

8/5/2021

# Microsoft Security and Compliance Toolkit

Gaganpreet Singh

## Contents

|  |    |
|--|----|
| <b>1 Security Template</b>   | 3  |
| 1.1 Account Lockout Threshold  | 3  |
| 1.2 Maximum Password age   | 4  |
| 1.3 Minimum Password Length  | 5  |
| 1.4 Password Must Meet Complexity Requirements   | 7  |
| 1.5 Accounts: Guest Account Status   | 8  |
| <b>2 Advance Audit Configuration</b>   | 9  |
| 2.1 Audit Credential Validation  | 10 |
| 2.2 Audit Kerberos Authentication Service  | 12 |
| 2.3 Audit Kerberos Service Ticket Operations   | 13 |
| 2.4 Audit Account Lockout  | 15 |
| 2.5 Audit Logon  | 16 |
| <b>3 Windows Defender Firewall</b>   | 17 |
| 3.1 Firewall State   | 18 |
| 3.2 Inbound Connections  | 20 |
| 3.3 Outbound Connections   | 20 |
| 3.4 Display a Notification   | 21 |
| 3.5 Logging- Name, Size, Log dropped Packages and log successful connections                         | 23 |
| <b>4 Services</b>  | 24 |
| 4.1 XBOX Live Auth Manager   | 25 |
| 4.2 Xbox Live Game Save  | 27 |
| 4.3 Xbox Accessory Management Service  | 28 |
| 4.4 XBOX Live Networking Service   | 29 |
| <b>5 Computer</b>  | 30 |
| 5.1 Ability to Enable/Disable LAN connections  | 30 |
| 5.2 Ability to Rename LAN connections  | 31 |
| 5.3 Prohibit Access to properties of a LAN connection  | 32 |
| 5.4 Prohibit deletions of remote access connections  | 34 |
| 5.5 Do not adjust default option to "Install Updates and Shut Down" in Shut Down windows dialog box. | 35 |
| <b>6 User</b>  | 36 |

|  |           |
|--|-----------|
| 6.1 Lock the Taskbar .....                             | 36        |
| 6.2 Hide the notification area .....                   | 38        |
| 6.3 Add Logoff to the Start Menu .....                 | 39        |
| 6.4 Remove Logoff to the Start Menu .....              | 39        |
| 6.5 Remove My Documents icon from the Start Menu ..... | 40        |
| <b>References .....</b>                                | <b>42</b> |

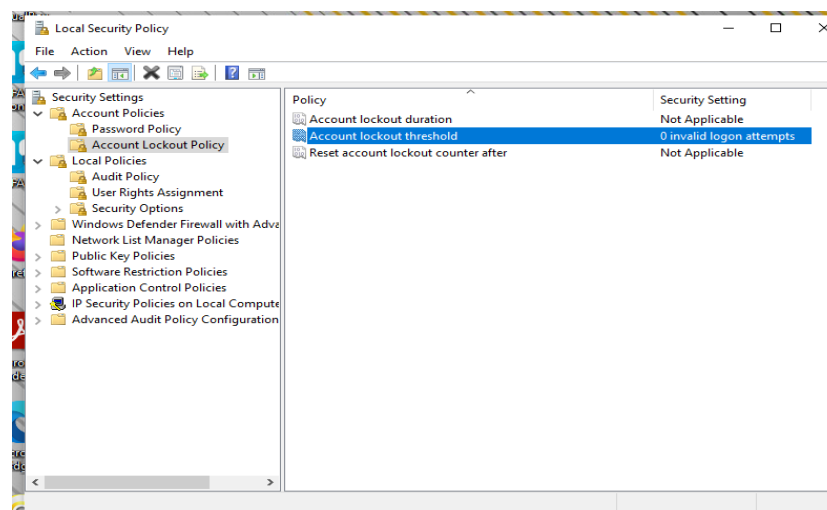
# 1 Security Template

There are several Security templates policies.

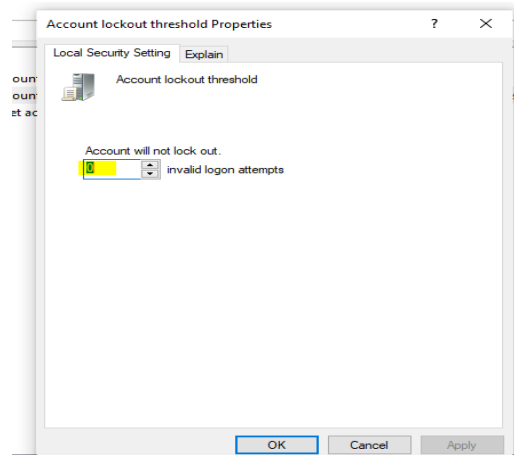
## 1.1 Account Lockout Threshold

- This policy determines after how many wrong passwords attempts the user account will be locked.
- Possible values for Account Lockout Threshold policy setting can be user defined number from 0 to 999 or not defined.
- **IMPORTANCE:** It is very important to set a value for this policy because it would prevent brute force attacks.

To Configure this policy Open **Local Security Policy**->Expand **Account Policies**->Click on **Account Lockout Policy**



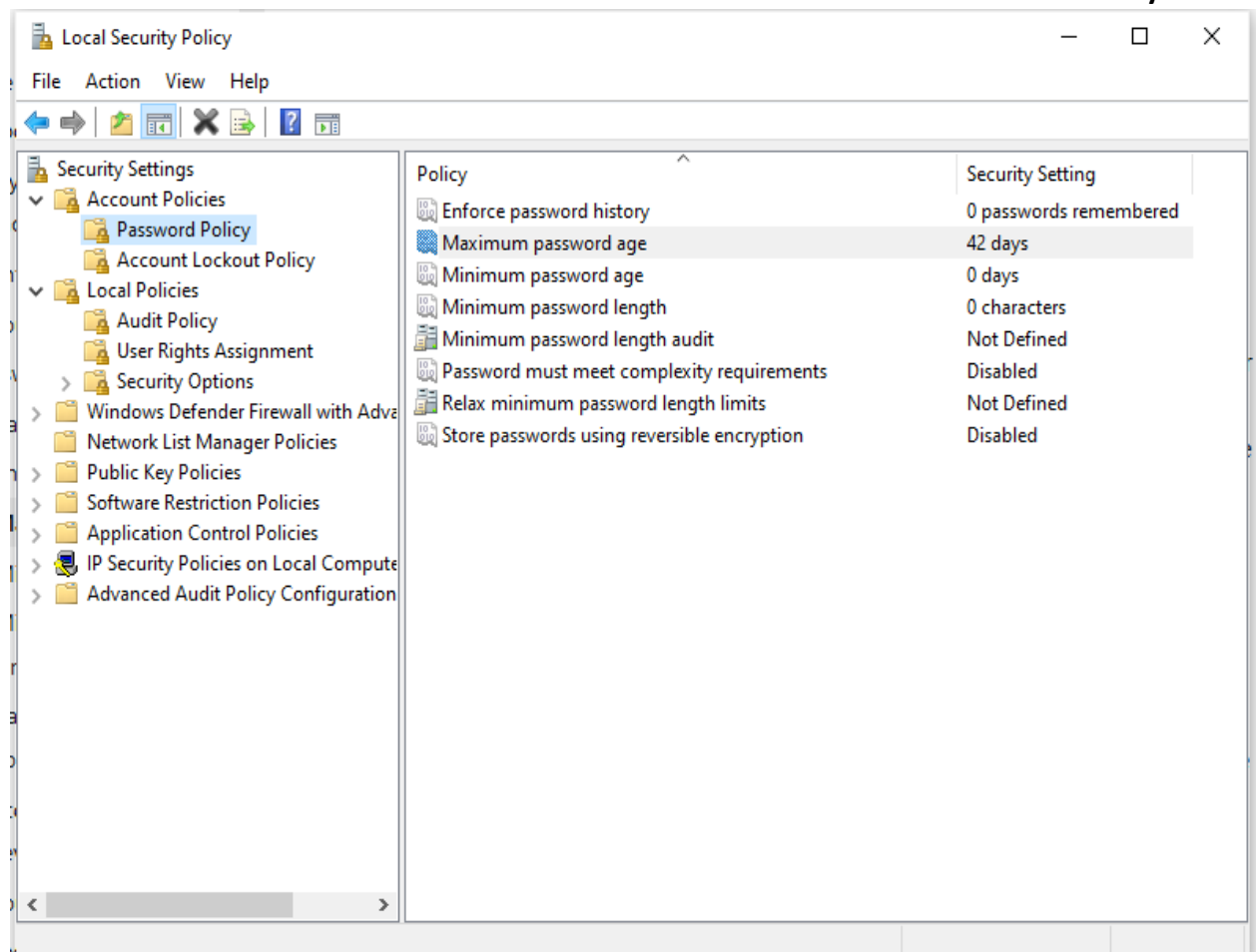
We can configure the policy value double clicking the policy and select a value for invalid logon attempts as shown in the image below.



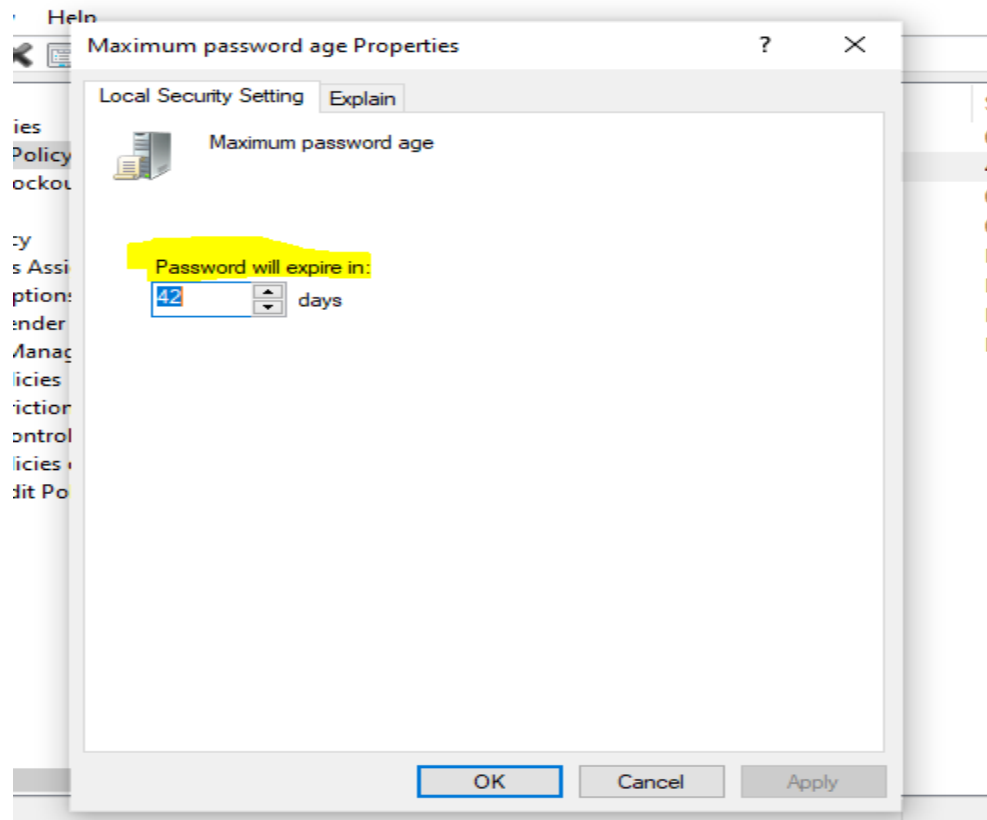
## 1.2 Maximum Password age

- This policy determines the time period for which a password can be used before the system will ask the user to change it.
- The value we can set the password to expires can range from 1 to 999 days or you can specify the password never expires by setting the value to be 0.
- **Importance:** It is known the longer the password exists, the higher the chance that it will be compromised by a brute force attack, as the attacker can gain valuable information about the users and his patterns. So to prevent this we need to set a expiry value.

To Configure this policy Open **Local Security Policy**->Expand **Account Policies**->Click on **Password Policy**



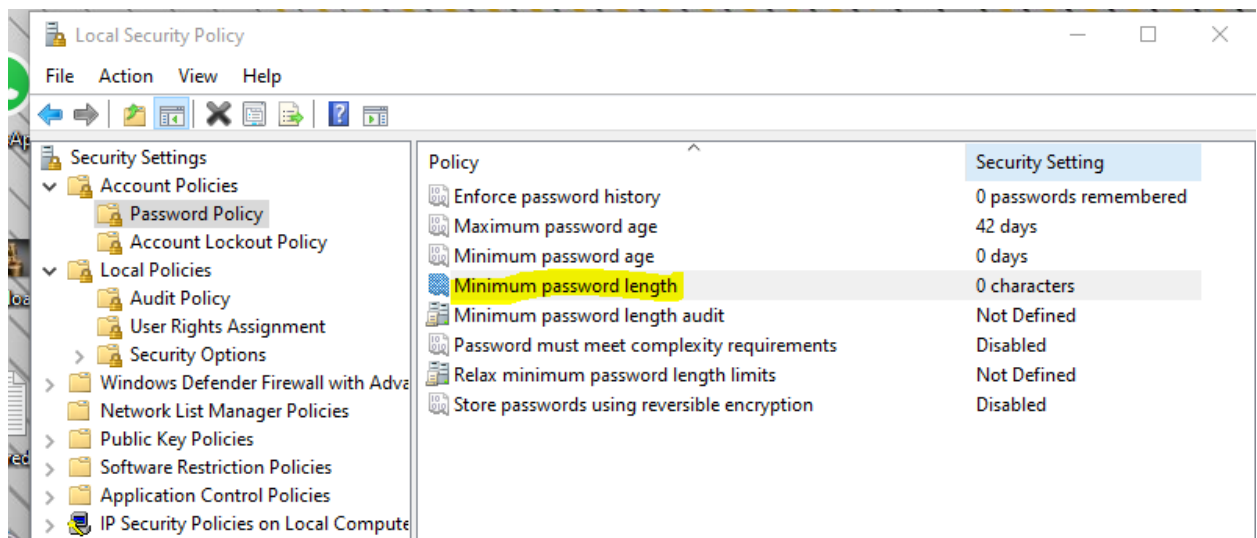
We can configure the policy value double clicking the policy and select a value for maximum password age as shown in the image below.



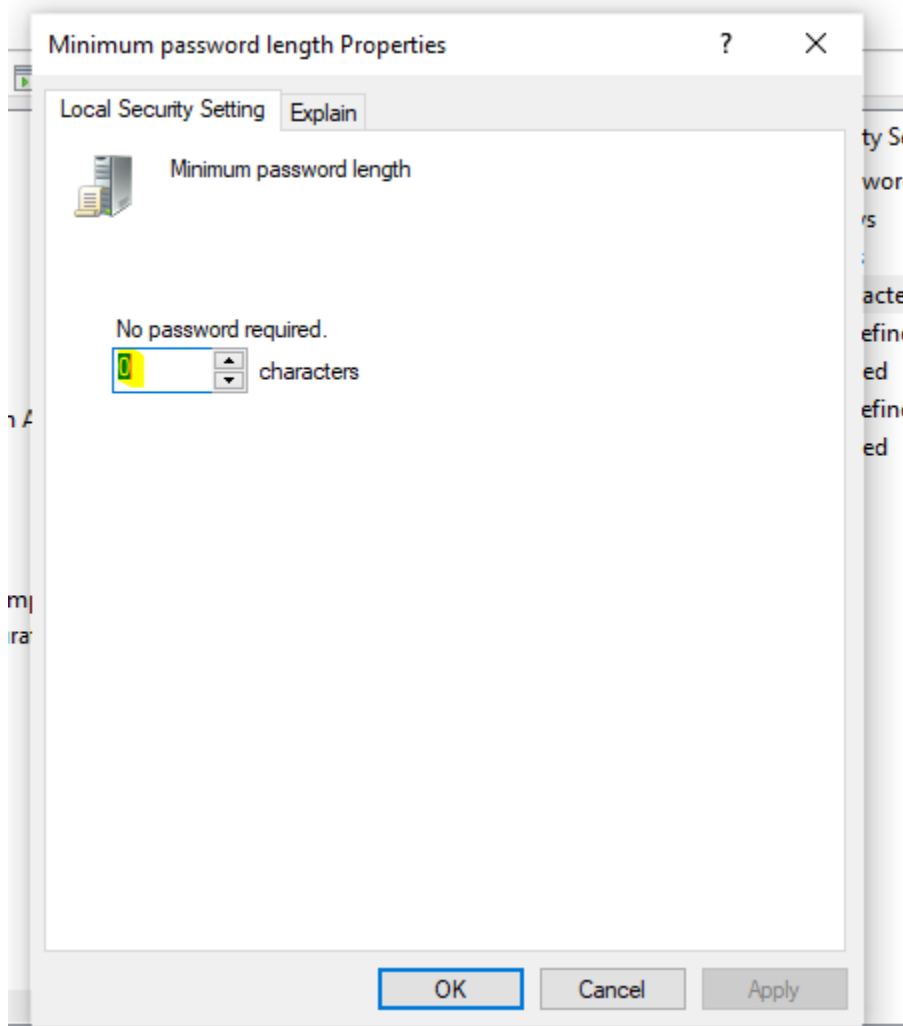
### 1.3 Minimum Password Length

- This policy determines the least number of characters required for a password creation.
- We can set a value between 1 to 14 characters including 1 and 14.
- **Importance:** This policy is very important to configure and the minimum value can be set to at least 8 characters because this length is adequate to prevent dictionary attacks and brute force attacks.

To Configure this policy Open **Local Security Policy**->Expand **Account Policies**->Click on **Password Policy**-> **Minimum Password length**



We can configure the policy value double clicking the policy and select a value for minimum password length as shown in the image below.



