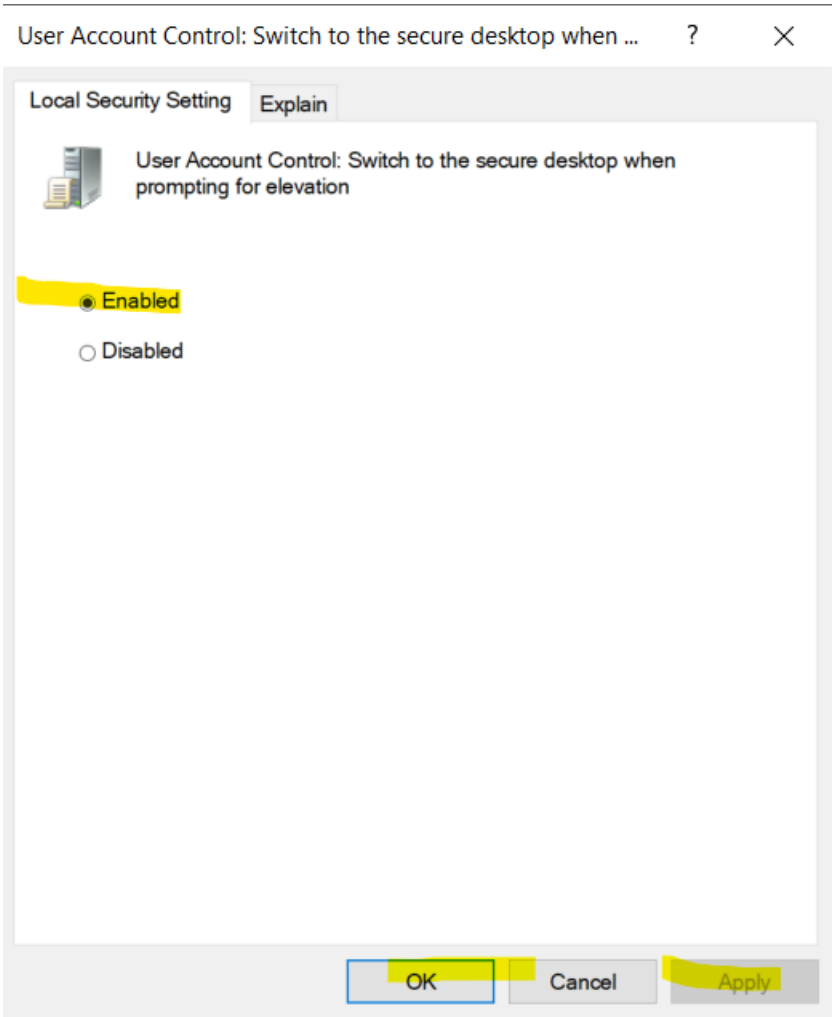

User Account Control: Allow UIAccess applications to pro...
Local Security Setting
Explain
User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop
Enabled
Disabled
OK
Cancel
Apply

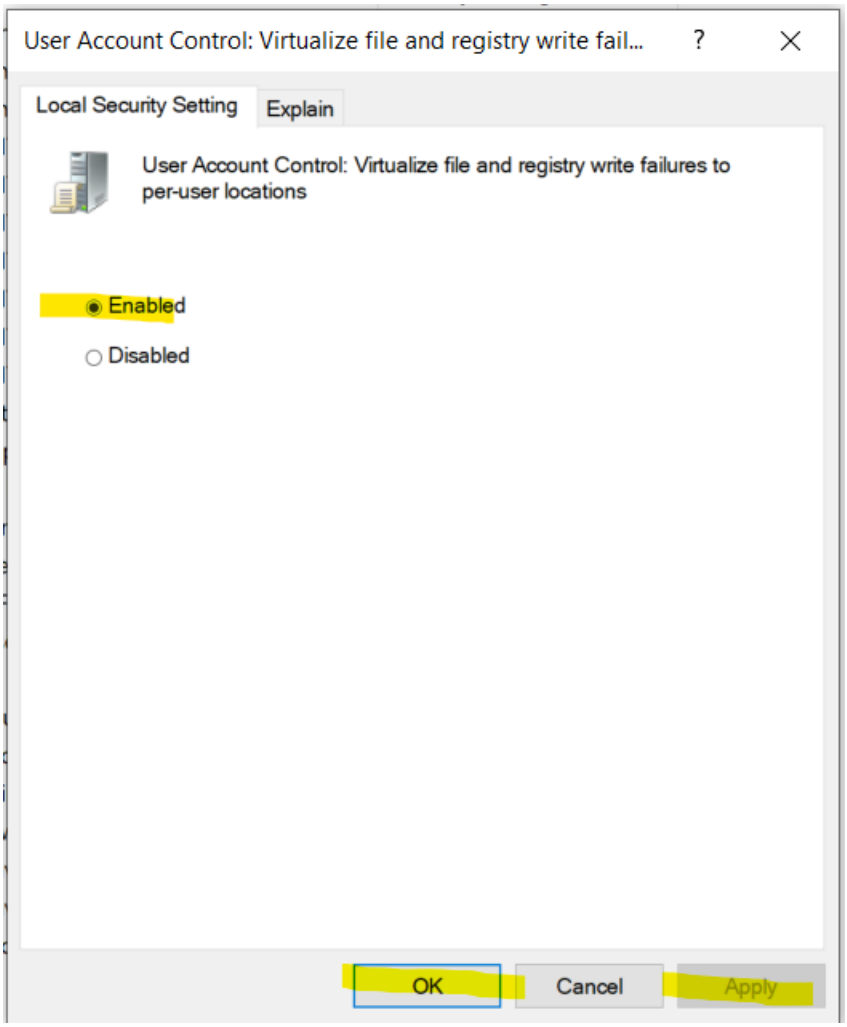

User Account Control: Behavior of the elevation prompt f...
Local Security Setting
Explain
User Account Control: Behavior of the elevation prompt for standard users
Automatically deny elevation requests
OK
Cancel
Apply

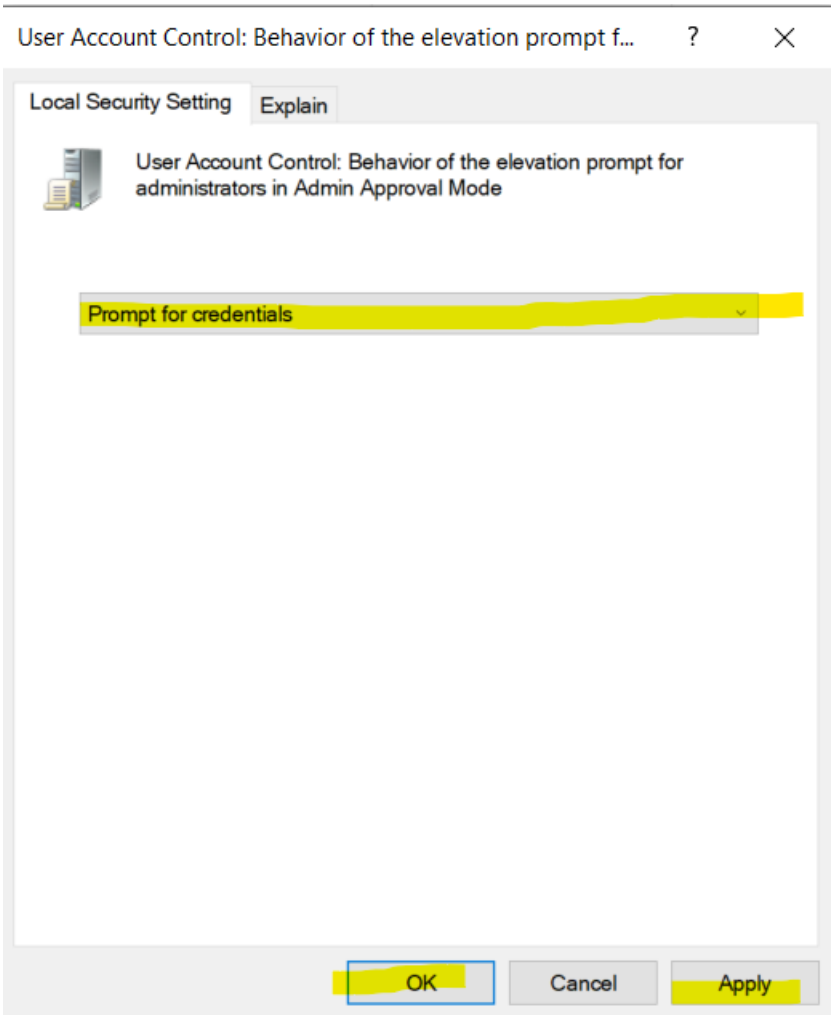

User Account Control: Detect application installations an...
Local Security Setting
Explain
User Account Control: Detect application installations and prompt for elevation
Enabled
Disabled
OK
Cancel
Apply


User Account Control: Only elevate UIAccess applications ...
Local Security Setting
Explain
User Account Control: Only elevate UIAccess applications that are installed in secure locations
Enabled
Disabled
OK
Cancel
Apply


User Account Control: Run all administrators in Admin Ap...
Local Security Setting
Explain
User Account Control: Run all administrators in Admin Approval Mode
Enabled
Disabled
OK
Cancel
Apply