## 1.4 Password Must Meet Complexity Requirements

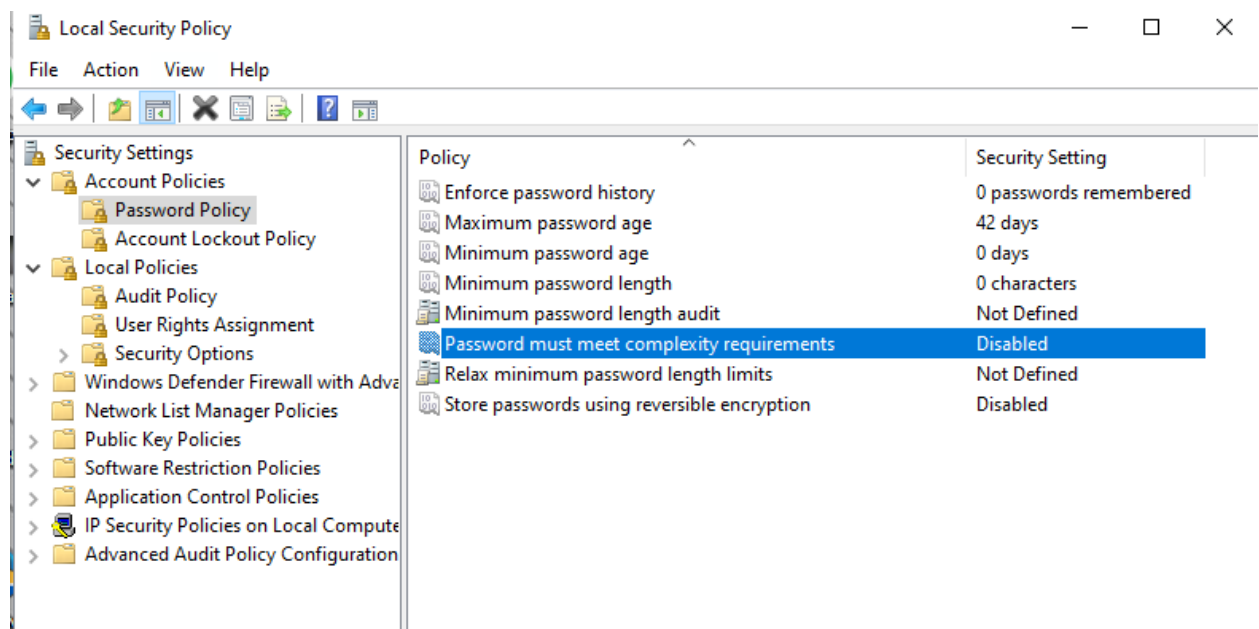
This policy determines that a password must meet a series of password guidelines which are listed below:

- Uppercase letters (A through Z)
- Lowercase letters (a through z)
- Base 10 digits (0 through 9)
- Special characters (!@#\$%^&\*)
- Many more

Possible values for the policy can be enabled or disabled.

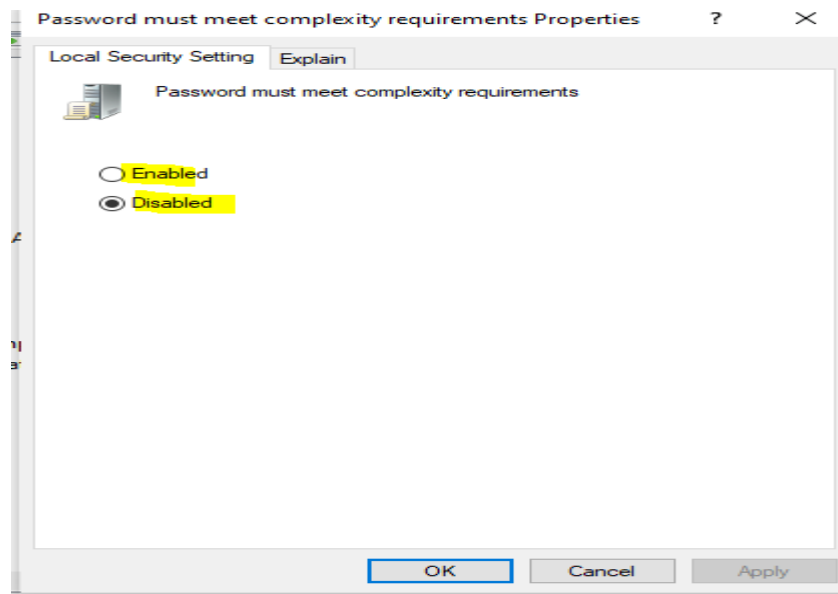
**Importance:** Passwords that contain only alphanumeric characters are very easy to crack so, we must increase the complexity of the password using these guidelines and to prevent brute force and dictionary attacks.

To Configure this policy Open **Local Security Policy**->Expand **Account Policies**->Click on **Password Policy**-> **Password must meet complexity requirements**



We can configure the policy value double clicking the policy and select enabled and disabled value as shown in the image below:

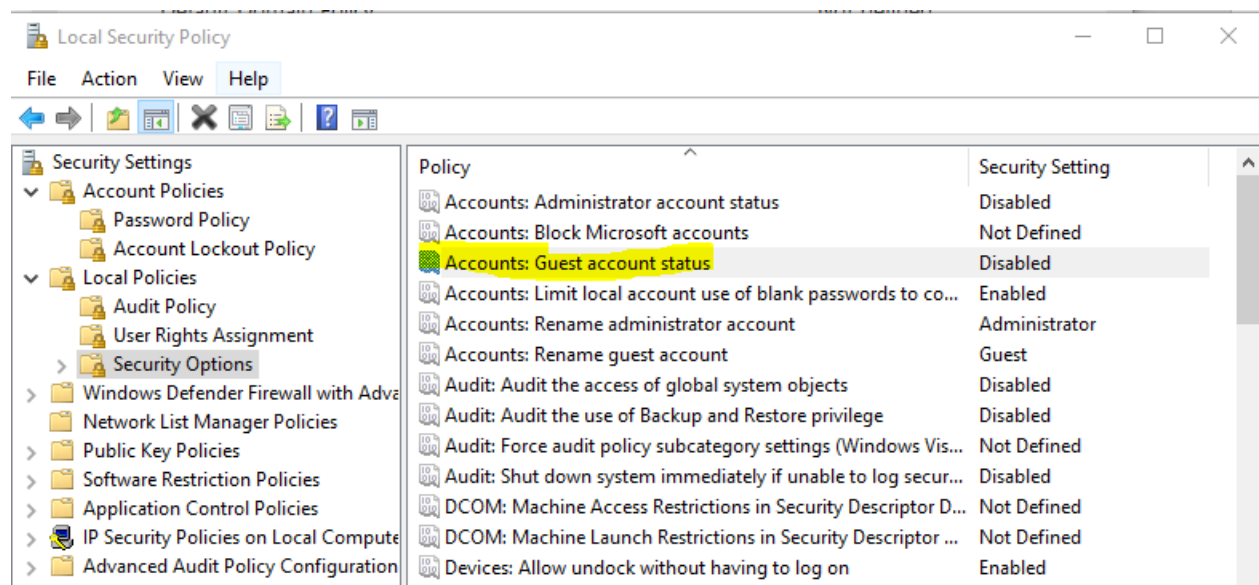




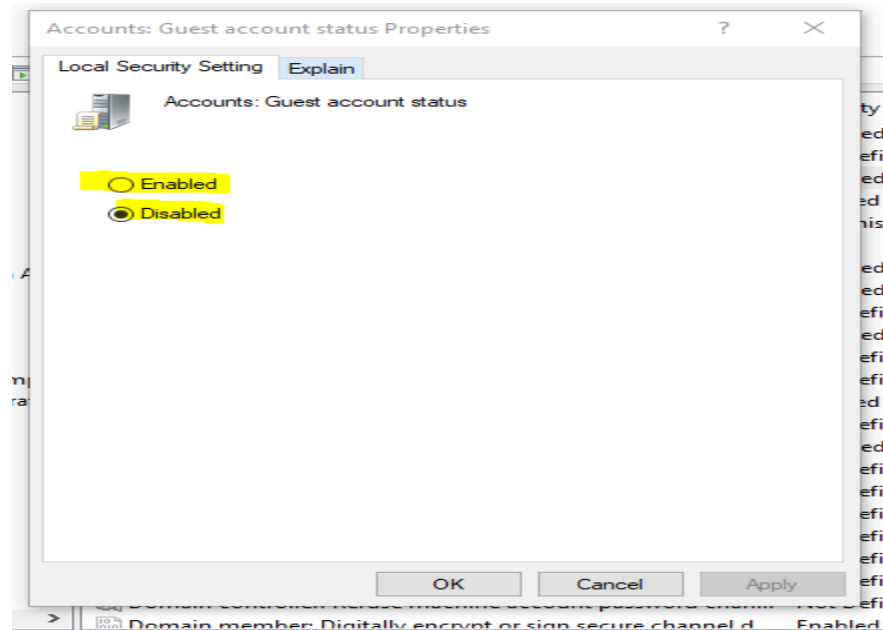
### 1.5 Accounts: Guest Account Status

- This policy determines whether the guest account is enabled or disabled.
- Enabling this account will allow unauthenticated users to access the system by logging on as a guest without any password
- **Importance: This policy must remain disabled to prevent unauthorized user access to the resources.**

To Configure this policy Open **Local Security Policy**->Expand **Local Policies**-> Click on **Security options**->**Account: Guest account status**.



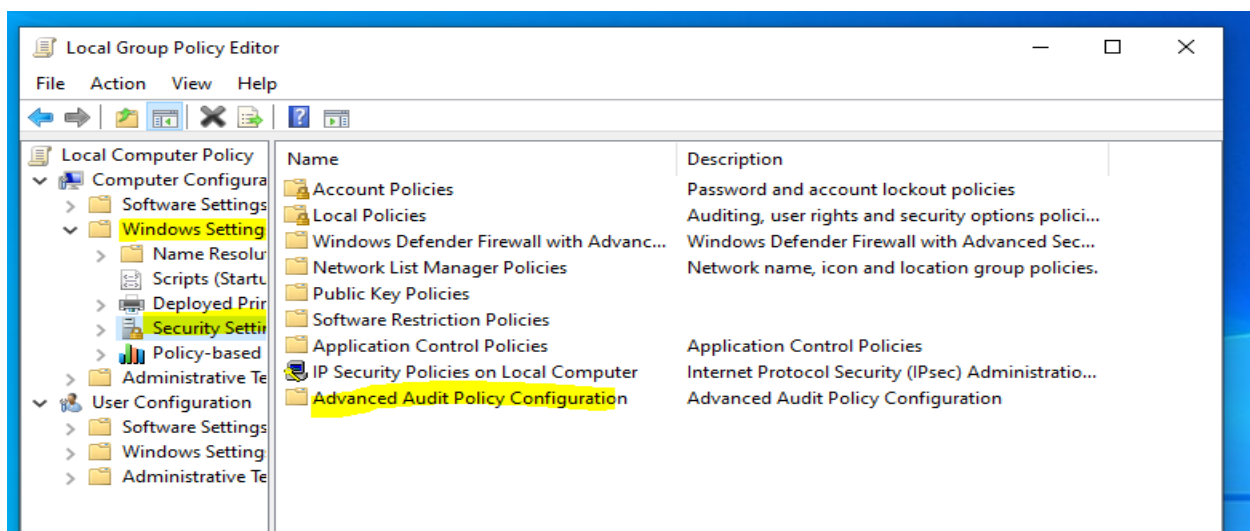
We can configure the policy value double clicking the policy and select enabled and disabled according to the requirement as shown in the image below:



## 2 Advance Audit Configuration

These policies help an organization with monitoring and auditing the activities of the system.

To configure the policy under Advance Audit Configuration Press Win + R Key-> in the run console type **gpedit.msc**->In the **Local Group Policy Editor**->expand **Windows Settings**-> Expand **Security Settings**->Click on **Advanced Audit Policy configuration**



On clicking the dropdown under Advanced Audit Policies, we will have different categories of policies.

The screenshot shows the Windows Security Policy console. On the left, the 'Advanced Audit Policy Configuration' folder is expanded, showing 'System Audit Policies - Local Group Policy Object'. On the right, a warning message states: 'When Advanced Audit Policy Configuration settings (Windows Vista or later) to override audit policy categories also be enabled.' Below this, there are links for 'More about' and 'Which editions of'. A summary table is displayed with the following data:

| Categories                    | Configuration  |
|-------------------------------|----------------|
| Account Logon                 | Not configured |
| Account Management            | Not configured |
| Detailed Tracking             | Not configured |
| DS Access                     | Not configured |
| Logon/Logoff                  | Not configured |
| Object Access                 | Not configured |
| Policy Change                 | Not configured |
| Privilege Use                 | Not configured |
| System                        | Not configured |
| Global Object Access Auditing | Not configured |

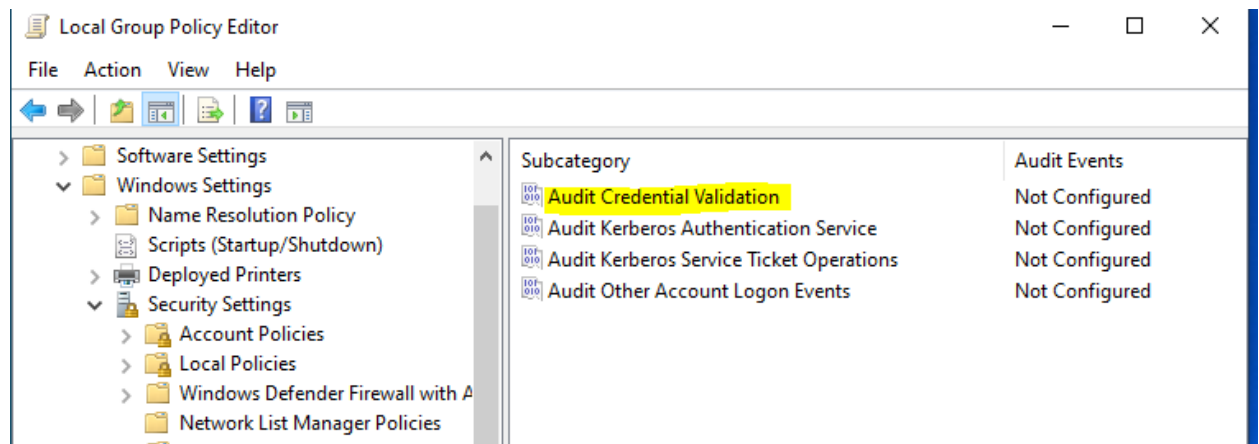
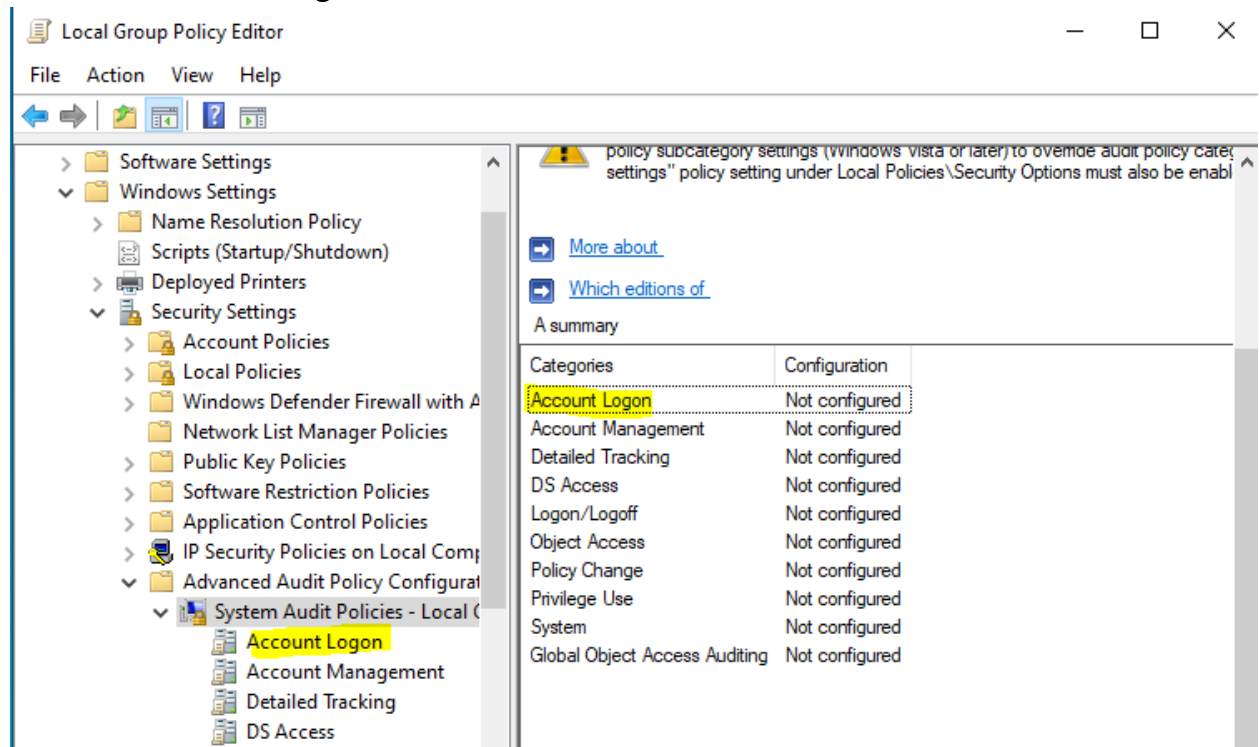
## 2.1 Audit Credential Validation

This policy determines whether the windows audit events on the credentials when a user attempts to logon.

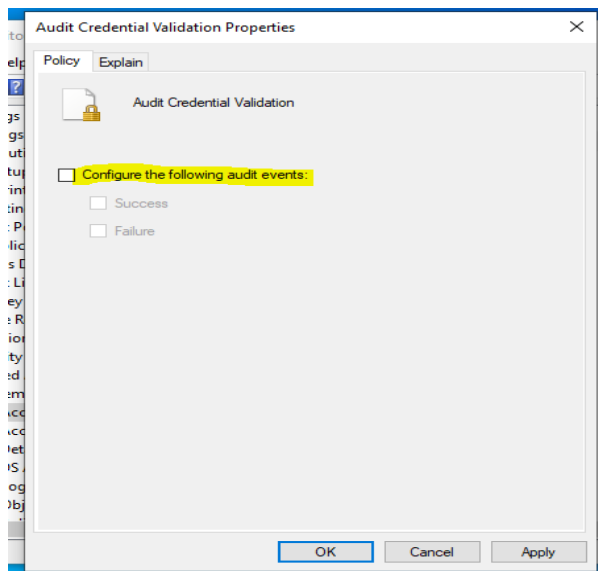
The default value for this policy is not configured.

**Importance:** It is important to audit whenever a user attempts to logon.

To configure the Policy, Navigate to **System Audit Policies-> Account Logon-> Double Click the Account Logon-> Select Audit Credential Validation-> Double Click It**



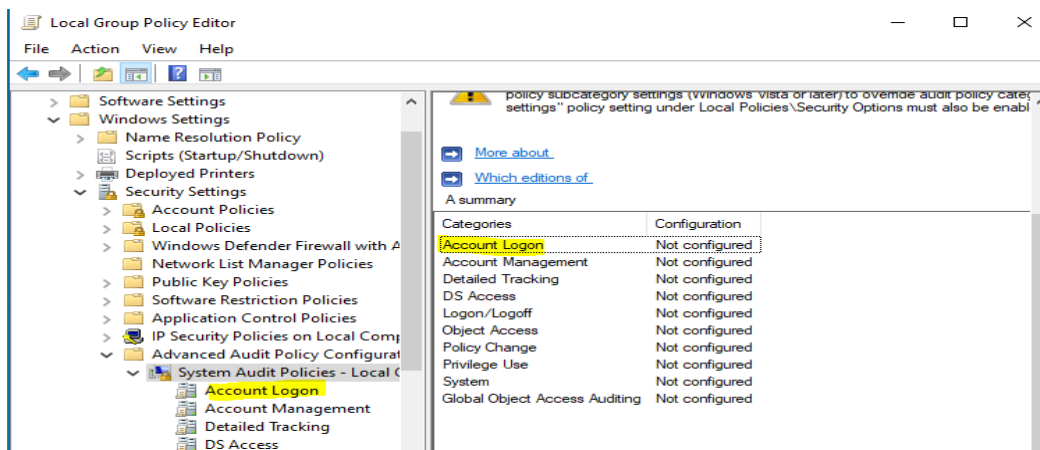
To Configure check the check box and select value success or failure.

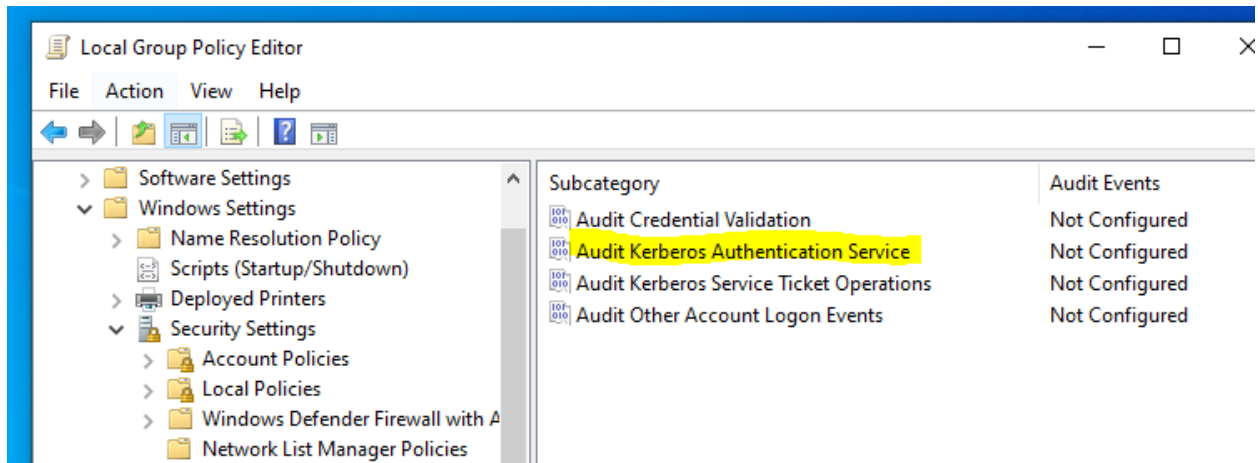


## 2.2 Audit Kerberos Authentication Service

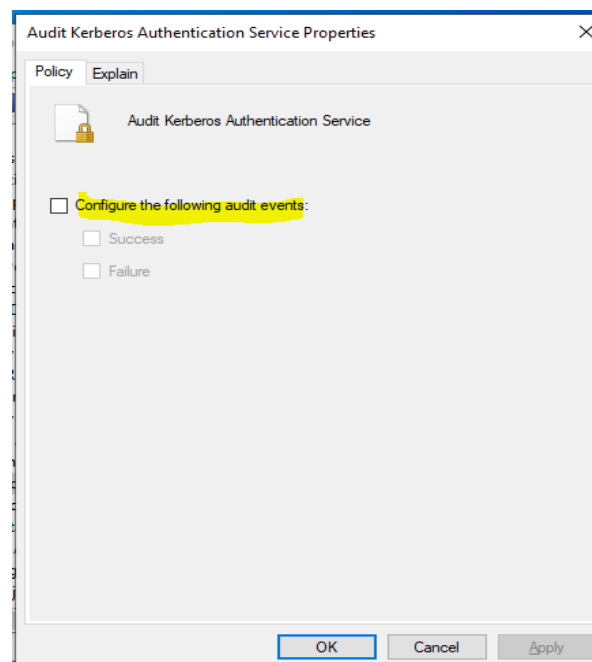
- This Policy Determines whether to generate auditing events for Kerberos authentication TGT Requests.
- Default Value: Not configured
- On Configuring Audit event will be generated after a TGT request.
- **Importance:** it is important to enable the service because it will help to know whether Kerberos authentication request failed or Kerberos pre-authentication was failed

To configure the Policy, Navigate to **System Audit Policies-> Account Logon-> Double Click the Account Logon-> Select Audit Kerberos Authentication Service-> Double Click It**





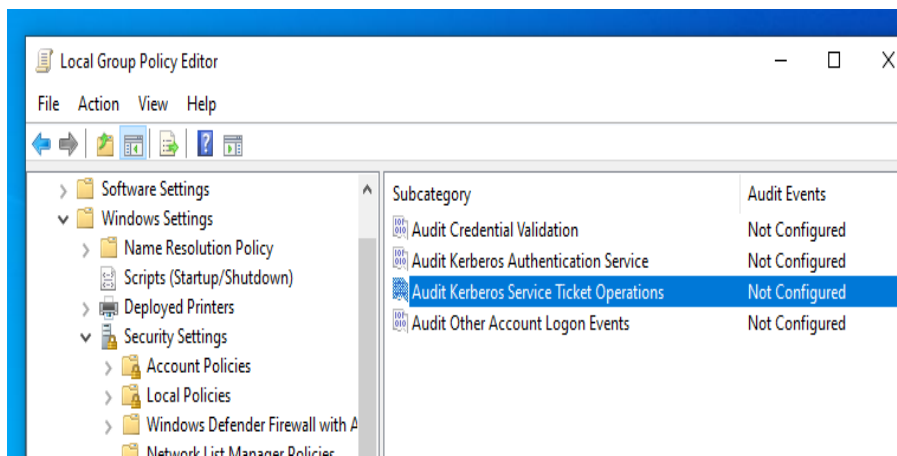
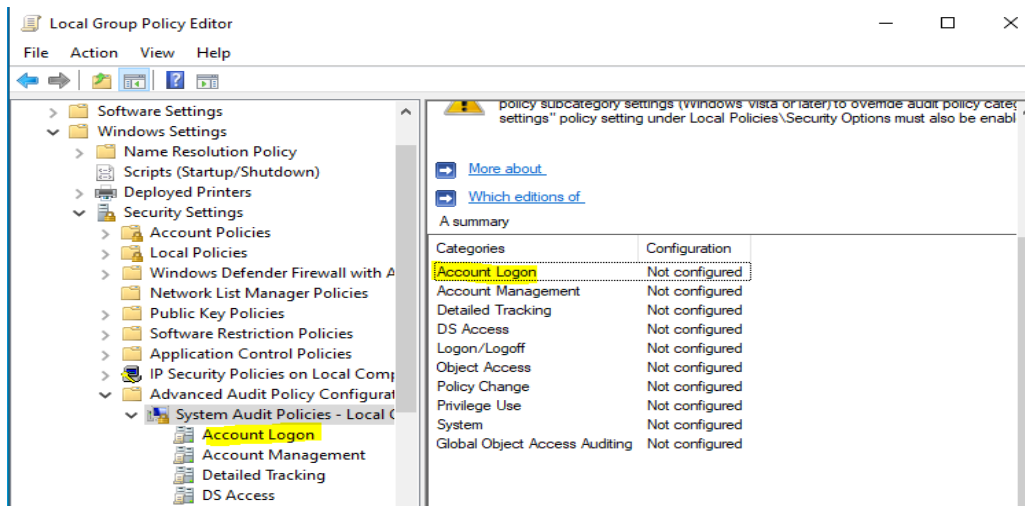
To Configure check the check box and select value success or failure as shown in the image below:



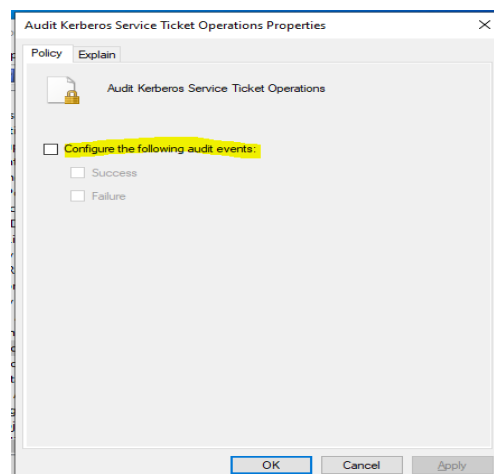
## 2.3 Audit Kerberos Service Ticket Operations

- This Policy Determines whether to generate security auditing events for Kerberos service ticket requests.
- Default Value: Not configured
- Audit events are generated when a user who wants access to network resource and the Kerberos is used to authenticate it.
- **Importance:** the service is important because it will help know whether a Kerberos ticket was requested or was renewed.

To configure the Policy, Navigate to **System Audit Policies-> Account Logon-> Double Click the Account Logon-> Select Audit Kerberos Service Ticket Operations-> Double Click It**



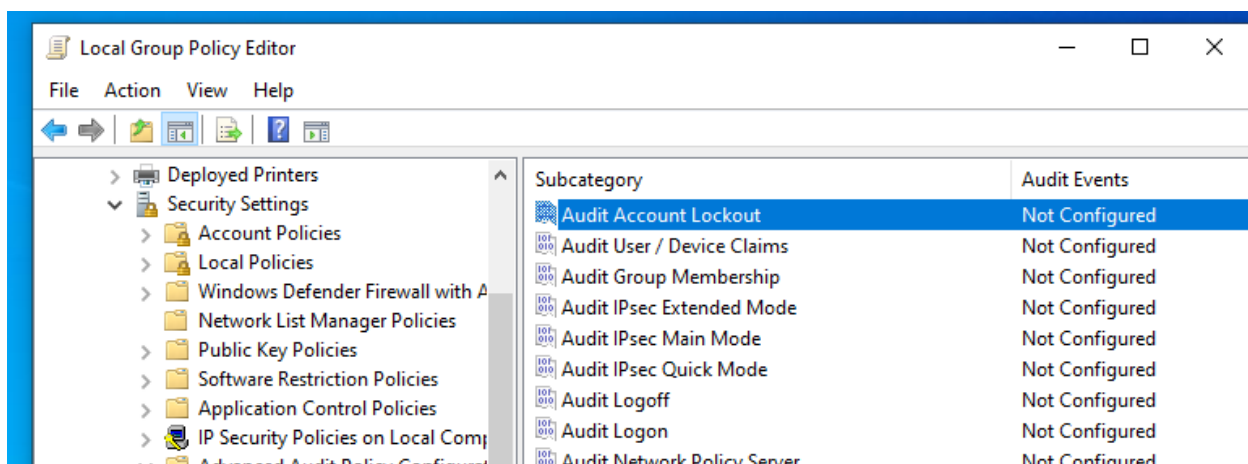
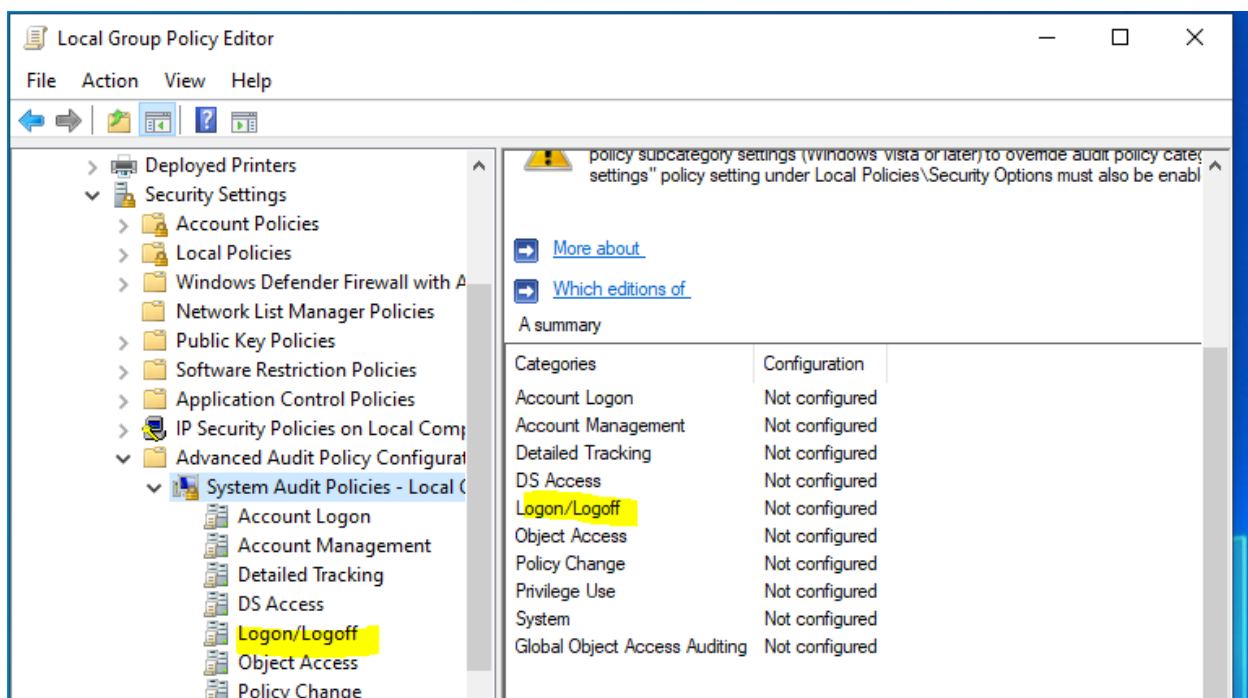
To Configure check the check box and select value success or failure as shown in the image below:



## 2.4 Audit Account Lockout

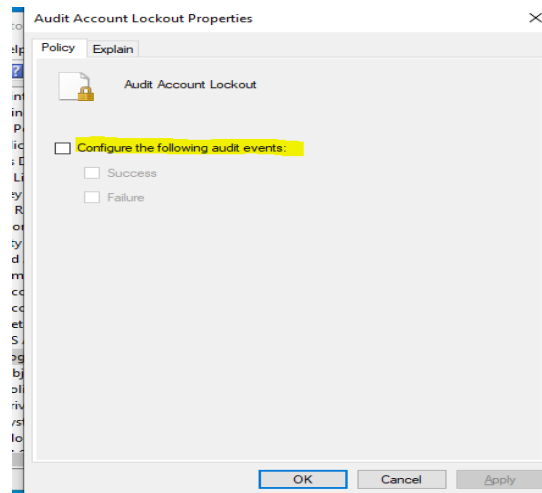
- Every time a user fails to log on to an account which is locked out an audit security events will be generated
- Default Value: Success
- The success audit events will record successful events and failure audits will record unsuccessful events.
- **Importance: It is important to audit when a user fails to logon to a locked account because it may determine that the system might be under DoS attack.**

To configure the Policy, Navigate to **System Audit Policies-> Logon/Logoff-> Double Click the Logon/Logoff-> Select Audit Account Lockout-> Double Click It**



To Configure check the check box and select value success or failure as shown in the image below:

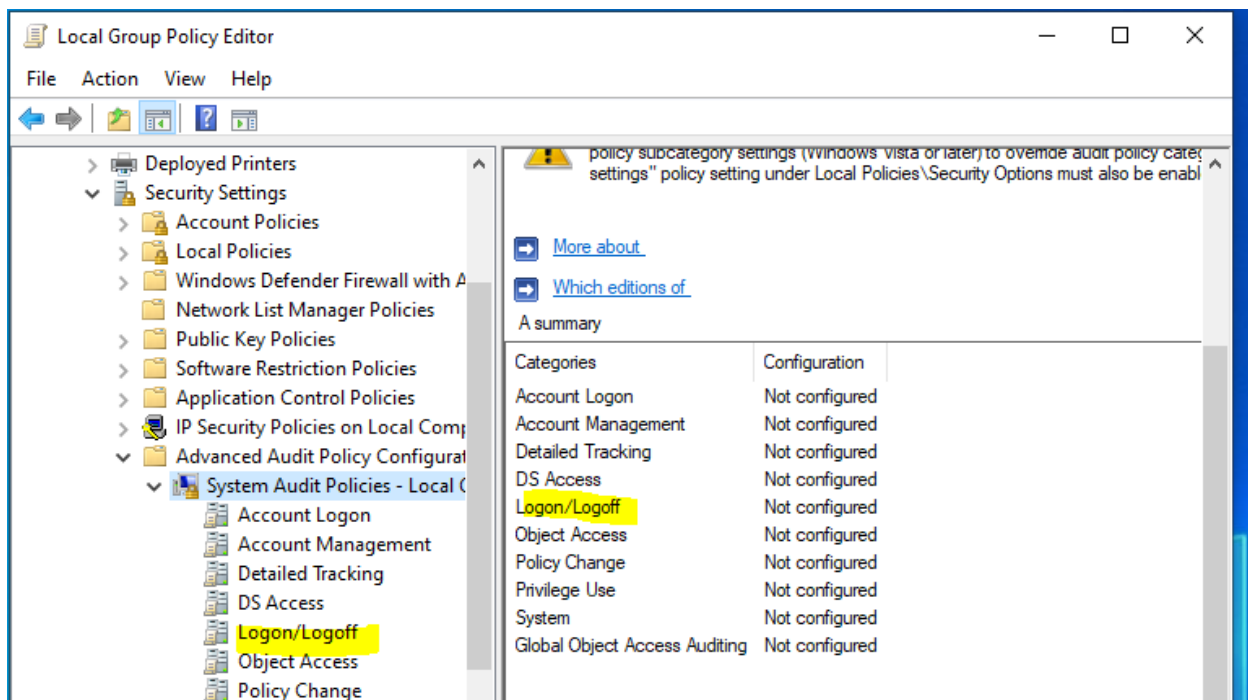


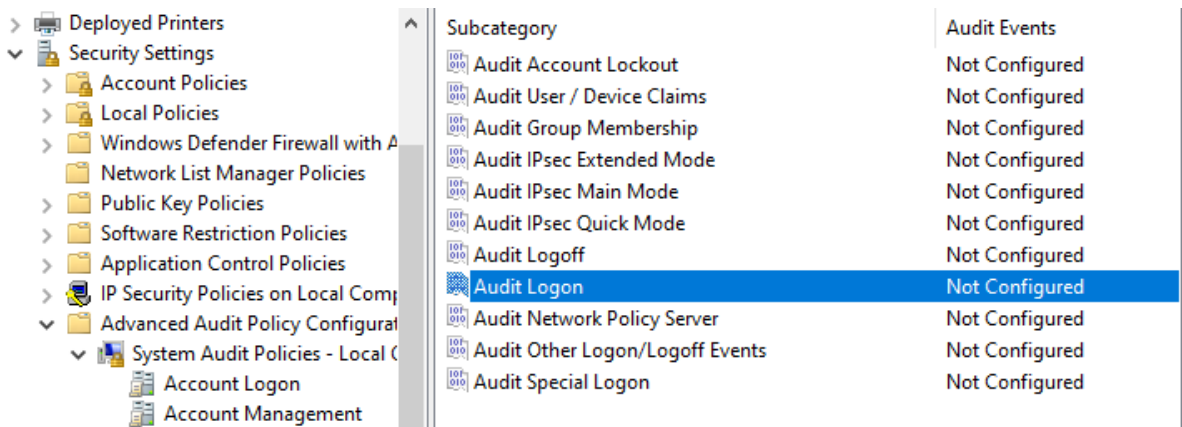


## 2.5 Audit Logon

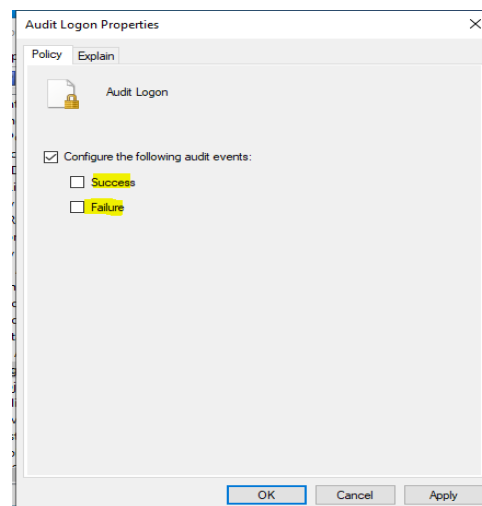
- Every time a user tries to Logon OS will generate audit security events.
- Default Value: Success
- **Importance:** Logon events are very important to understand a user activity and help detect which will further prevent attacks.