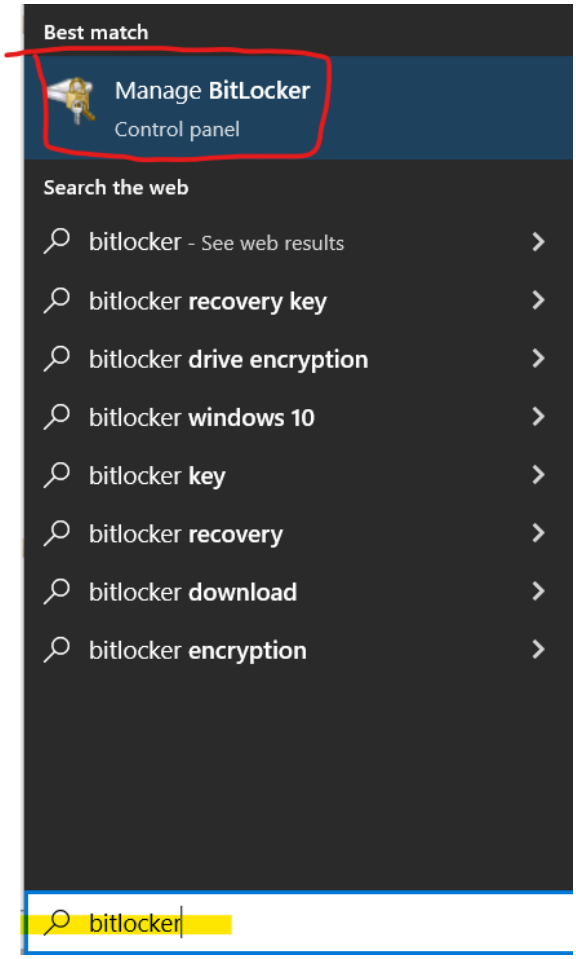

User Account Control: Switch to the secure desktop when ...
Local Security Setting
Explain
User Account Control: Switch to the secure desktop when prompting for elevation
Enabled
Disabled
OK
Cancel
Apply


User Account Control: Virtualize file and registry write fail...
Local Security Setting
Explain
User Account Control: Virtualize file and registry write failures to per-user locations
Enabled
Disabled
OK
Cancel
Apply

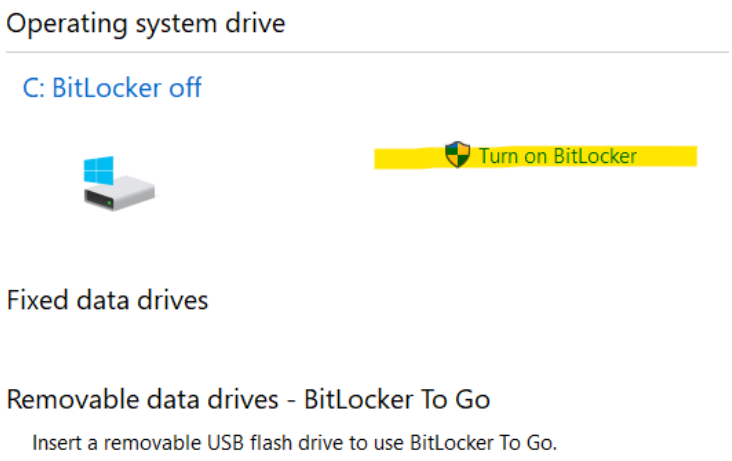

User Account Control: Behavior of the elevation prompt f...
Local Security Setting
Explain
User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode
Prompt for credentials
OK
Cancel
Apply

Enabling BitLocker

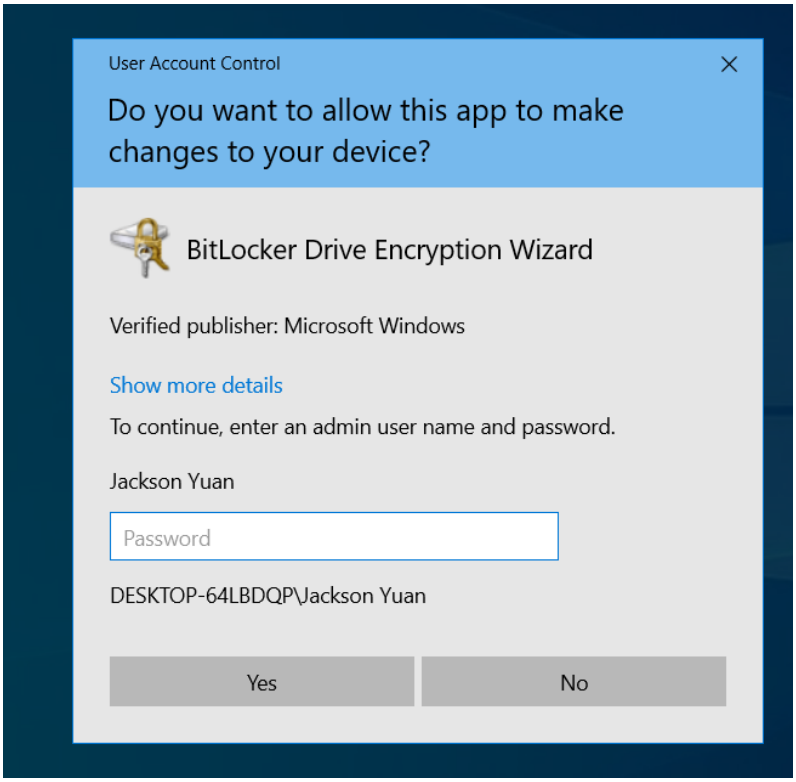
Finally, we now enable BitLocker from all the security steps we've applied from above



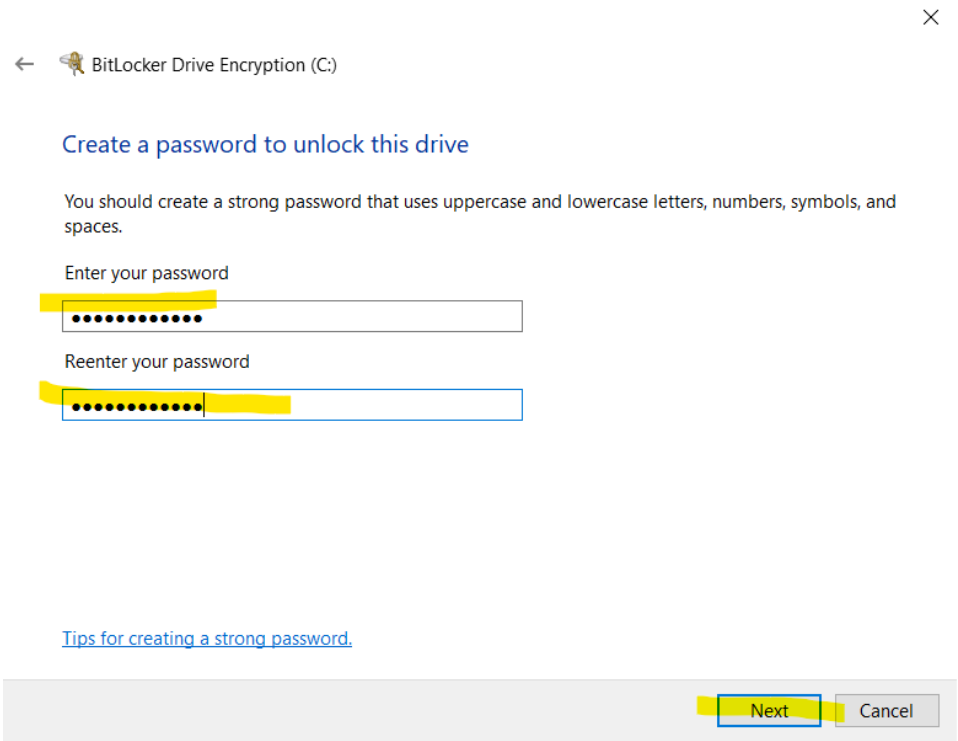
(Type in "bitlocker" in the search bar after pressing the ⊞ key)



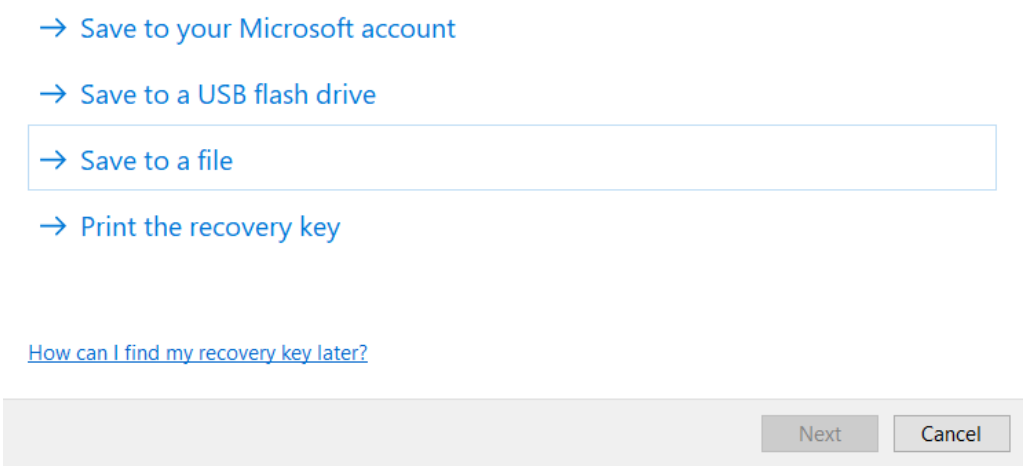
(Click “turn on BitLocker”)