To configure the Policy, Navigate to **System Audit Policies-> Logon/Logoff-> Double Click the Logon/Logoff-> Select Audit Logon-> Double Click It**



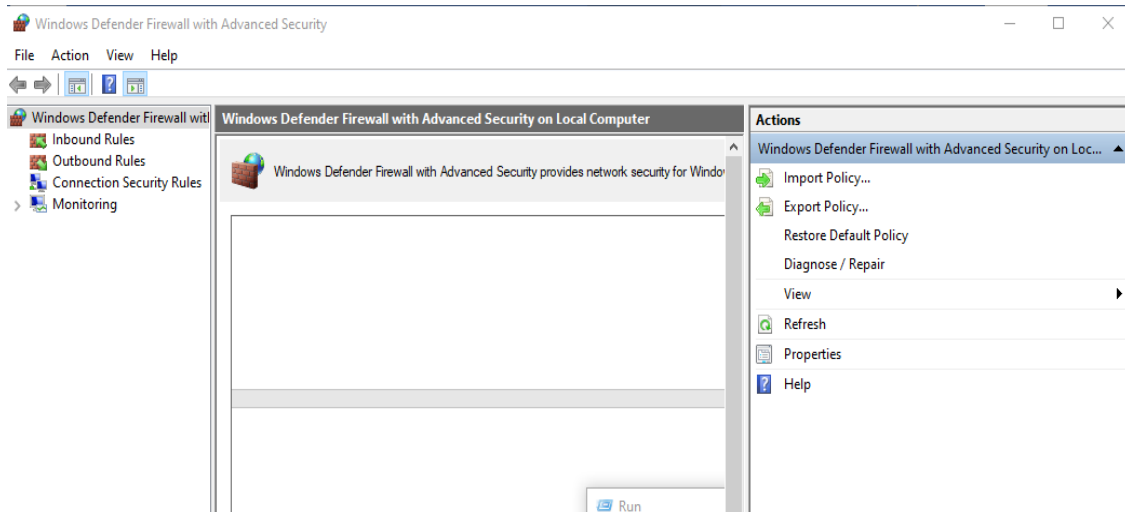


To Configure check the check box and select value success or failure as shown in the image below:

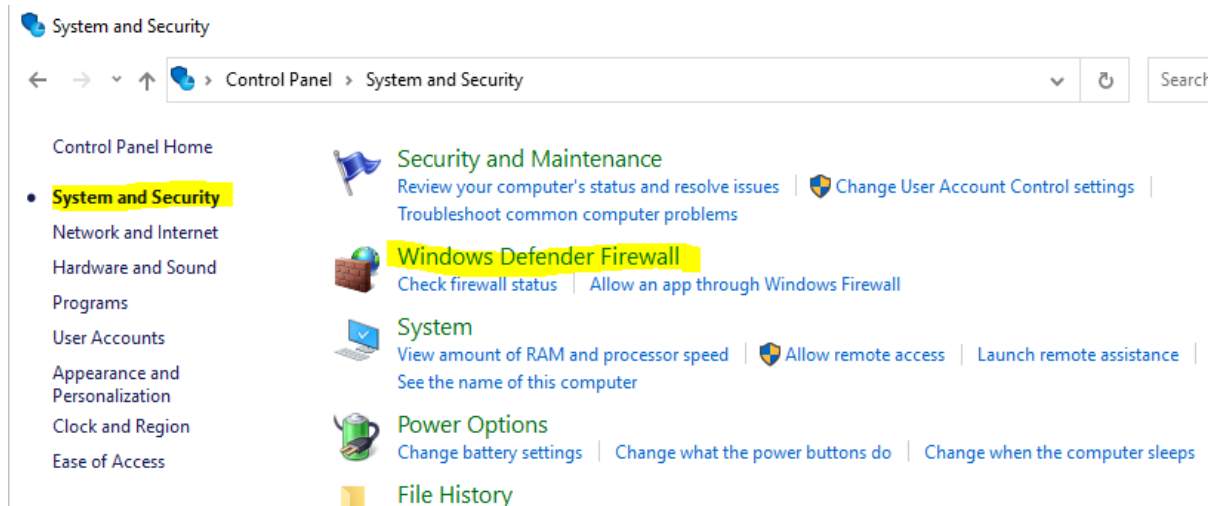


### 3 Windows Defender Firewall

- Windows defender help reduce the risk of network security threats and keep sensitive data safe. It also filters the data traffic inbound to the system.
- Windows Firewall has three different profiles naming Public, Private and Domain.
- We can open Windows Defender from:
  - Windows Run by typing wf.msc and clicking ok.



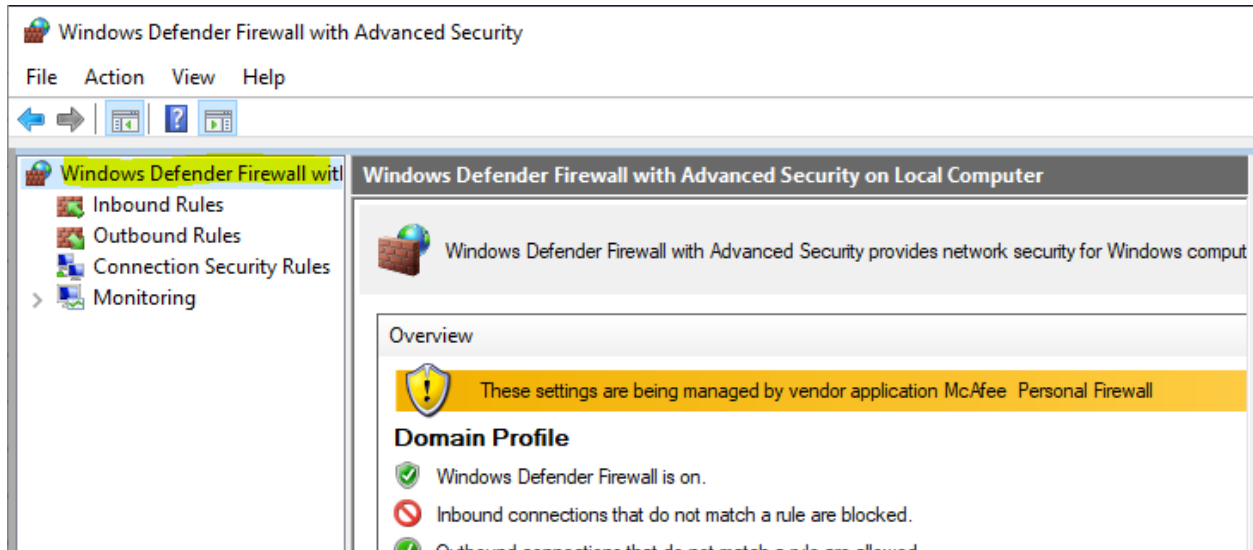
- From Control panel->System and Security->Select Windows defender firewall



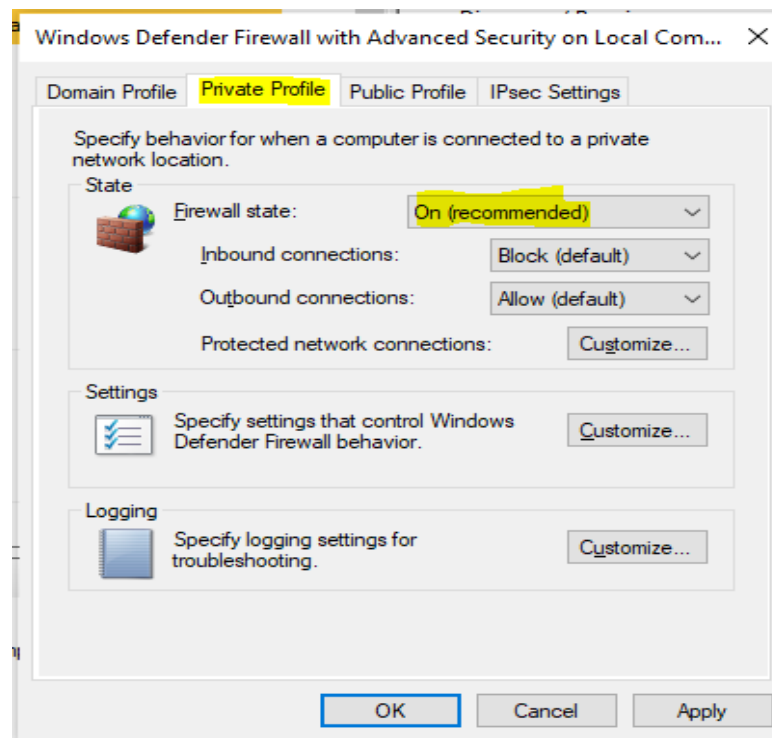
### 3.1 Firewall State

- This setting states whether the firewall is on or off.
- Firewall can protect your network by filtering the data traffic and help against worms, viruses and malware.
- **Importance:** If the windows defender firewall is off your computer is vulnerable to worms, viruses and malwares.

To turn firewall on or off. Navigate-> **Windows Defender Firewall with advanced security** tab-> Right click on Windows Defender Firewall drop down and click properties.



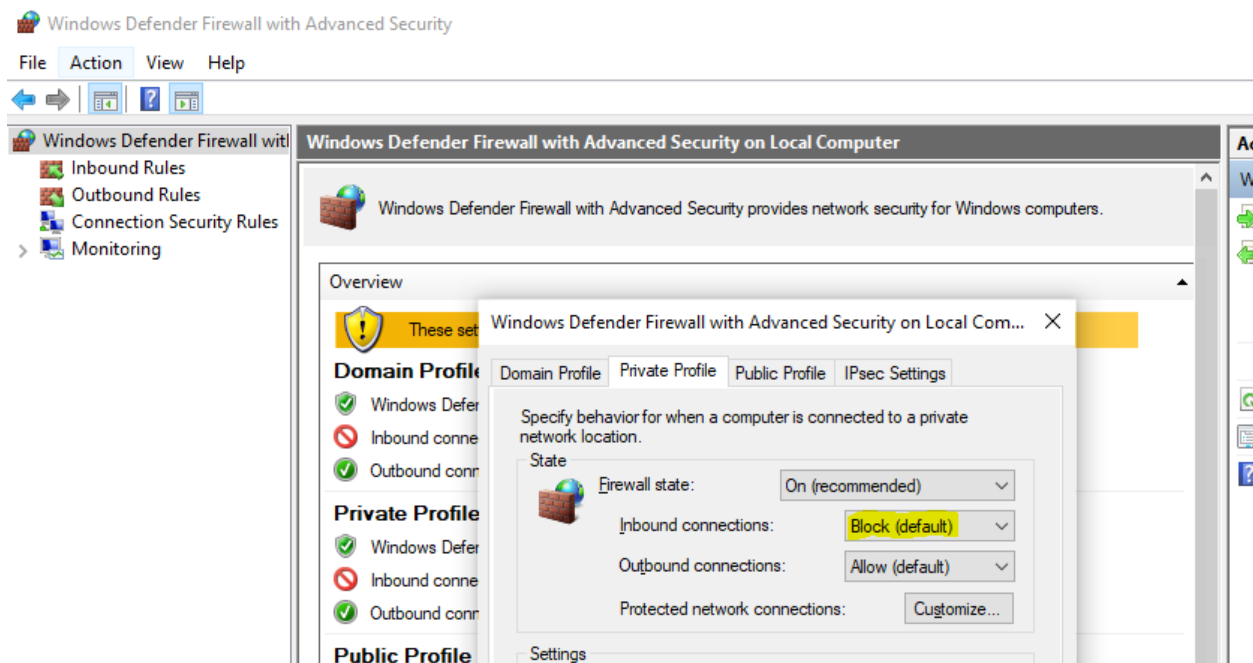
Firewall is managed in my system by vendor application McAfee but still we can configure firewall state for domain, private, and public profile by turning it on and off as shown in the image below:



### 3.2 Inbound Connections

- Inbound connections mean someone from outside can initiate a connection to your computer which will make traffic flow inward to your machine.
- Default value for this should always be block.
- **Importance:** this service blocks all inbound connections from outside which help prevent your machine from outer threats.

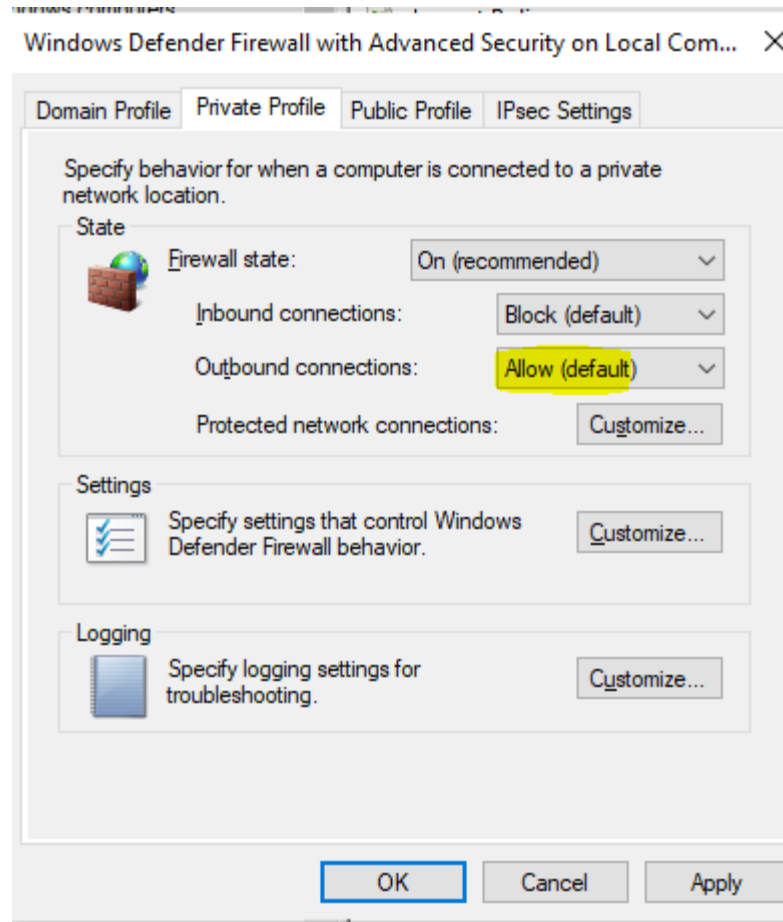
To allow or block inbound connections. Navigate-> **Windows Defender Firewall with advanced security** tab-> Right click on Windows Defender Firewall drop down and click properties. Now select allow, Block and Block all connections from the dropdown list as shown in the image below.



### 3.3 Outbound Connections

- Outbound connections mean you can connect to the internet and the data traffic start flowing from your computer to the destination you want.
- Default value for the service is allow.
- **Importance:** If this service is set to block you want be able to connect to internet so you must always allow outbound traffic. Blocking outbound traffic can stop an attacker from compromising your system.

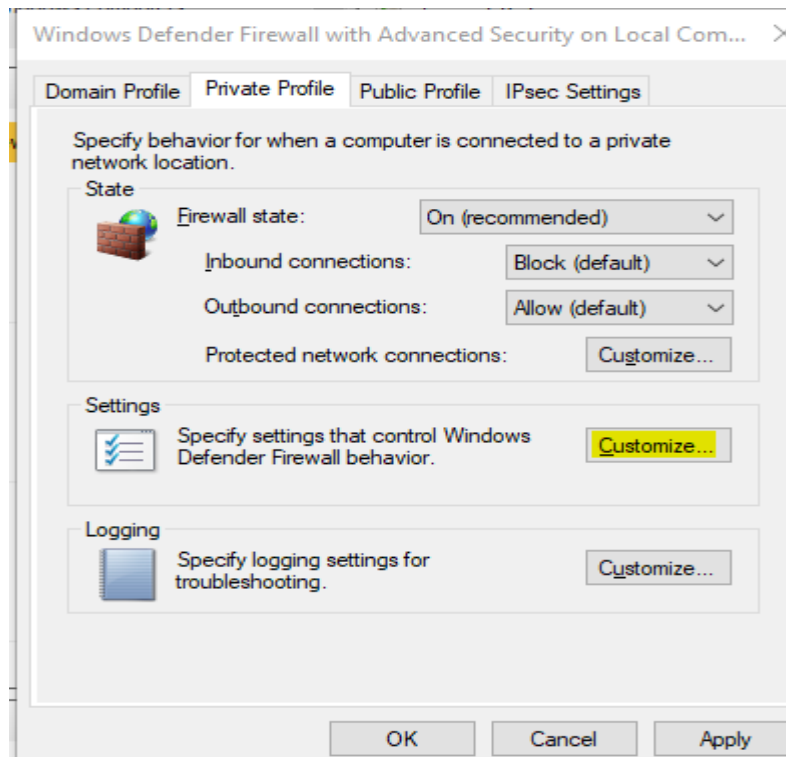
To allow or block outbound connections. Navigate-> **Windows Defender Firewall with advanced security** tab-> Right click on Windows Defender Firewall drop down and click properties. Now select allow and Block from the dropdown list as shown in the image below.