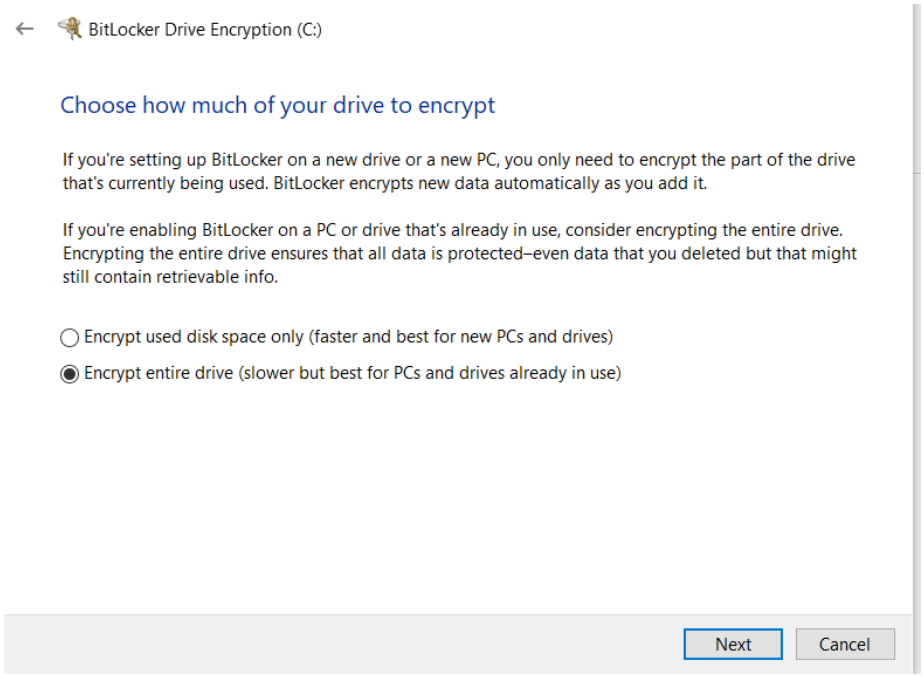
(Type your PC password in)



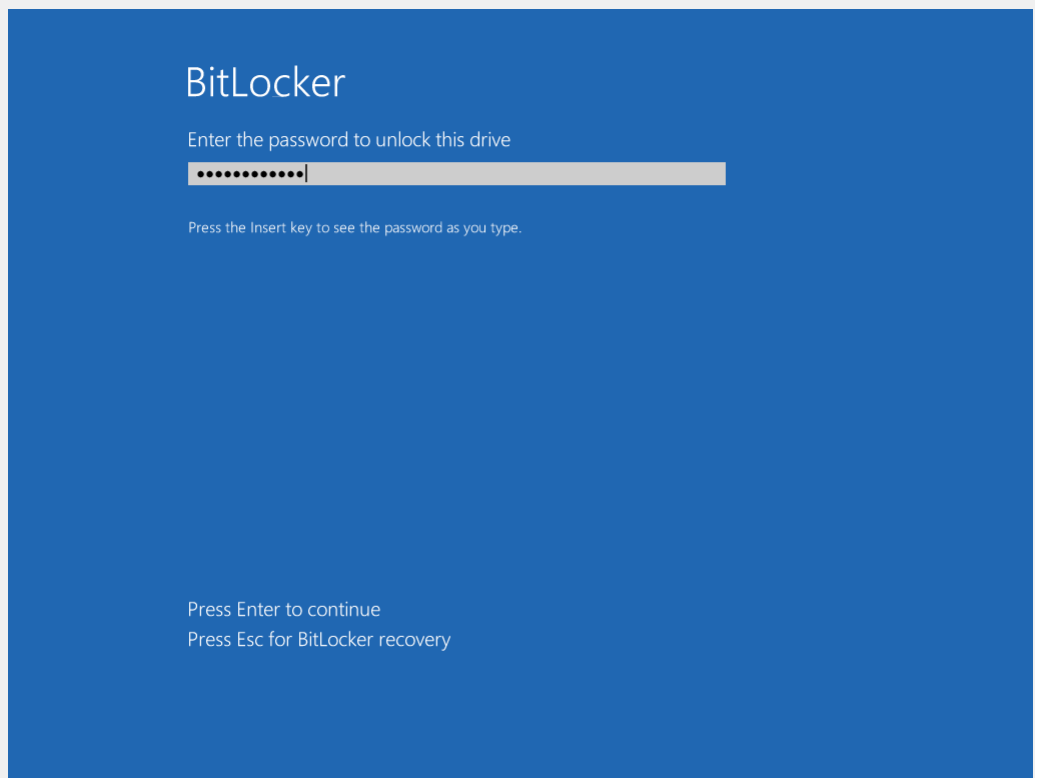
(Enter a password of choice)



(pick an option to save this password)



(Pick “Encrypt entire drive”)



(Once configured properly, you should see this blue screen to enter password)

Part 2 – Auditing on Windows 10

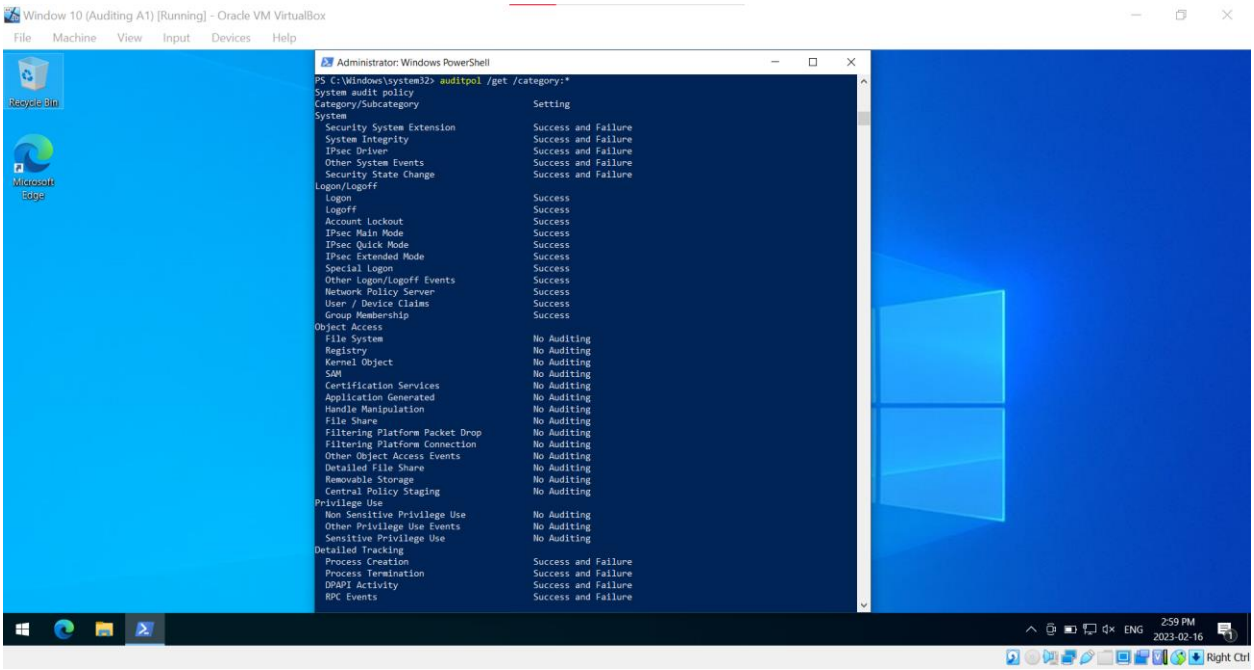
2.1 Enable Auditing

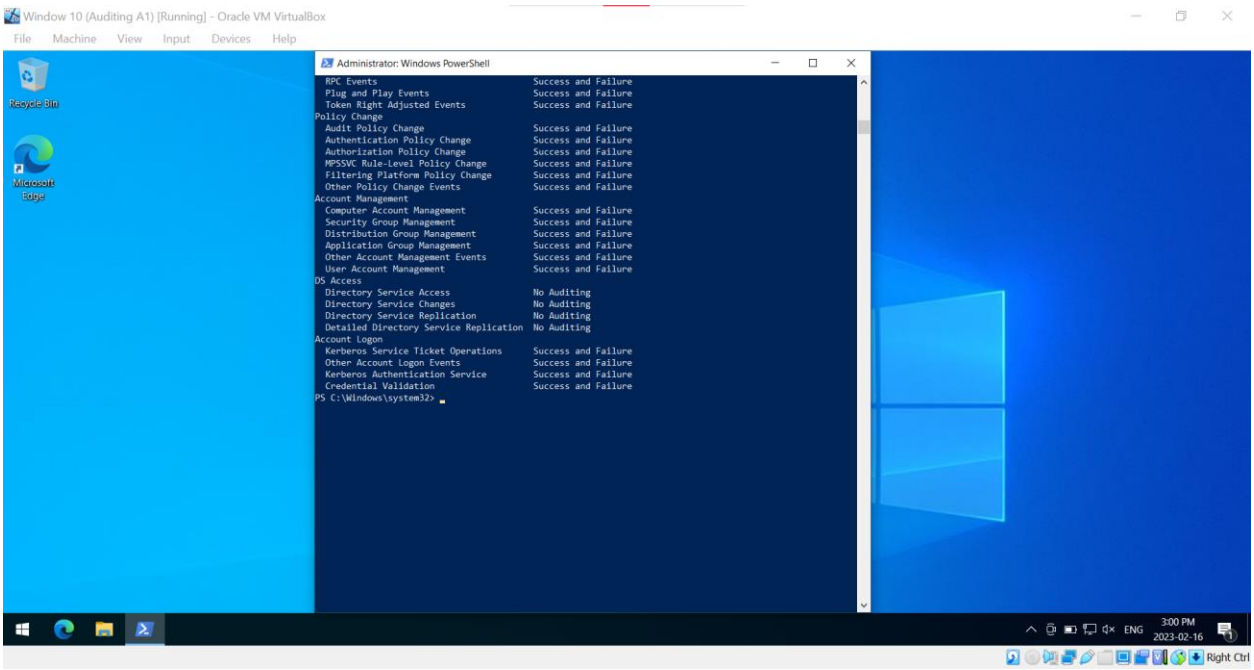
Auditing for this Windows 10 virtual machine was enabled using the command line tool auditpol or Local Group Policy Editor (gpedit.msc) to edit audit policies. Splunk was used to capture and analyze event logs.