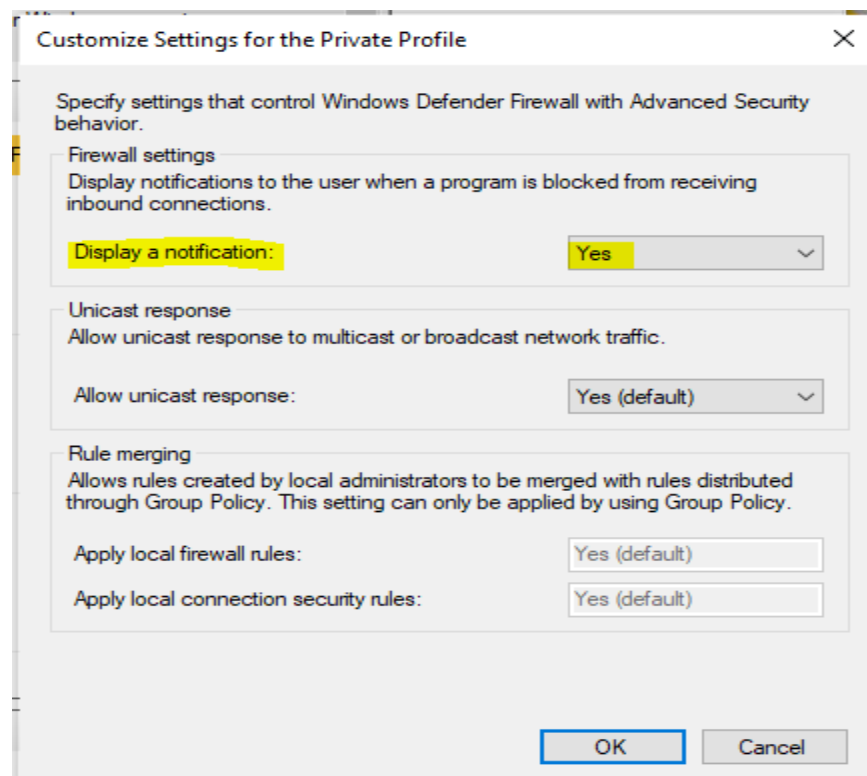
### 3.4 Display a Notification

- This service will display a notification to the user when a program in the system is blocked from receiving inbound connections.
- Default value of the service is set to yes.
- **Importance:** A user must know why the application is not connecting to the network with a prompt that the application is blocked from inbound connections.

To set yes or no value for display a notification service. Navigate-> **Windows Defender Firewall with advanced security** tab-> Right click on Windows Defender Firewall drop down and click properties. Now click customize under settings->



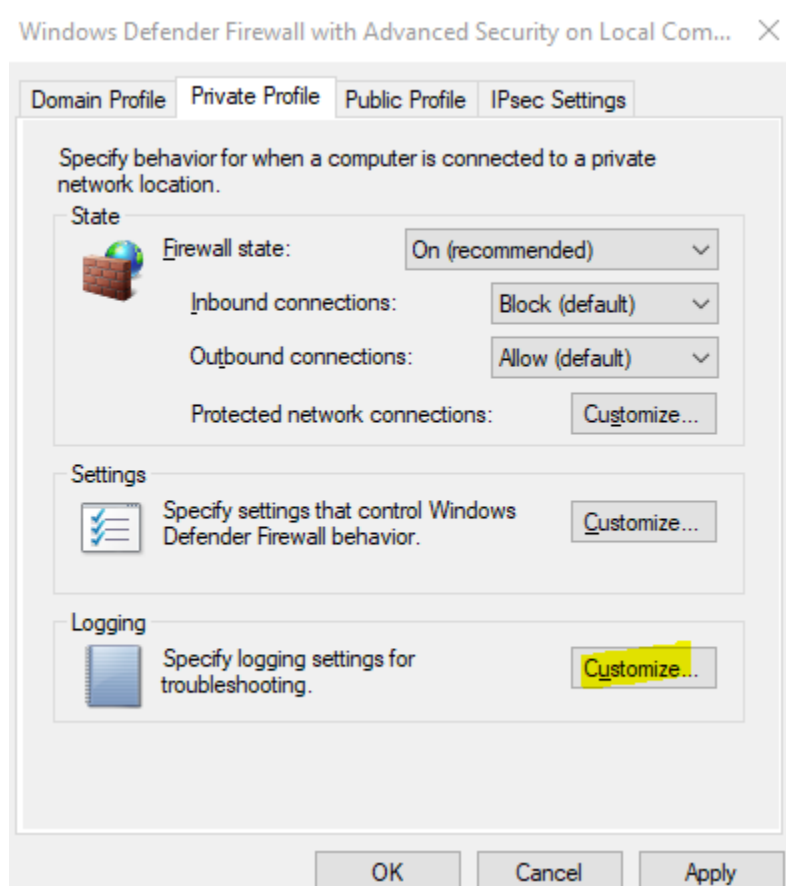
In the customize setting for the private profile tab, select yes or no from the dropdown list as shown in the image below.



### 3.5 Logging- Name, Size, Log dropped Packages and log successful connections

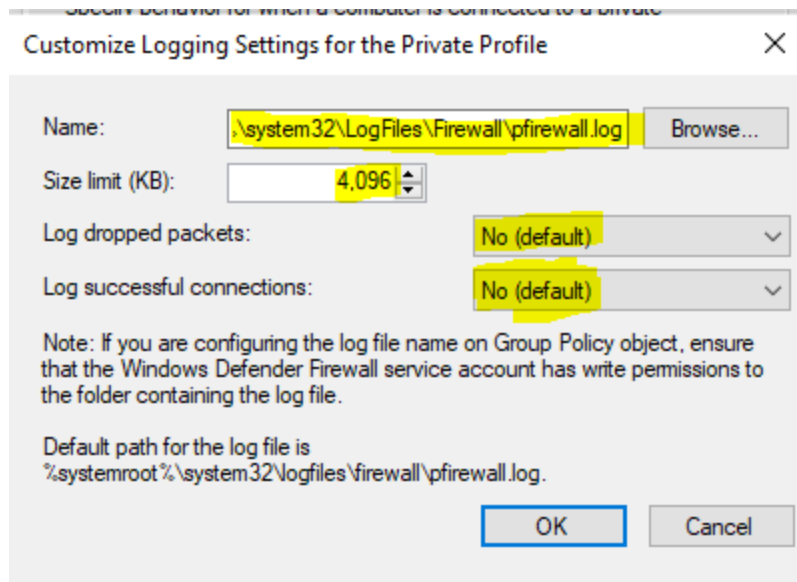
- **Importance:** By customizing these settings one can log and analyze the dropped network packages and successful connections which can be later used to ensure whether the network is secured
- We can select the path for the log file and its size limit and select whether to log dropped packets and successful connections by setting their value to yes.

To set yes or no value for display a notification service. Navigate-> **Windows Defender Firewall with advanced security** tab-> Right click on Windows Defender Firewall drop down and click properties. Now click customize under logging->



In the customize logging setting for the private profile tab, select yes or no from the dropdown list as shown in the image below.



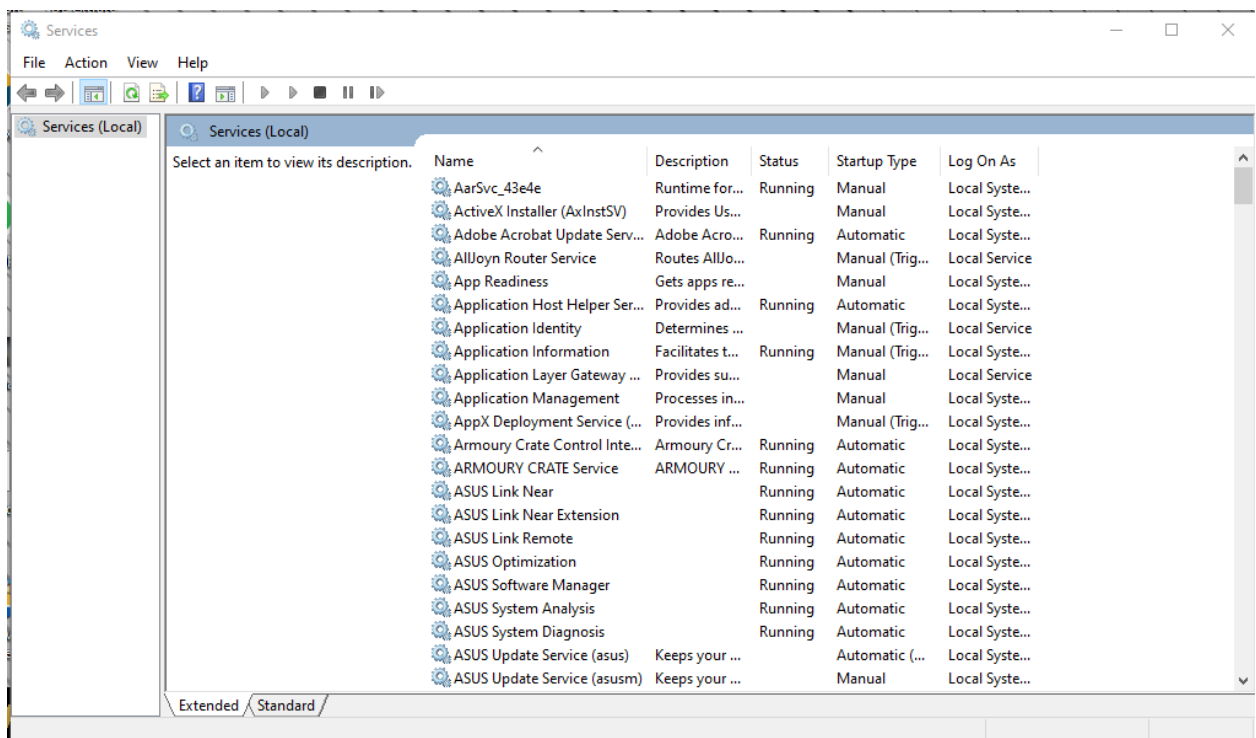
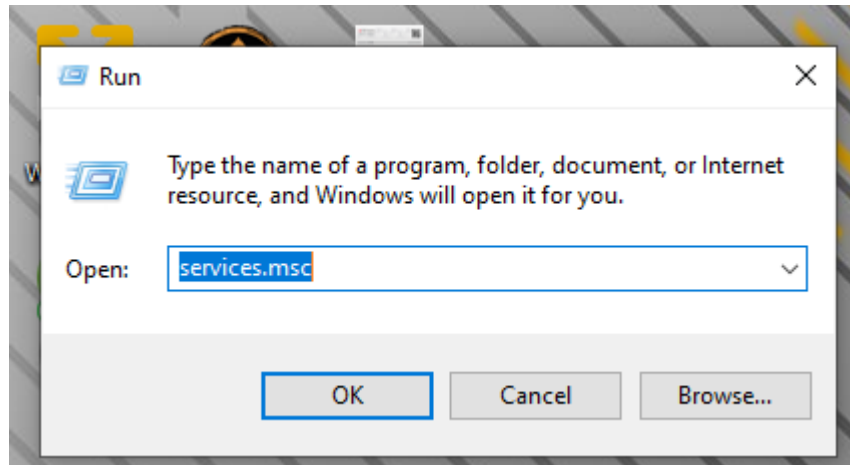


## 4 Services

There are 4 Service policies listed under services tab can be seen in the image below:

|    | A              | B                                 | C          |  |
|----|----------------|-----------------------------------|------------|--|
| 1  | Type           | Name                              | Windows 10 |  |
| 2  | Scheduled Task | XblGameSaveTask                   | Disabled   |  |
| 3  | Services       | Xbox Accessory Management Service | Disabled   |  |
| 4  | Services       | Xbox Live Auth Manager            | Disabled   |  |
| 5  | Services       | Xbox Live Game Save               | Disabled   |  |
| 6  | Services       | Xbox Live Networking Service      | Disabled   |  |
| 7  |                |                                   |            |  |
| 8  |                |                                   |            |  |
| 9  |                |                                   |            |  |
| 10 |                |                                   |            |  |

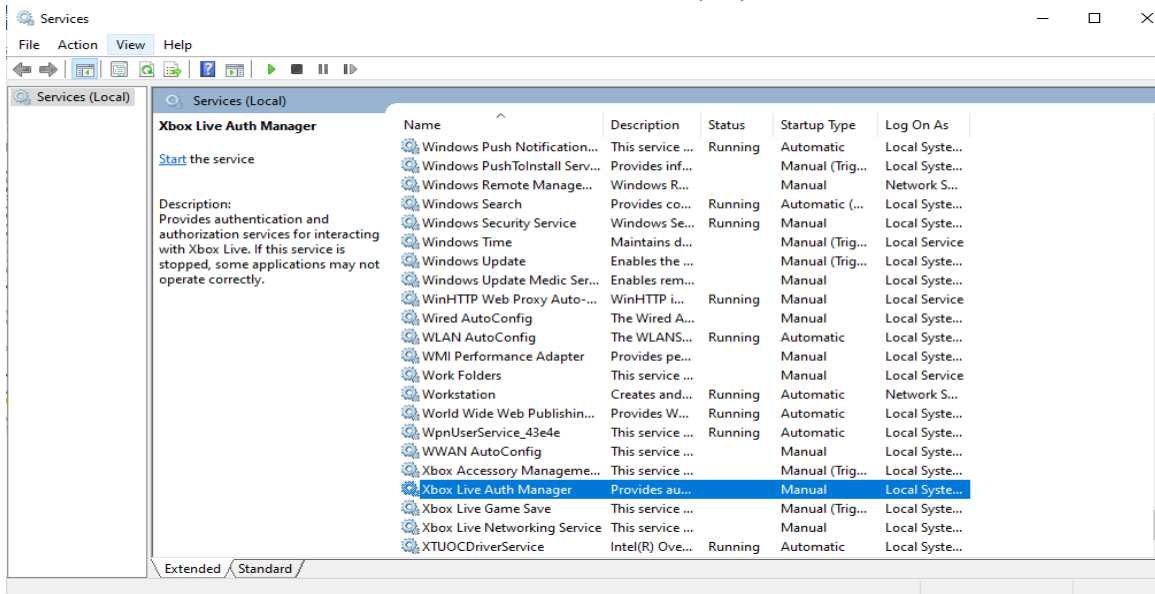
To Configure these policies, navigate to **Start** menu-> type **run**->In the run console type **services.msc** and **click ok**.



## 4.1 XBOX Live Auth Manager

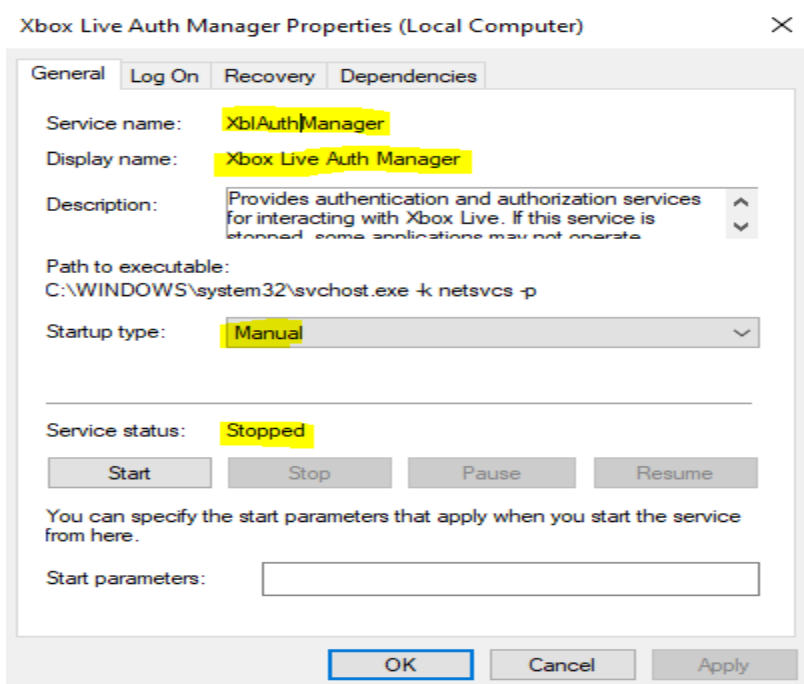
This service provides authorization and authentication services for the purpose of Xbox live interaction.

Below is the screenshot of the properties tab of the service.



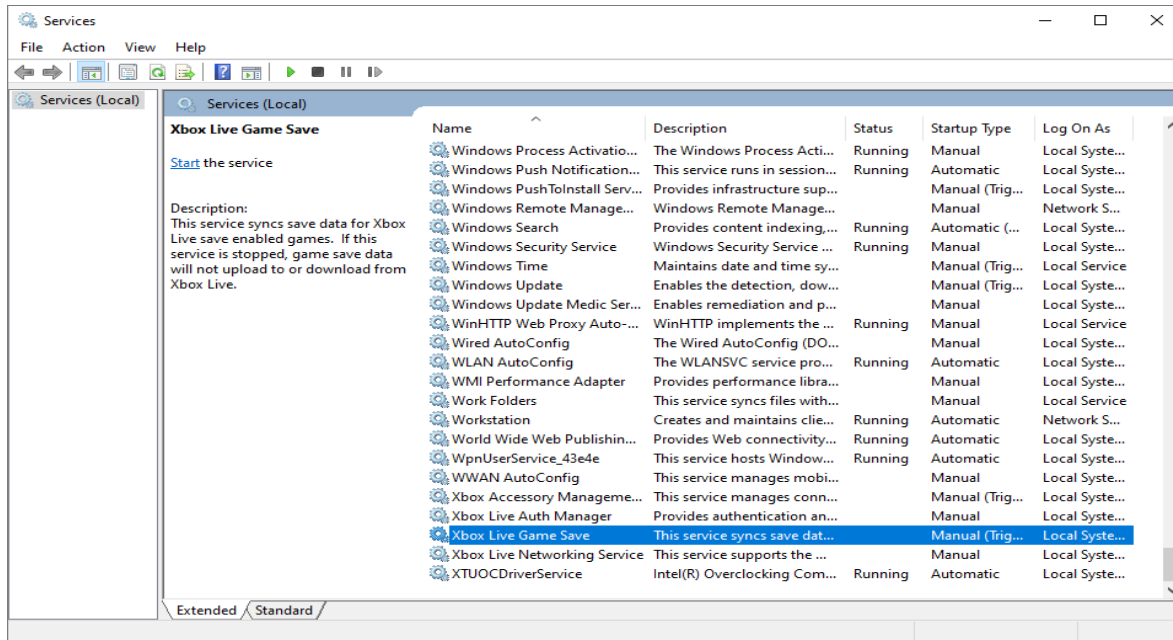
The startup type of the service is manual which means it can only be started by a user, application or another service. If this service is stopped, some applications may not operate correctly.

We can change the startup type by clicking the dropdown list and selecting other startup type values.

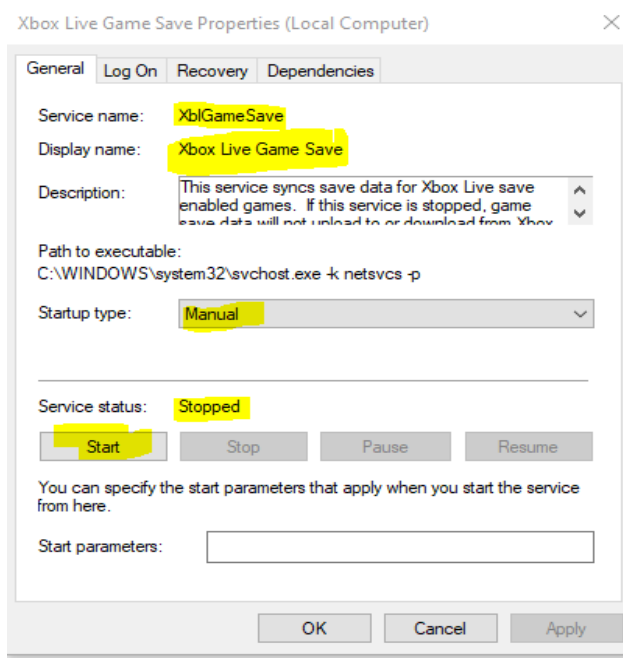


## 4.2 Xbox Live Game Save

Xbox live Game Save service syncs save data for games which are Xbox Live save enabled. Any halt to this service will hinder the downloading and uploading of data from Xbox Live.

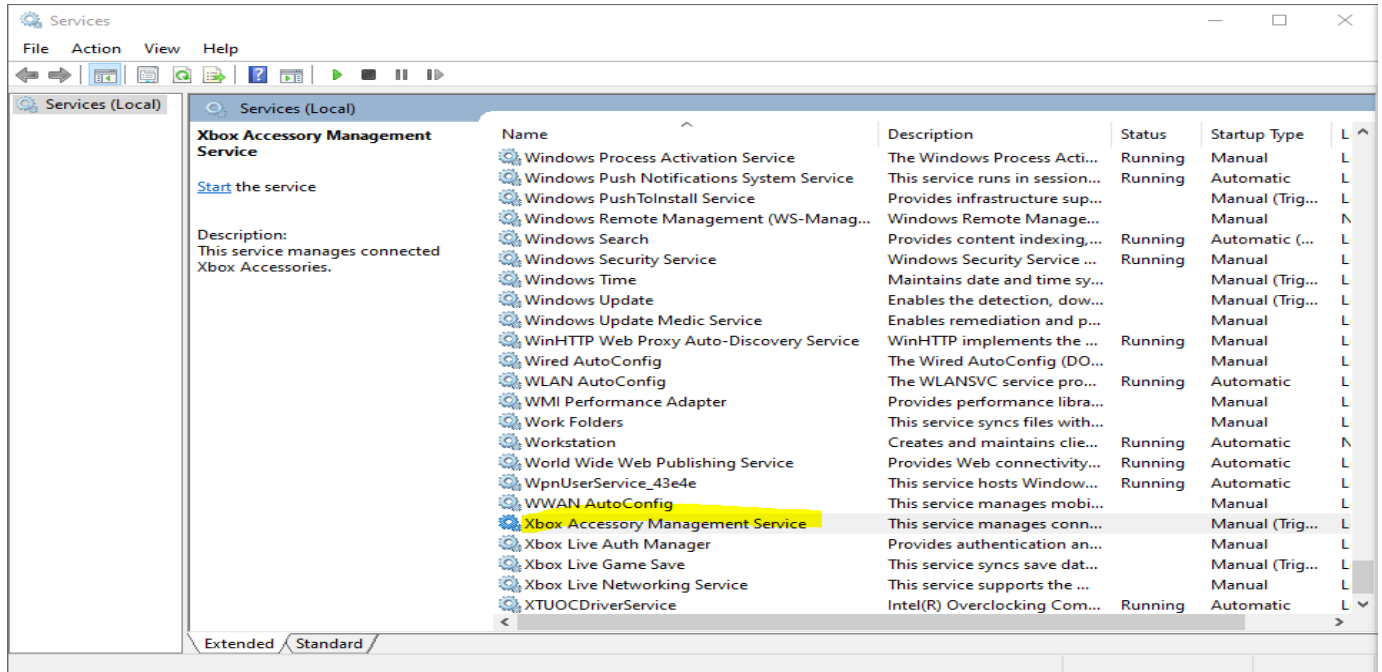


To open the properties tab to change any configuration of the service just double click the service.

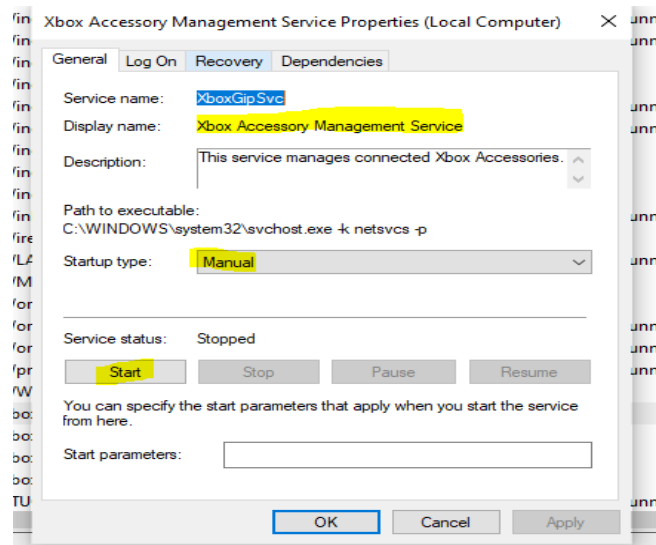


### 4.3 Xbox Accessory Management Service

This service is a Win32 Service. It can only be started when the user, application or another service starts it. The Service manages all the connected Accessories of Xbox.

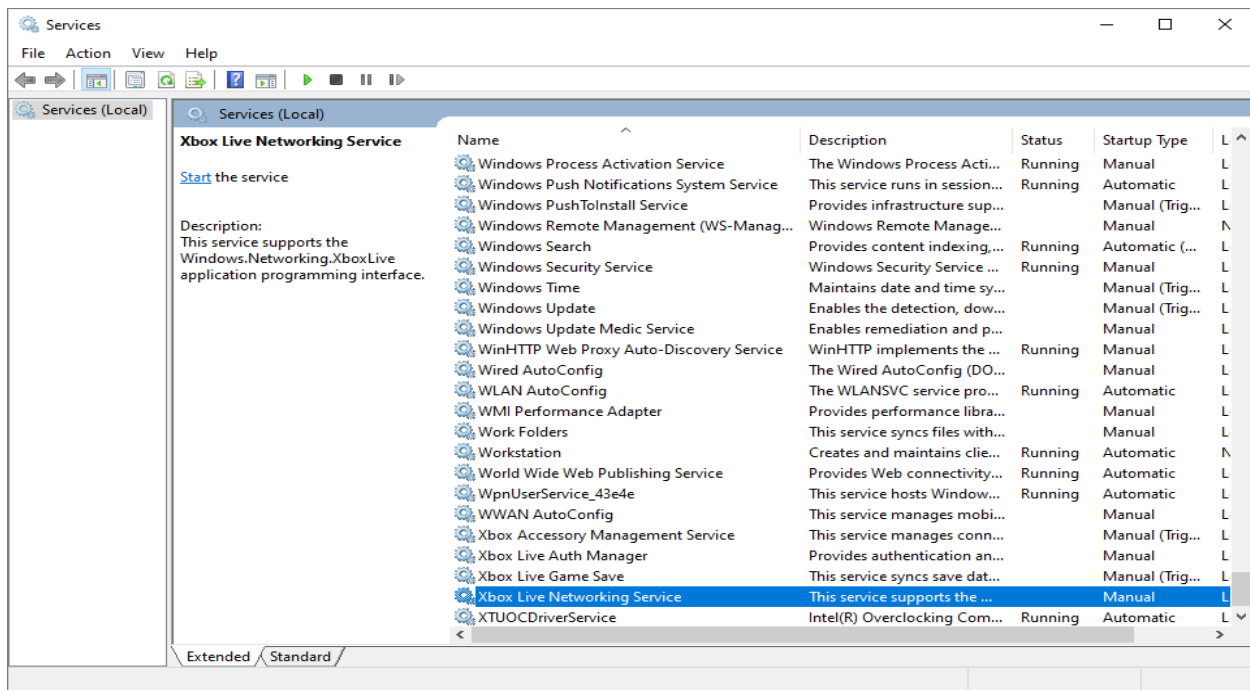


We can configure the service to Automatic, Disabled or Manual by double clicking the policy and selecting the required drop-down option of the Startup type as shown in the picture below:

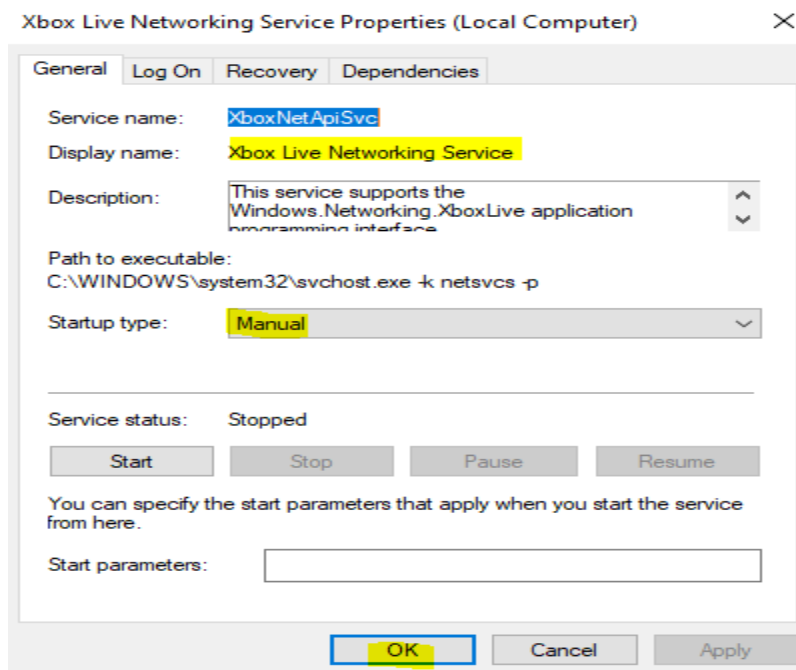


## 4.4 XBOX Live Networking Service

Xbox Live networking service is an online multiplayer gaming service which connects with the network, without this service Xbox live won't work.



We can configure the service to Automatic, Disabled or Manual by double clicking the policy and selecting the required drop-down option of the Startup type as shown in the picture below:

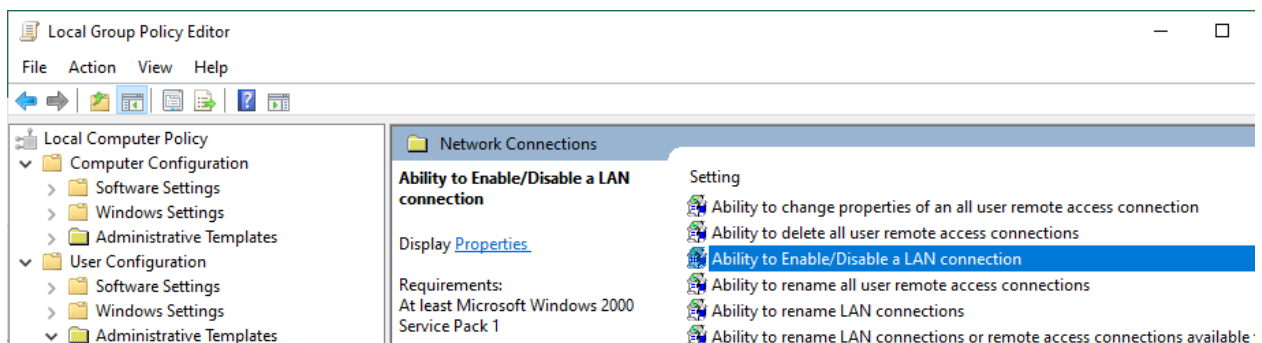
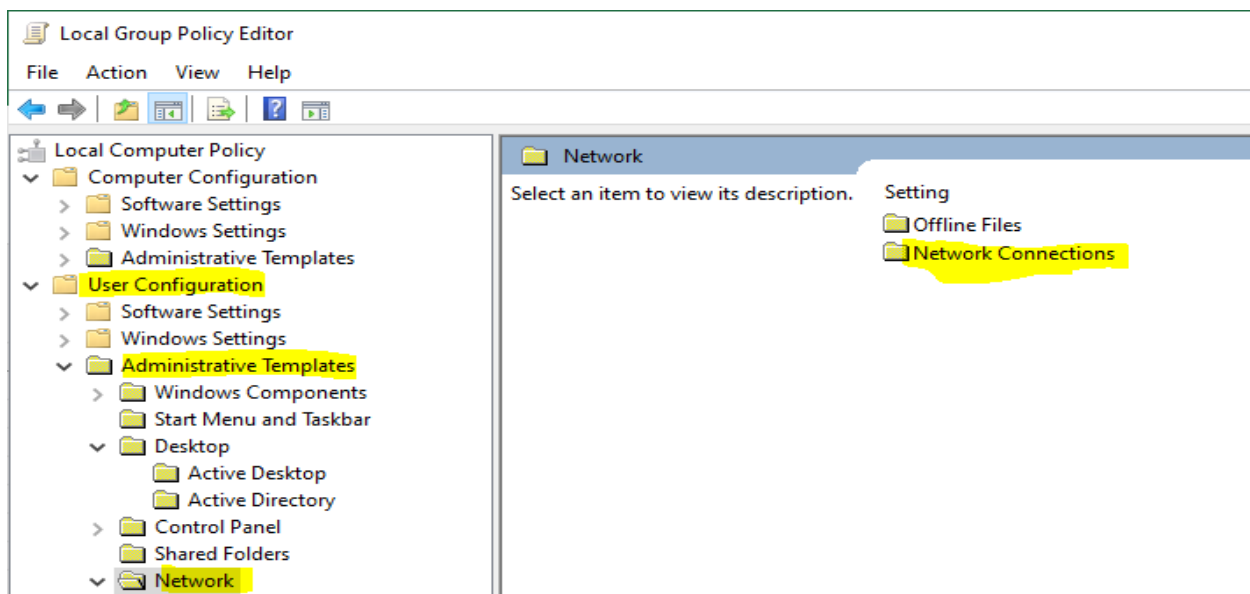


## 5 Computer

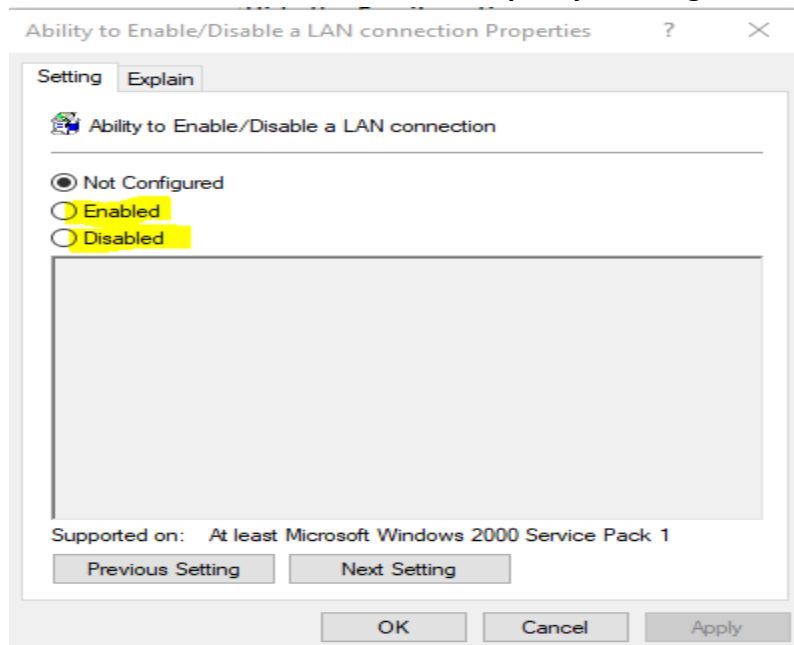
### 5.1 Ability to Enable/Disable LAN connections

- This policy determines whether a user can enable/disable LAN connections.
- **Importance:** Enabling the Setting will enable the Lan Connections for the user
- **Importance:** Disabling will Disable the LAN connections
- **Default value is not configured.**

To configure the policy->Open Local Group Policy editor->Expand User Configuration-> Expand Administrative Templates->Expand Network->Select Network Connections.



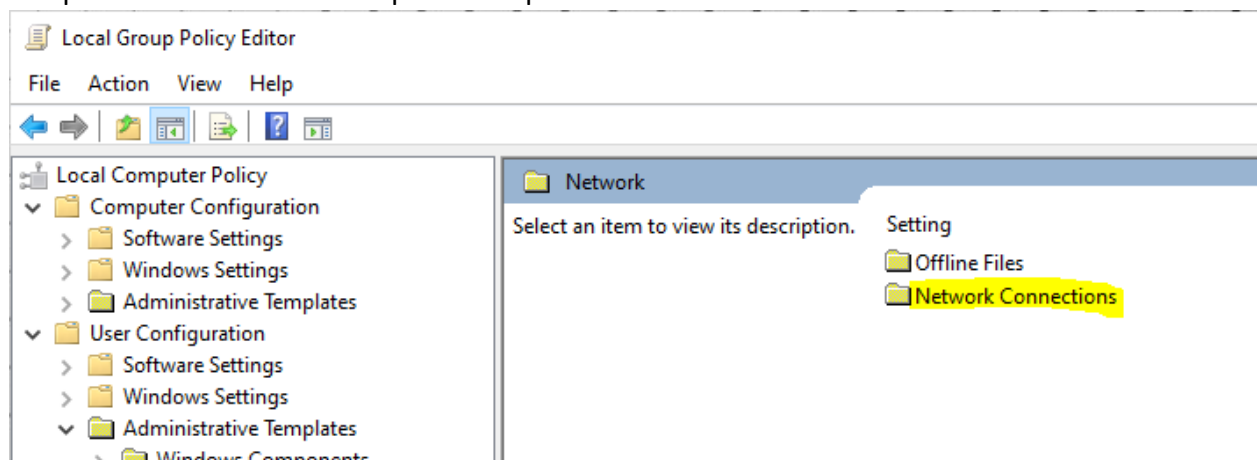
We can enable or disable the policy setting as shown in the image below:



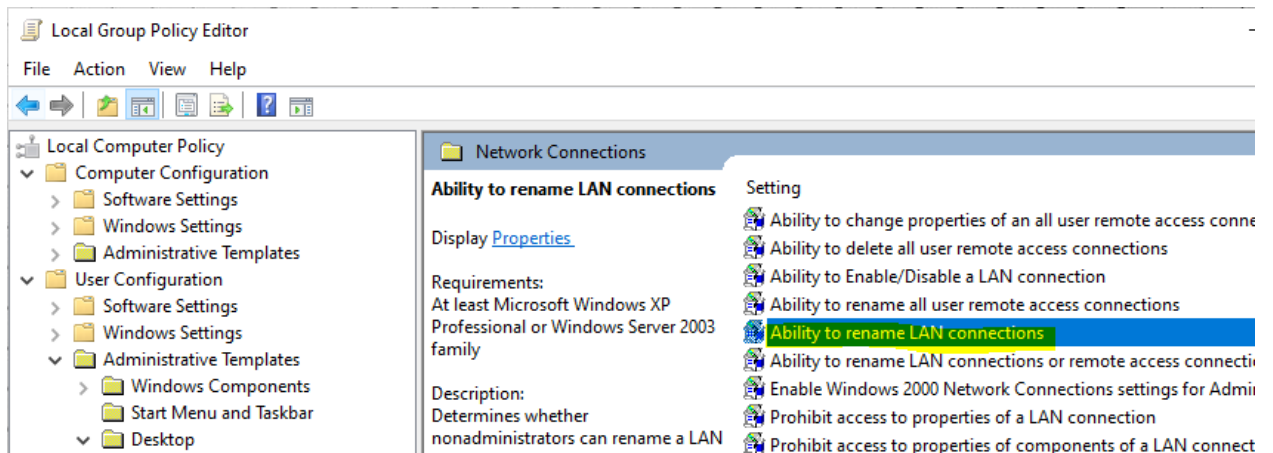
## 5.2 Ability to Rename LAN connections

- This policy determines whether a non-administrative user can rename a LAN connection.
- **Importance:** Enable this setting to allow non administrators to rename a LAN connection or disable for vice versa.
- **Default value is not configured.**

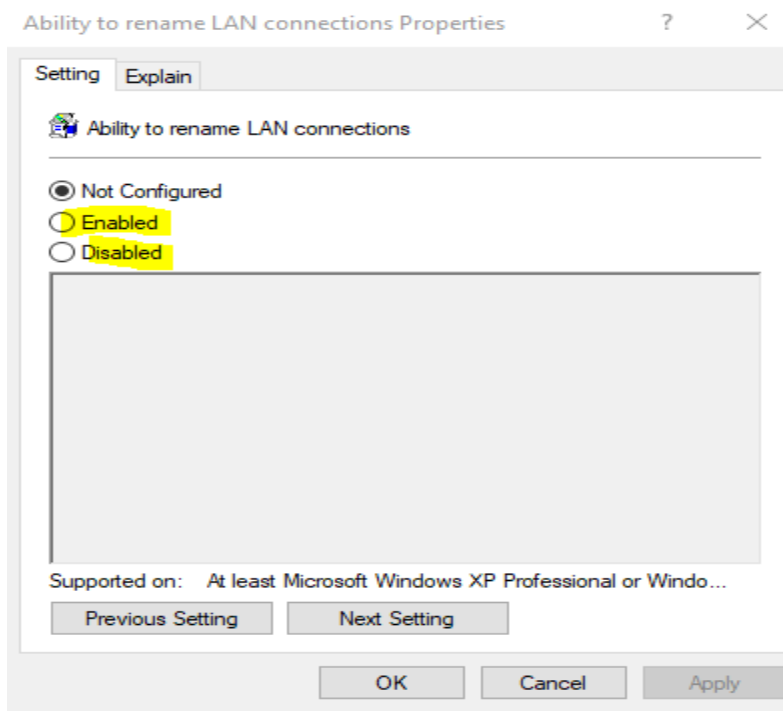
To configure the policy->Open Local Group Policy editor->Expand User Configuration->Expand Administrative Templates->Expand Network->Select Network Connections.