Audit policies were enabled according to Microsoft's Stronger Audit Policy Recommendations. To accomplish this, the following commands were run in command prompt in administrator mode:

```
# Account Logon
auditpol /set /category:"Account Logon"  /subcategory:"Credential Validation" /success:enable /failure:enable
auditpol /set /category:"Account Logon"  /subcategory:"Kerberos Authentication Service" /success:enable /failure:enable
auditpol /set /category:"Account Logon"  /subcategory:"Kerberos Service Ticket Operations" /success:enable /failure:enable
auditpol /set /category:"Account Logon"  /subcategory:"Other Account Logon Events" /success:enable /failure:enable

# Account Management
auditpol /set /category:"Account Management"  /subcategory:"Computer Account Management" /success:enable /failure:enable
auditpol /set /category:"Account Management"  /subcategory:"Other Account Management Events" /success:enable /failure:enable
auditpol /set /category:"Account Management"  /subcategory:"Security Group Management" /success:enable /failure:enable
auditpol /set /category:"Account Management"  /subcategory:"User Account Management" /success:enable /failure:enable

# Detailed Tracking
auditpol /set /category:"Detailed Tracking"  /subcategory:"DPAPI Activity" /success:enable /failure:enable
auditpol /set /category:"Detailed Tracking"  /subcategory:"Process Creation" /success:enable /failure:enable

# Logon and Logoff
auditpol /set /category:"Logon/Logoff" /subcategory:"Account Lockout" /success:enable /failure:disable
auditpol /set /category:"Logon/Logoff" /subcategory:"Logoff" /success:enable /failure:disable
auditpol /set /category:"Logon/Logoff" /subcategory:"Logon" /success:enable /failure:enable
auditpol /set /category:"Logon/Logoff" /subcategory:"Special Logon" /success:enable /failure:disable

# Policy Change
auditpol /set /category:"Policy Change" /subcategory:"Audit Policy Change" /success:enable /failure:enable
auditpol /set /category:"Policy Change" /subcategory:"Authentication Policy Change" /success:enable /failure:enable

# System
auditpol /set /category:"System" /subcategory:"IPsec Driver" /success:enable /failure:enable
auditpol /set /category:"System" /subcategory:"Security State Change" /success:enable /failure:enable
auditpol /set /category:"System" /subcategory:"Security System Extension" /success:enable /failure:enable
auditpol /set /category:"System" /subcategory:"System Integrity" /success:enable /failure:enable
```

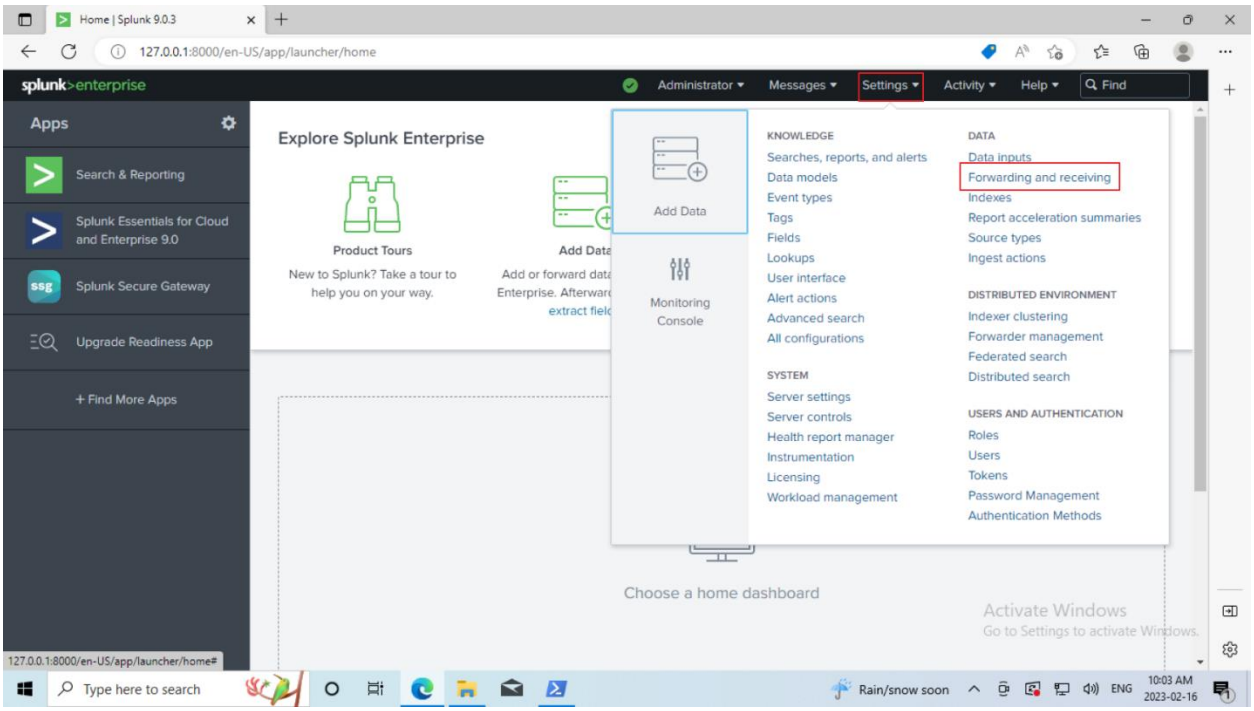
A screenshot of the currently enabled audit policies is shown below:



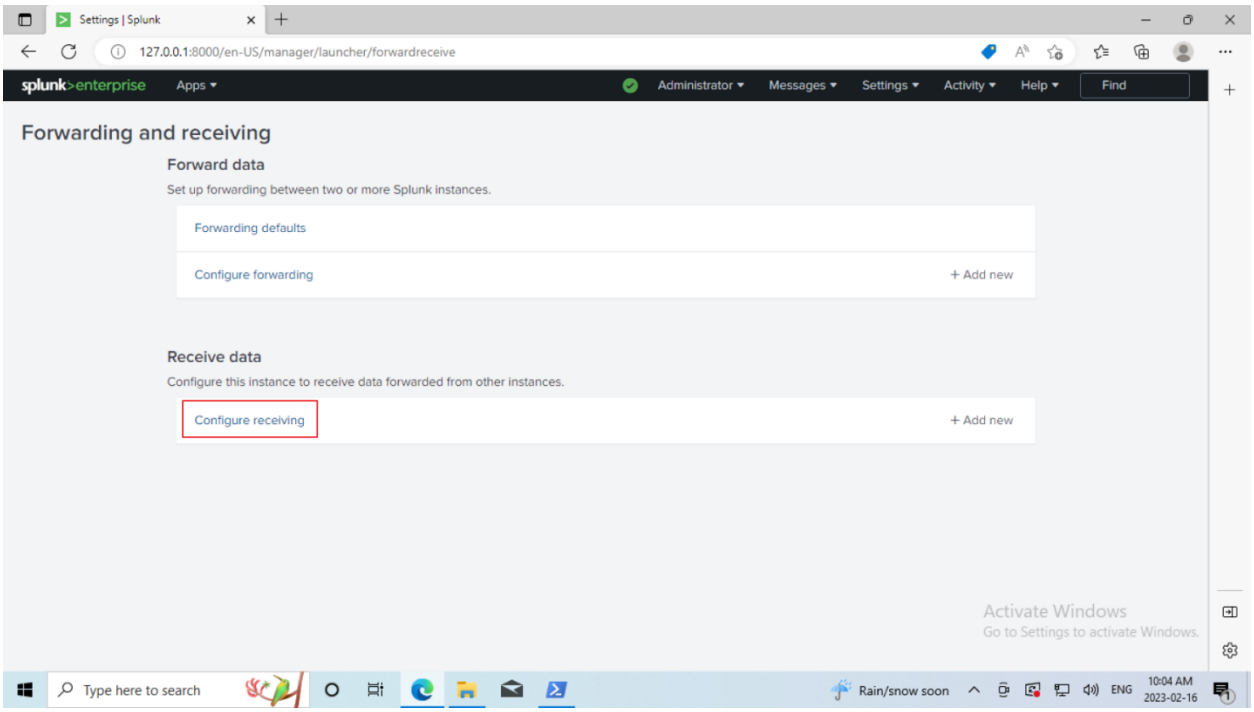


Splunk was then installed the same Windows 10 virtual machine. Splunk was configured to receive logs by selecting the following options:

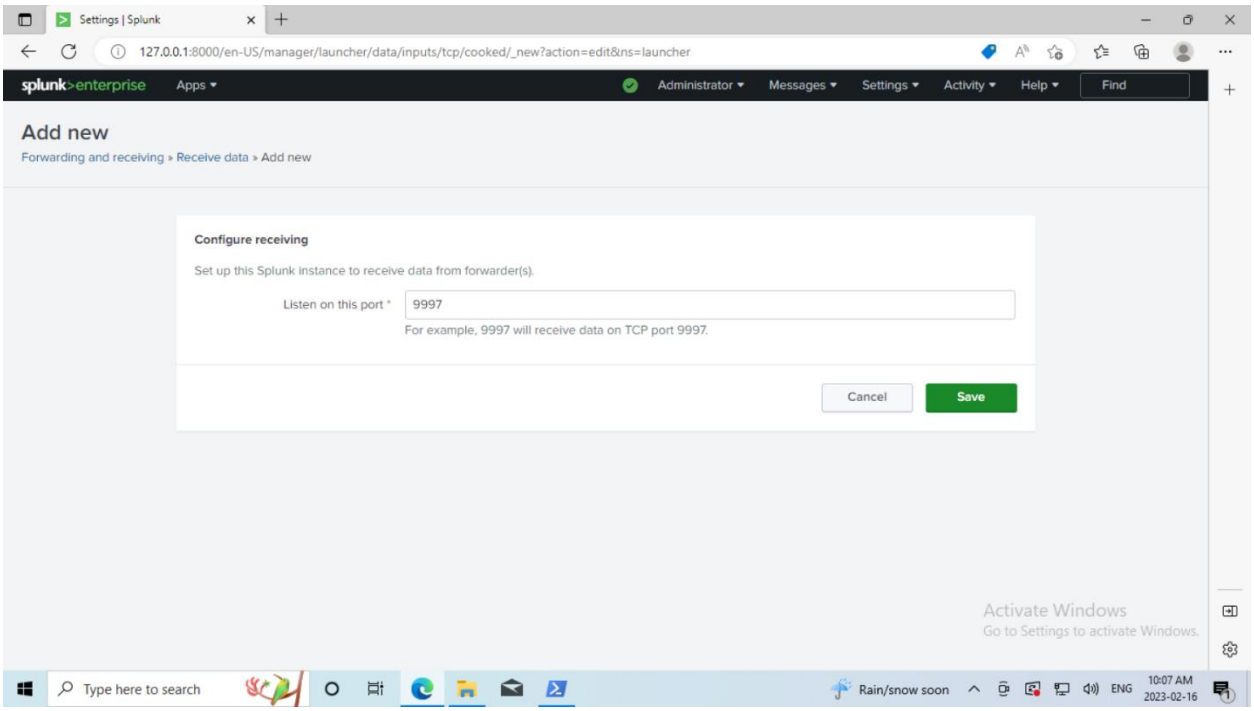
Settings > Forwarding and receiving

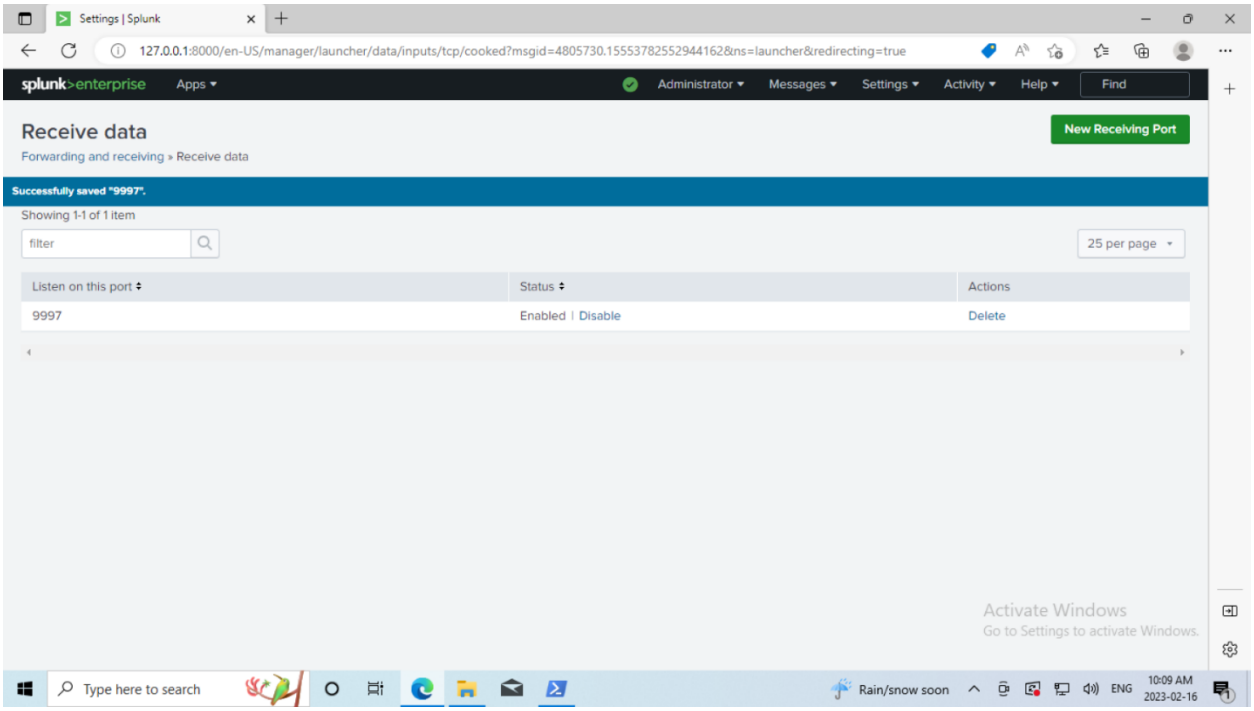


Configure receiving

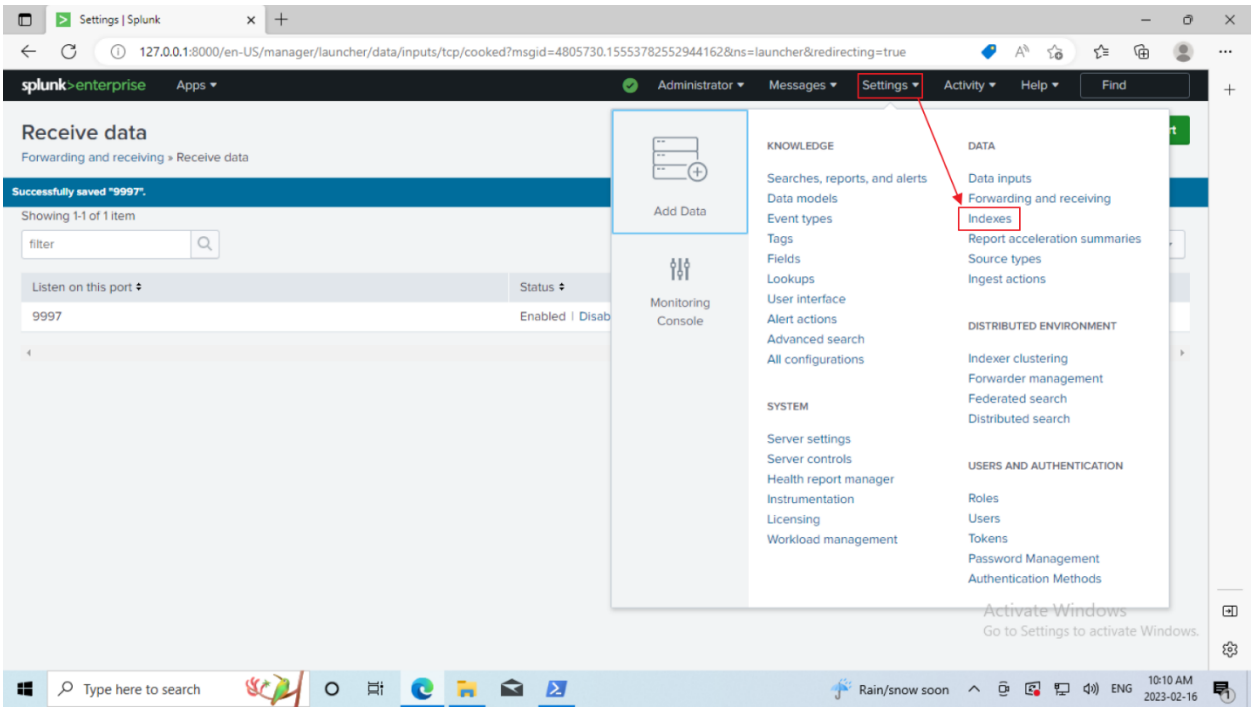


Add a New Receiving Port where Splunk will listen for the Universal Forwarder. The default port of 9997 was used.