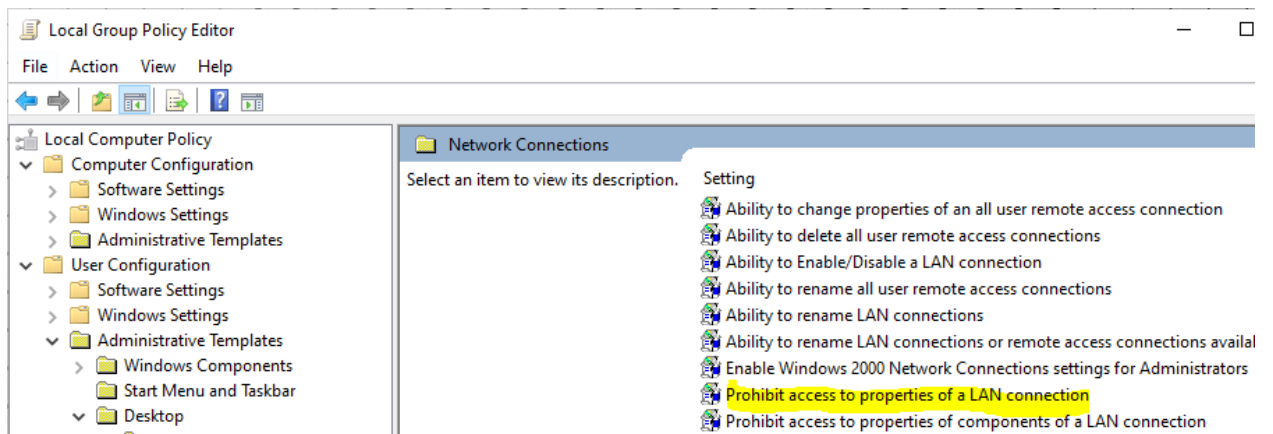
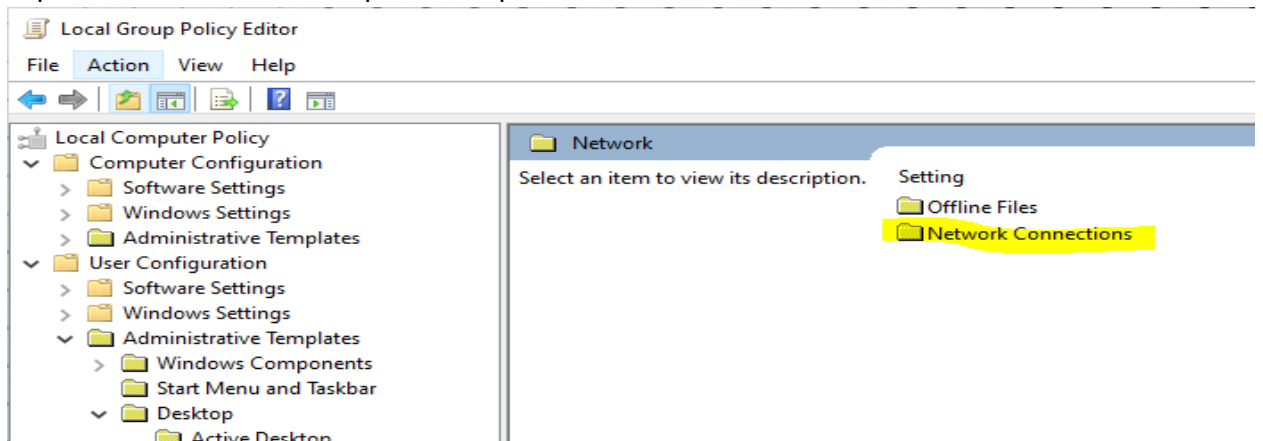
We can enable or disable the policy setting as shown in the image below:



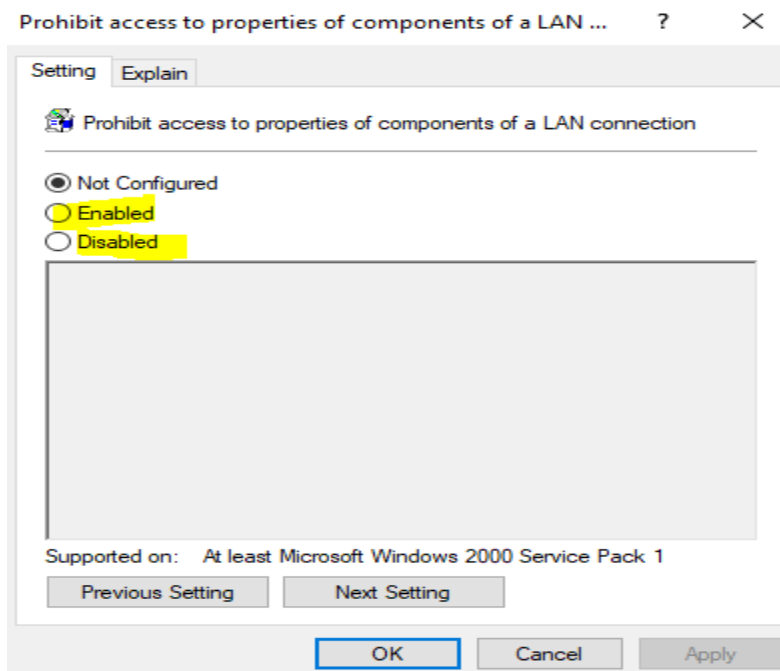
### 5.3 Prohibit Access to properties of a LAN connection

- This policy determines whether the properties menu tab is enabled and whether the LAN properties dialog box is available to users.
- **Importance:** Enable this setting will make Properties menu items disabled for all the users and users cannot open LAN properties dialog box or vice versa
- **Default value is not configured.**

To configure the policy->Open Local Group Policy editor->Expand User Configuration->Expand Administrative Templates->Expand Network->Select Network Connections.



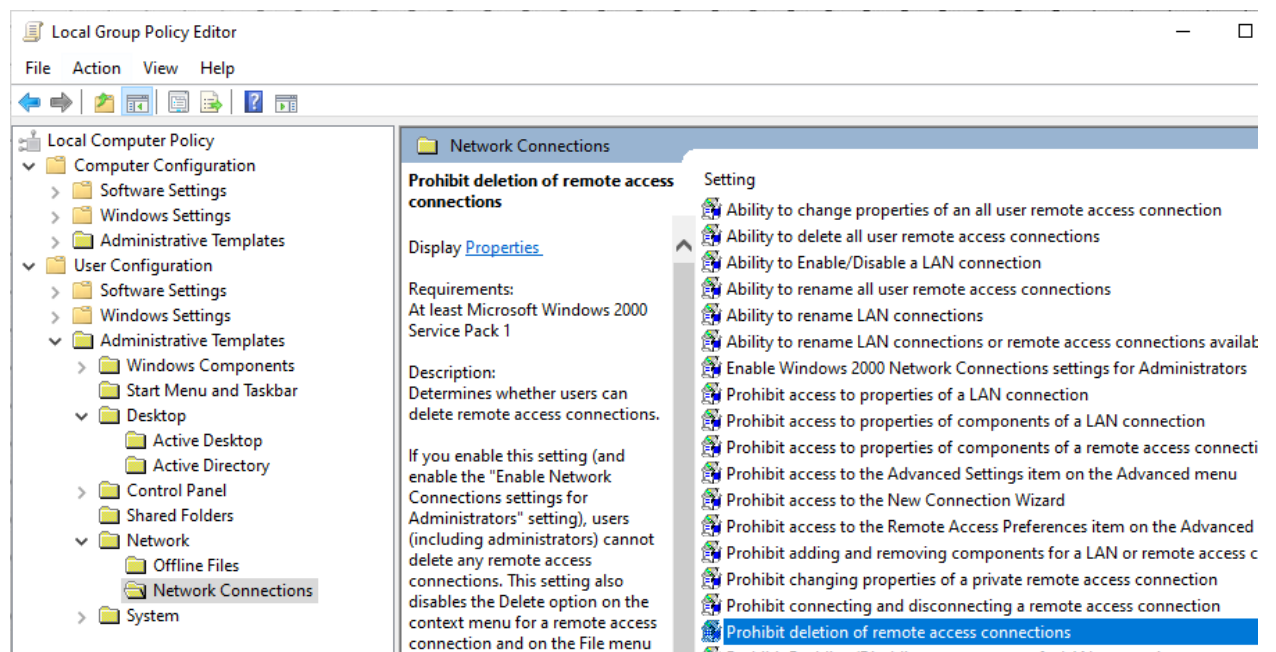
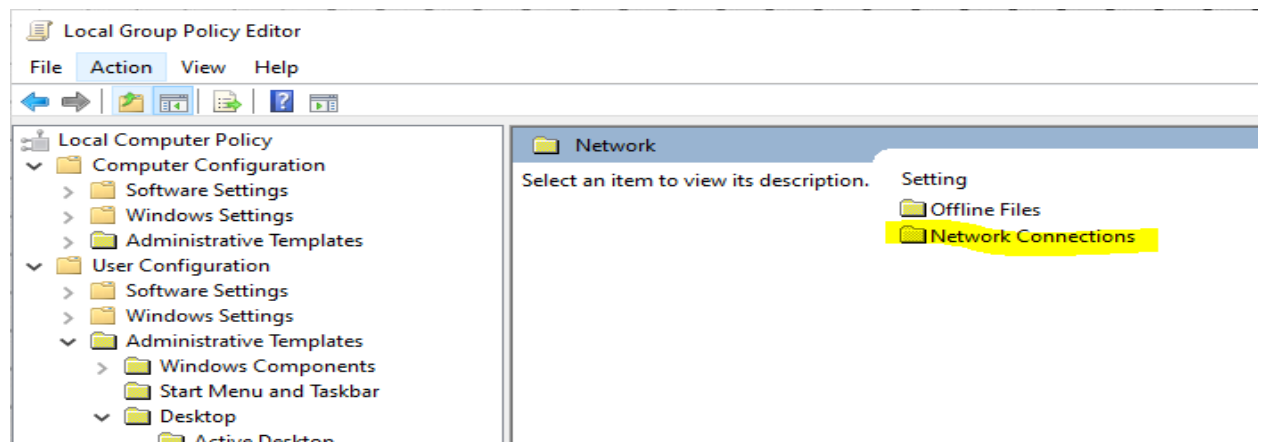
We can enable or disable the policy setting as shown in the image below:



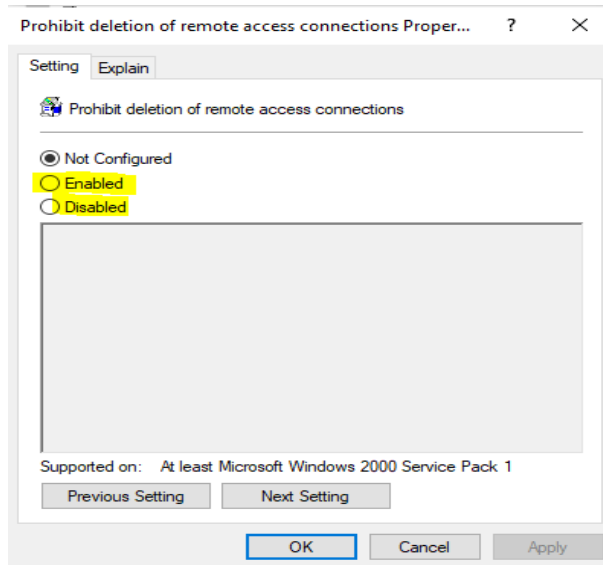
## 5.4 Prohibit deletions of remote access connections

- This policy determines whether users can delete Remote Access connections.
- **Importance:** Enable this setting will make restrict users from deleting any remote access connections or vice versa.
- **Default value is not configured.**

To configure the policy->Open Local Group Policy editor->Expand User Configuration-> Expand Administrative Templates->Expand Network->Select Network Connections.



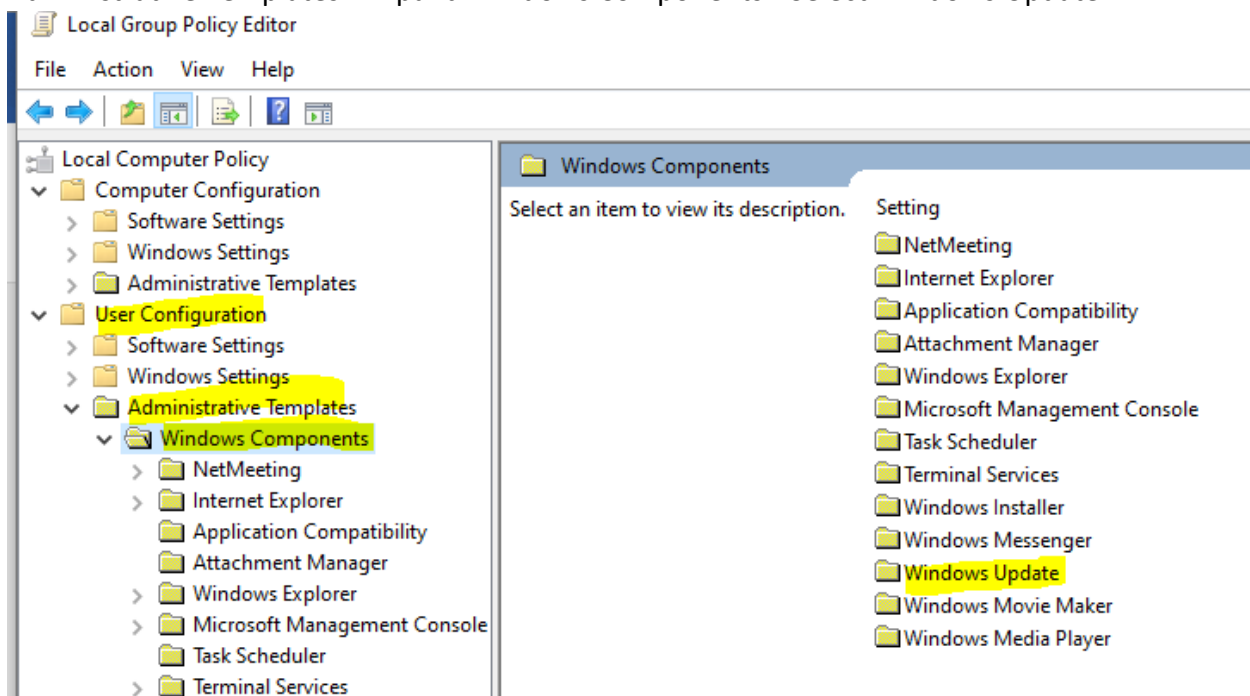
We can enable or disable the policy setting as shown in the image below:

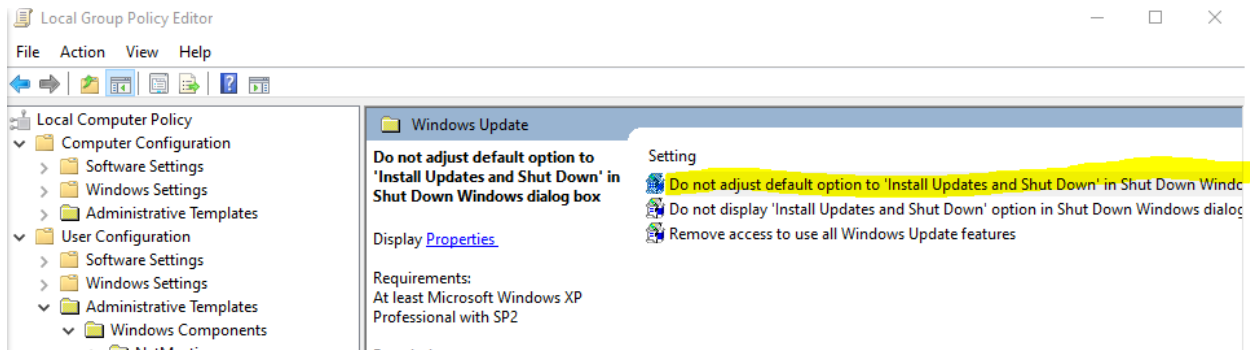


### 5.5 Do not adjust default option to “Install Updates and Shut Down” in Shut Down windows dialog box.

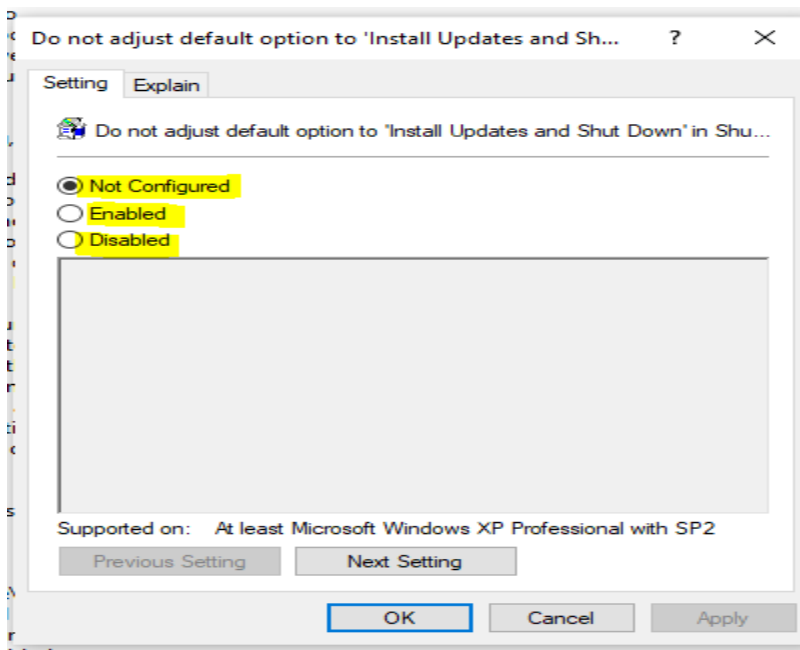
- This policy allows you to select whether the “Install Updates and Shut Down” option is default option in shut down dialog box.
- Enabling this policy will set user’s last shut down choice as the default option in shut down windows box.