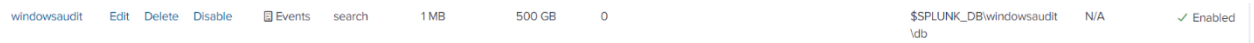




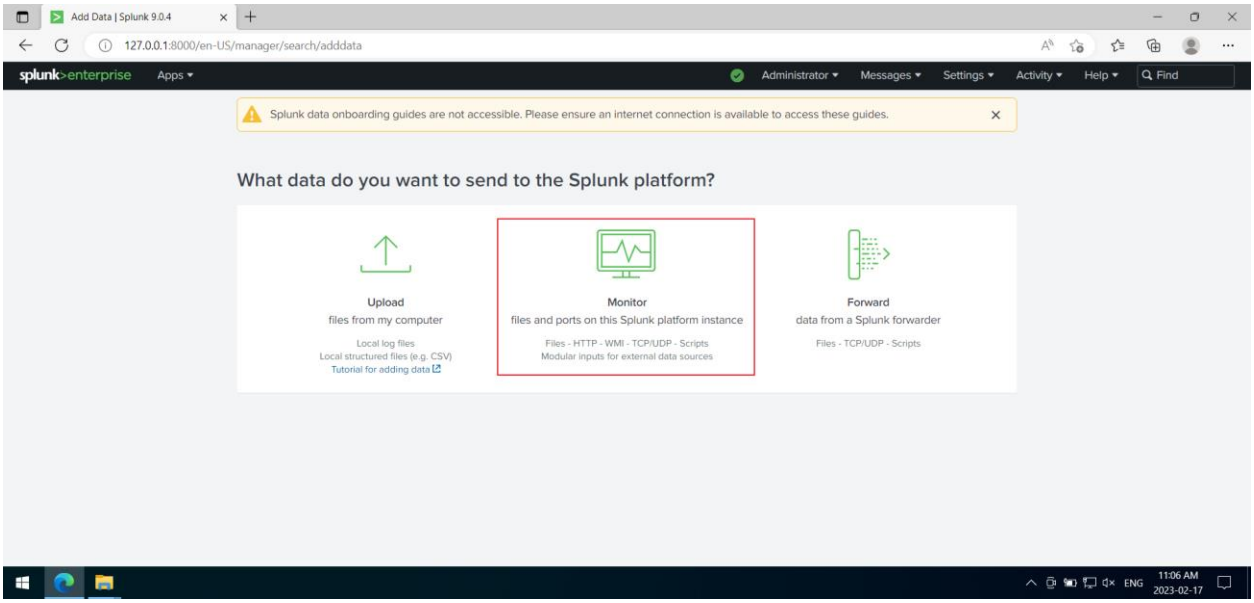
The next step is to create an Index for the incoming logs. Navigate to Settings > Indexes.



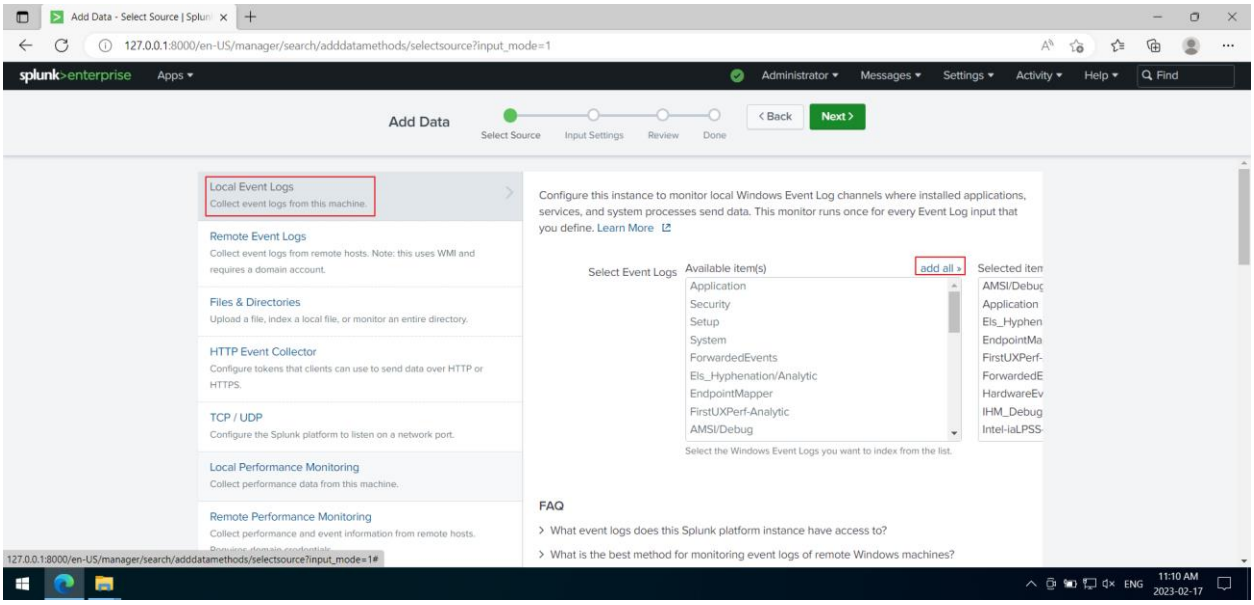
A New Index was created called windowsaudit.



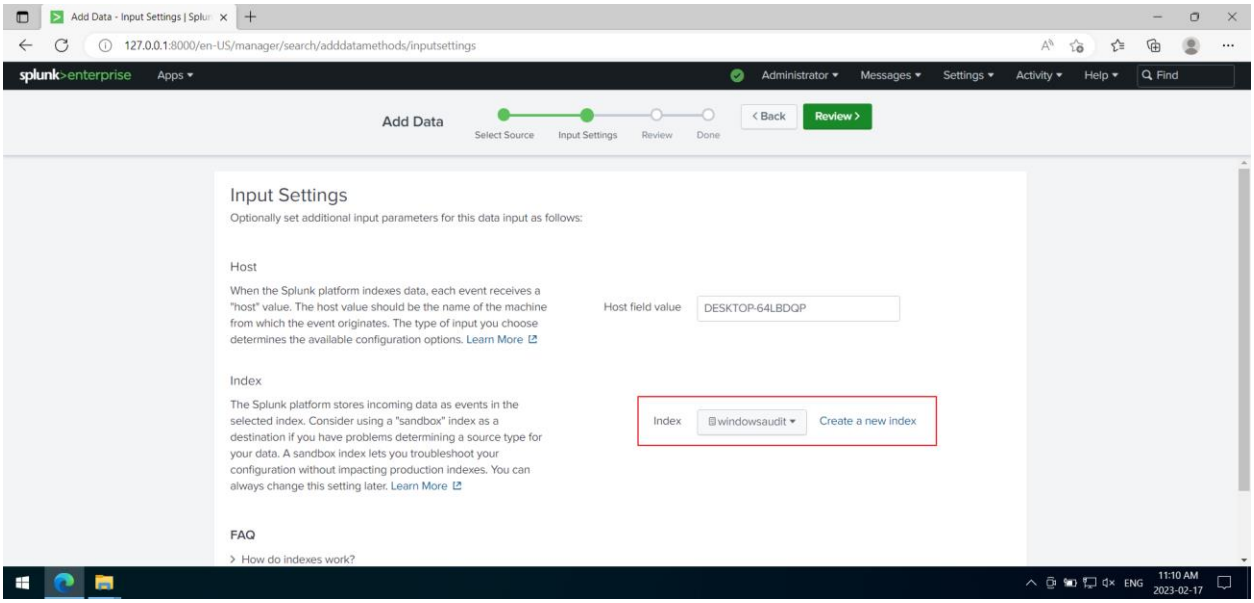
To start capturing logs on the current machine, navigate to Settings > Add data > Monitor.



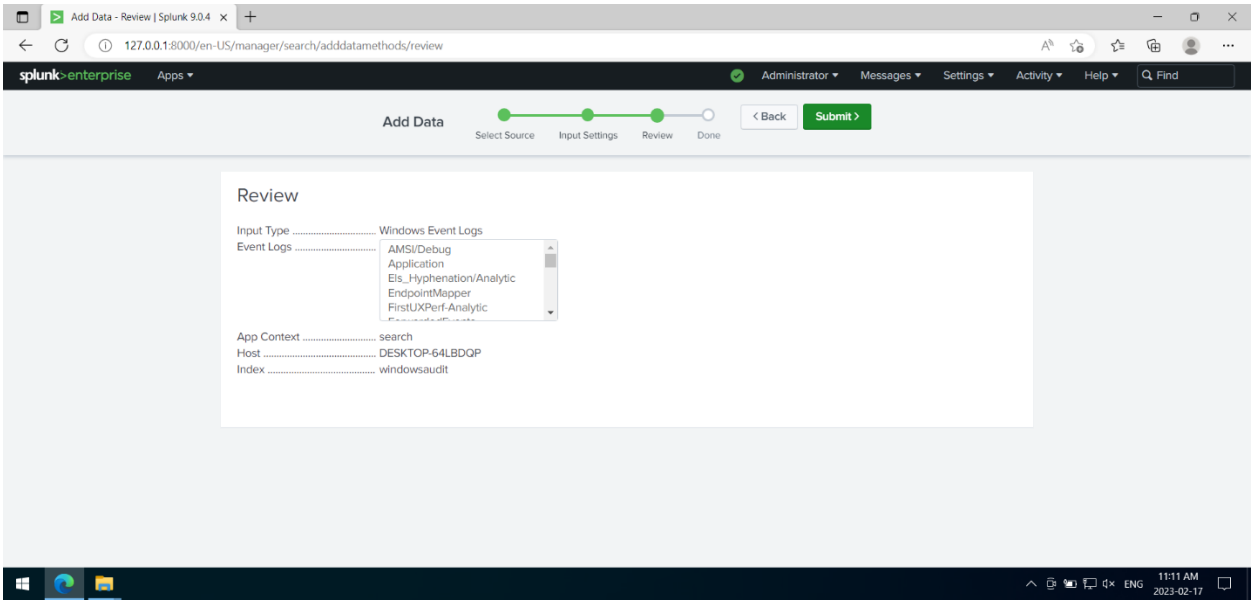
Then select: Local Event Logs and add all logs.