To configure the policy->Open Local Group Policy editor->Expand User Configuration-> Expand Administrative Templates->Expand Windows Components->Select Windows Update.





To configure Select the options Enable and disabled as shown in the image below:

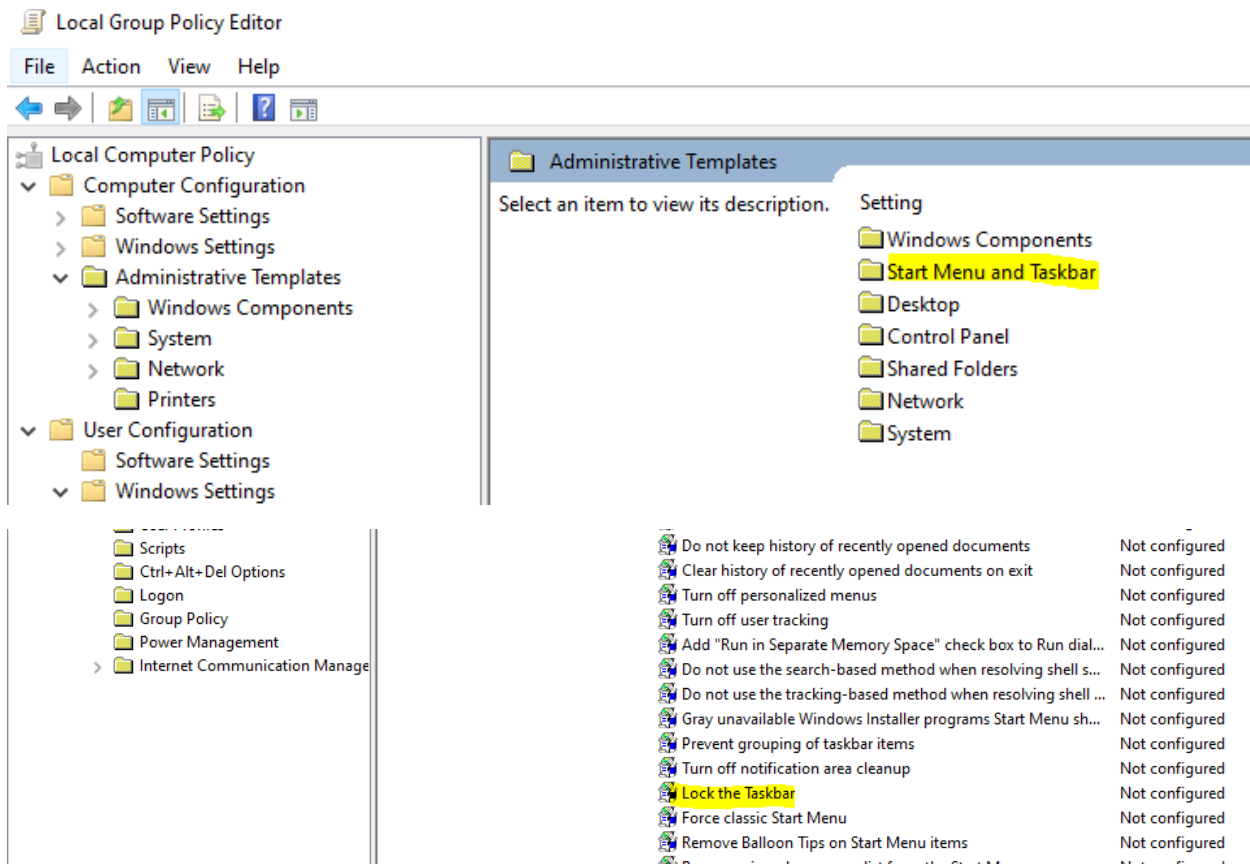


## 6 User

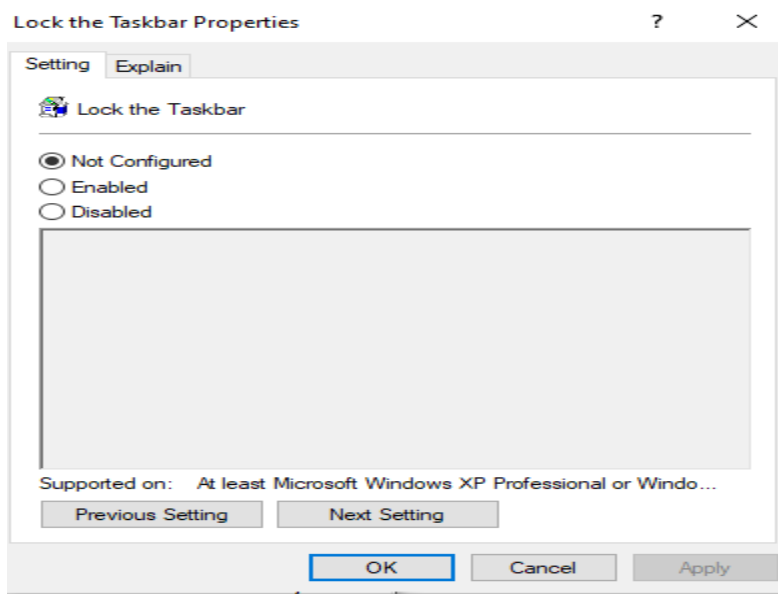
### 6.1 Lock the Taskbar

- This setting will enable or disable the taskbar which is used to switch between running applications.
- **Importance:** Enable this setting will restrict the user from resizing or moving the taskbar or vice versa.
- **Default value is not configured.**

To configure the policy->Open Local Group Policy editor->Expand User Configuration-> Expand Administrative Templates->Expand Start menu and Taskbar.














To configure Select the options Enable and disabled as shown in the image below:



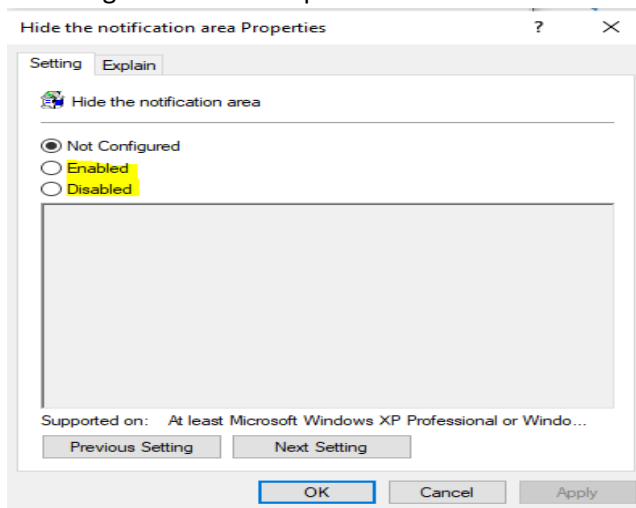
## 6.2 Hide the notification area

- This setting will enable or disable the taskbar which is used to switch between running applications.
- **Importance:** Enable this setting will hide the entire user notification area and icons or disabling it will do vice versa.
- **Default value is not configured.**

To configure the policy->Open Local Group Policy editor->Expand User Configuration-> Expand Administrative Templates->Expand Start menu and Taskbar To configure the policy->Open Local Group Policy editor->Expand User Configuration-> Expand Administrative Templates->Expand Start menu and Taskbar.

|  |                |
|--|----------------|
|  Force classic Start Menu                                 | Not configured |
|  Remove Balloon Tips on Start Menu items                  | Not configured |
|  Remove pinned programs list from the Start Menu          | Not configured |
|  Remove frequent programs list from the Start Menu       | Not configured |
|  Remove All Programs list from the Start menu           | Not configured |
|  Remove the "Undock PC" button from the Start Menu      | Not configured |
|  Remove user name from Start Menu                       | Not configured |
|  Remove Clock from the system notification area         | Not configured |
|  <b>Hide the notification area</b>                      | Not configured |
|  Do not display any custom toolbars in the taskbar      | Not configured |
|  Remove Set Program Access and Defaults from Start menu | Not configured |

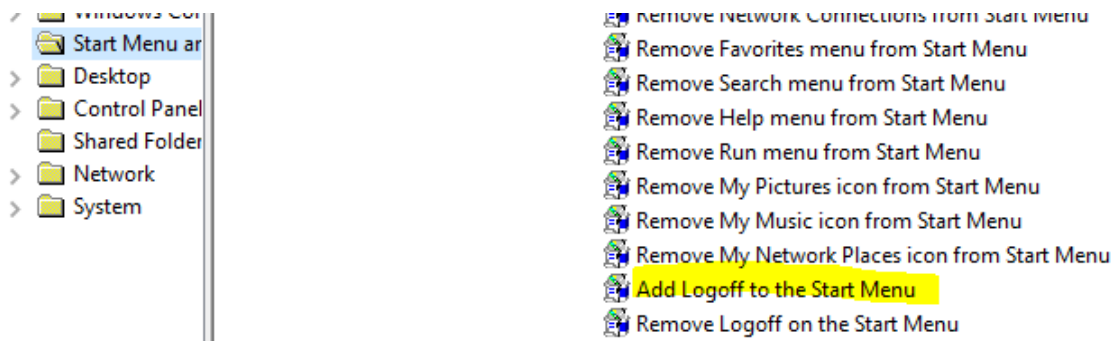
To configure Select the options Enable and disabled as shown in the image below:



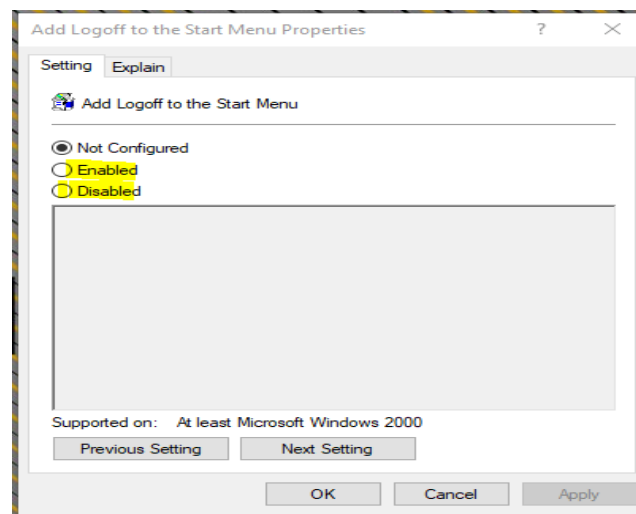
## 6.3 Add Logoff to the Start Menu

- This setting will remove the “Log Off <username>” button to the start menu
- **Importance:** Enable this setting will make the Log Off button invisible in the Start Menu or vice versa.
- **Default value is not configured.**

To configure the policy->Open Local Group Policy editor->Expand User Configuration-> Expand Administrative Templates->Expand Start menu and Taskbar To configure the policy->Open Local Group Policy editor->Expand User Configuration-> Expand Administrative Templates->Expand Start menu and Taskbar.



To configure Select the options Enable and disabled as shown in the image below:














## 6.4 Remove Logoff to the Start Menu

- This setting will remove the “Log Off <username>” button to the start menu
- **Importance:** Enable this setting will make the Log Off button invisible in the Start Menu or vice versa.

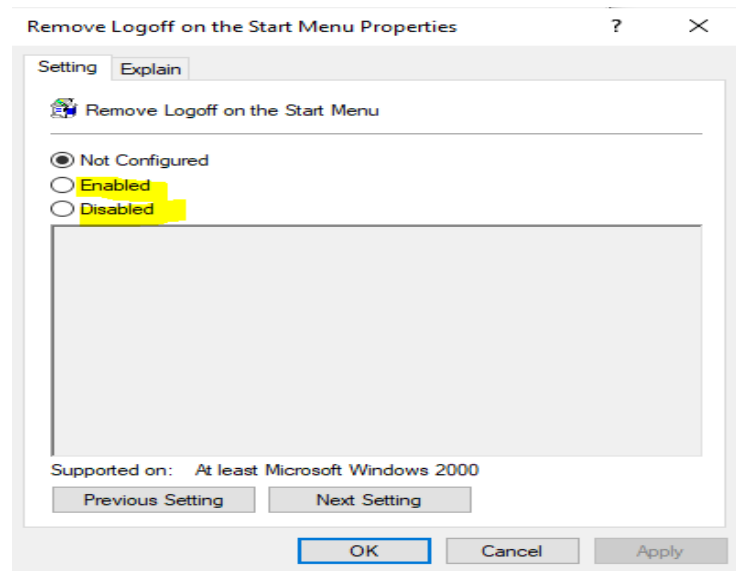


- **Default value is not configured.**

To configure the policy->Open Local Group Policy editor->Expand User Configuration-> Expand Administrative Templates->Expand Start menu and Taskbar To configure the policy->Open Local Group Policy editor->Expand User Configuration-> Expand Administrative Templates->Expand Start menu and Taskbar.

|   |  |                |
|---|--|----------------|
|  | Remove Help menu from Start Menu                     | Not configured |
|  | Remove Run menu from Start Menu                      | Not configured |
|  | Remove My Pictures icon from Start Menu              | Not configured |
|  | Remove My Music icon from Start Menu                 | Not configured |
|  | Remove My Network Places icon from Start Menu        | Not configured |
|  | Add Logoff to the Start Menu                         | Not configured |
|  | Remove Logoff on the Start Menu                      | Not configured |
|  | Remove and prevent access to the Shut Down command   | Not configured |
|  | Remove Drag-and-drop context menus on the Start Menu | Not configured |
|  | Prevent changes to Taskbar and Start Menu Settings   | Not configured |
|  | Remove access to the context menus for the taskbar   | Not configured |

To configure Select the options Enable and disabled as shown in the image below:

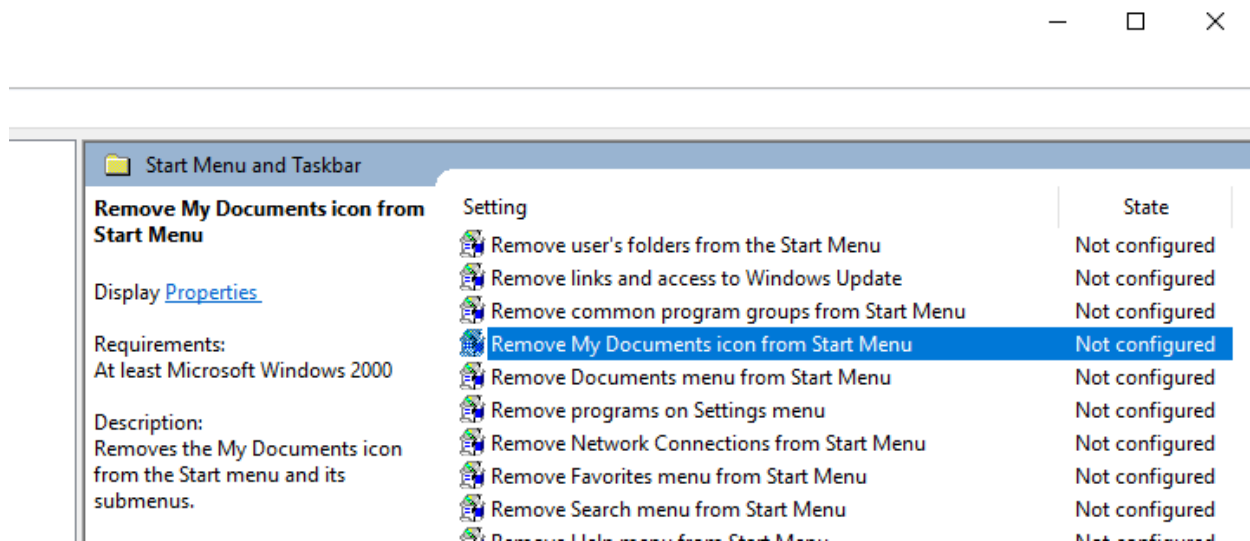


## 6.5 Remove My Documents icon from the Start Menu

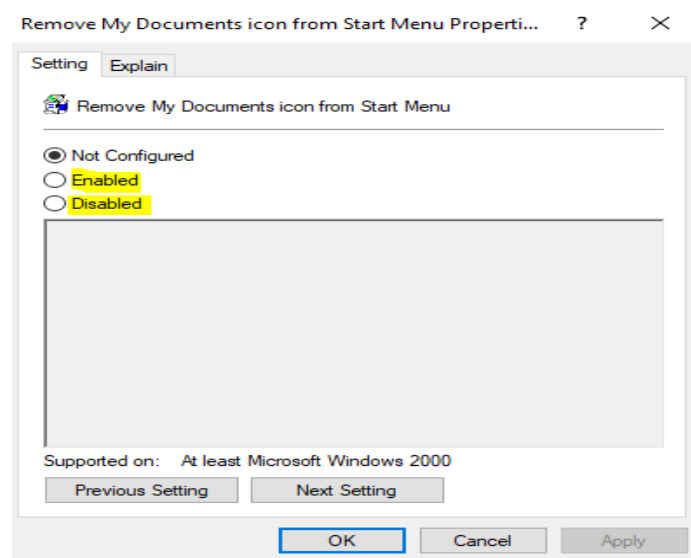
- This setting will remove MY Documents icon from the start menu
- **Importance:** The setting only removes the icon. It does not prevent user from accessing My