Change the index to the one we created, windowsaudit:



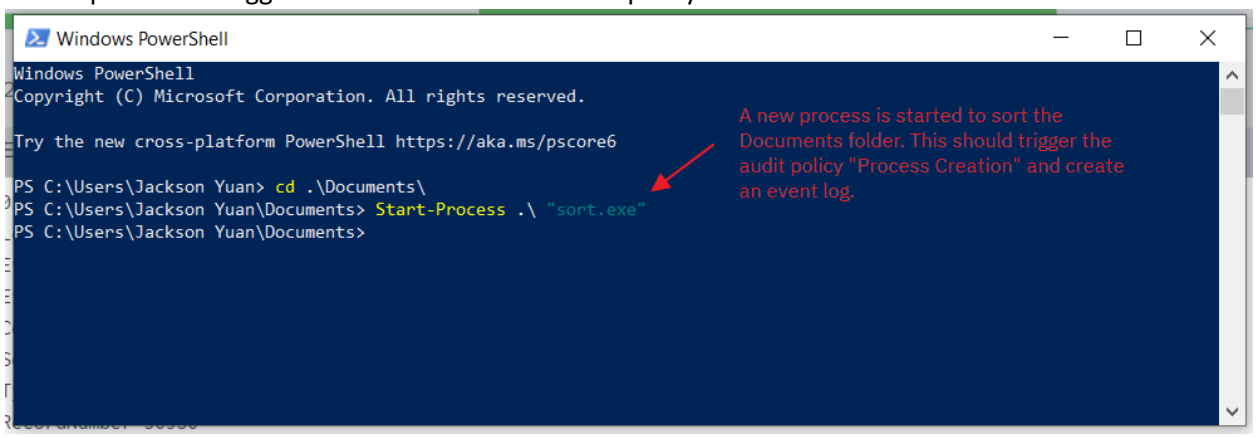
Review and submit.

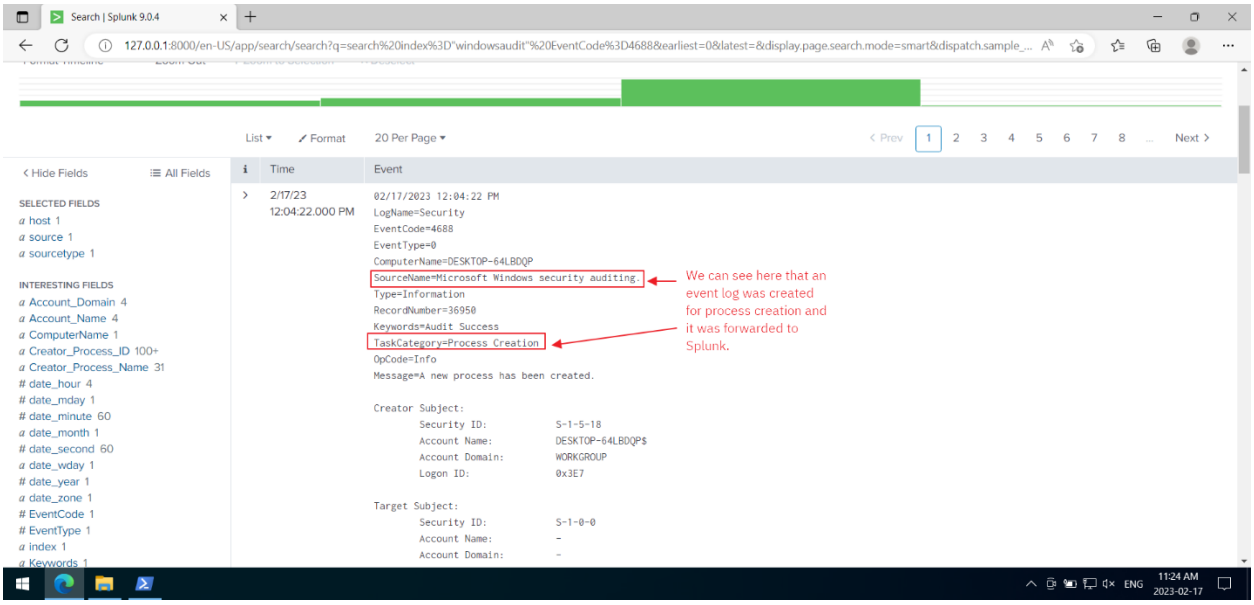


2.2 Generate Audit Events

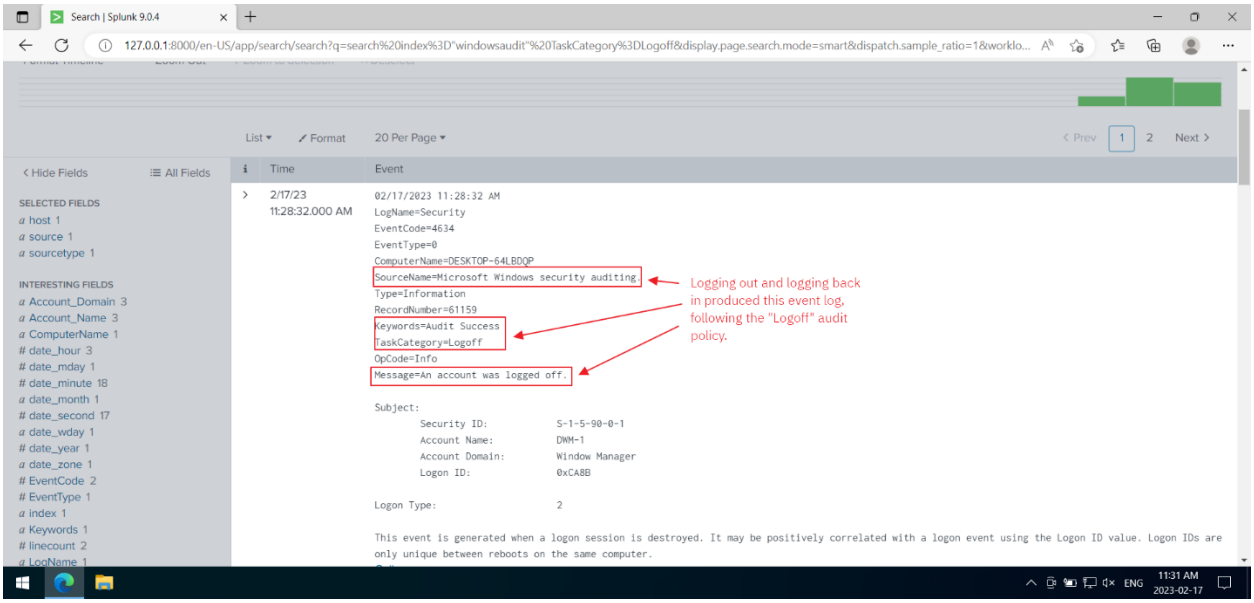
The following actions were done to generate audit logs:

1. Start a process to trigger the **Process Creation** audit policy.



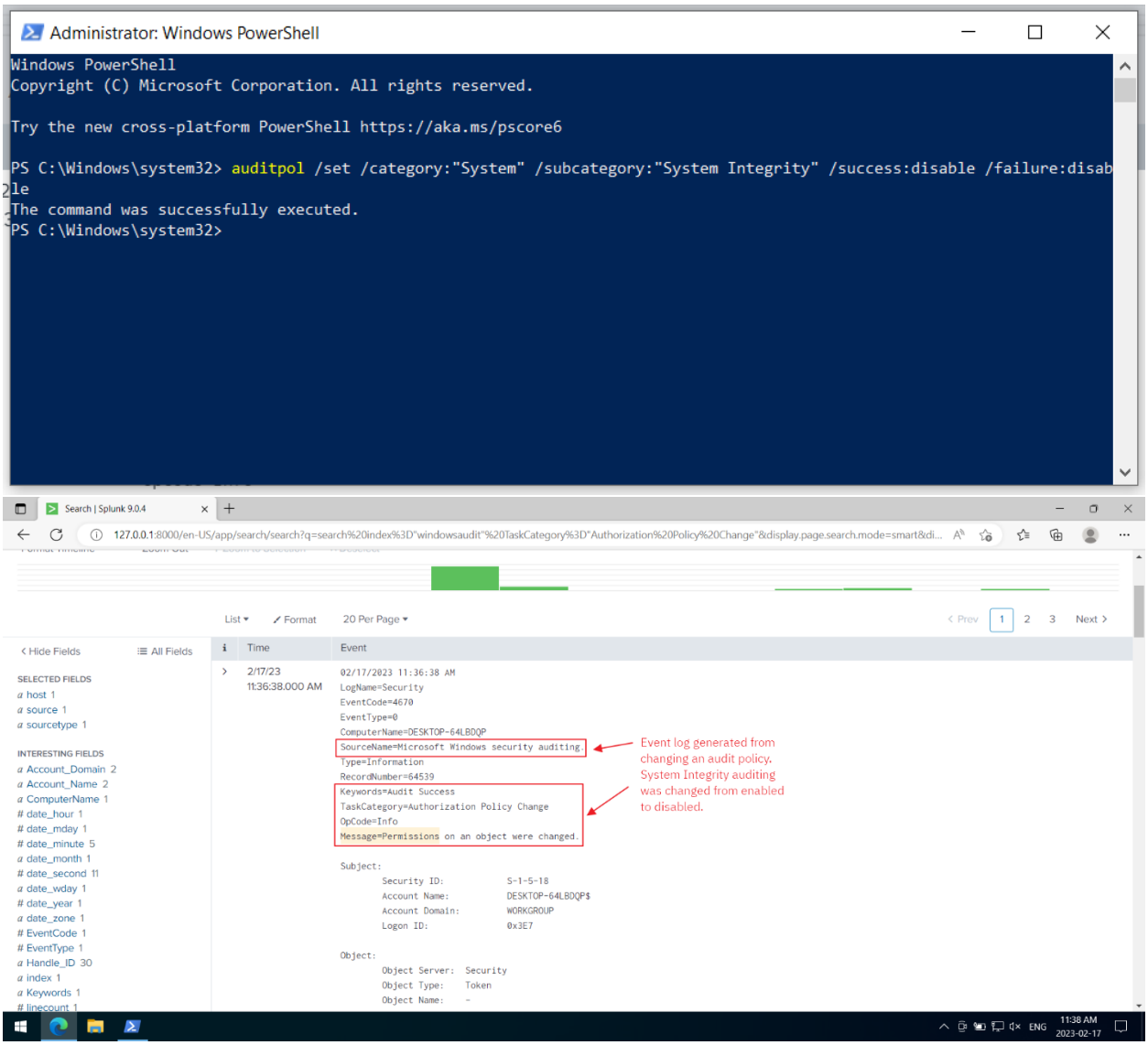


2. Log out of the current user account to trigger the **Logoff** audit policy.



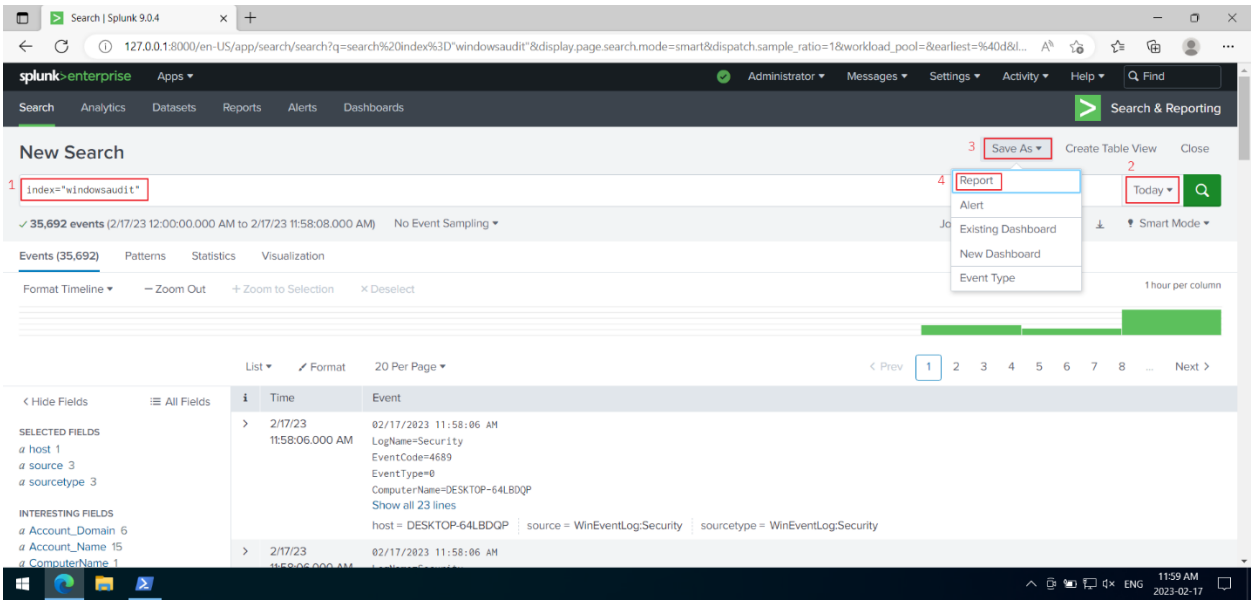
3. Change an audit policy to trigger the **Audit Policy Change** event.
   The **System Integrity** policy was changed by entering the following command in powershell:

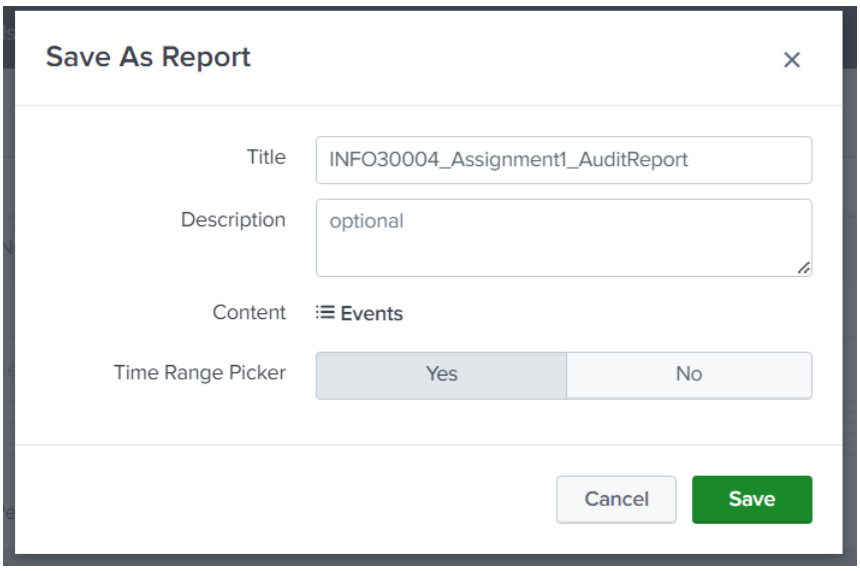
```
auditpol /set /category:"System" /subcategory:"System Integrity" /success:disable /failure:disable
```



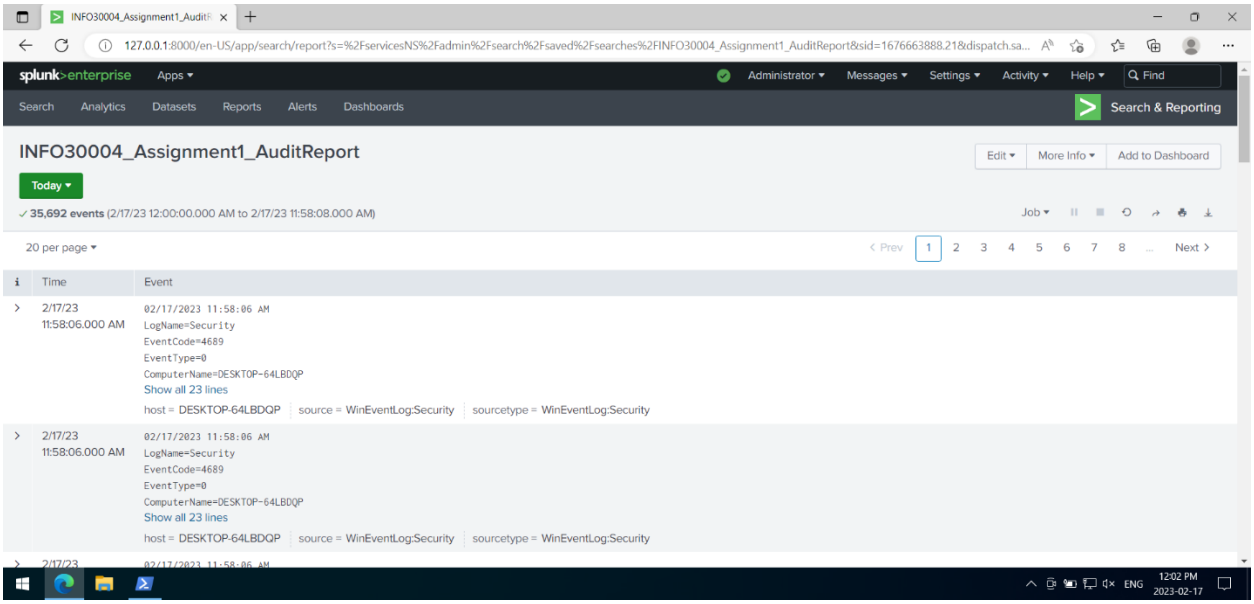
2.3 Produce an Audit Report

To create a report of the forwarded event logs in Splunk, we can search for all audit logs generated today and save it as a report.





We can then view the audit report in Splunk.



The report can be exported as a pdf by creating a new dashboard and then selecting Export > Export PDF.

References

https://www.lifars.com/wp-content/uploads/2020/11/Guide-to-Hardening-Windows-10.pdf

https://helpcenter.itopia.com/en/articles/4859965-restricting-application-access-using-applocker#:~:text=In%20the%20GPO%20Editor%2C%20navigate,and%20select%20Create%20Default%20Rules.

https://ourtechroom.com/fix/addinprocess-exe-how-do-i-remove-delete-it/

https://www.tenforums.com/tutorials/87609-change-account-lockout-threshold-local-accounts-windows-10-a.html

https://attack.mitre.org/techniques/T1546/003/

https://www.cyber.gov.au/acsc/view-all-content/publications/hardening-microsoft-windows-10-version-21h1-workstations

https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations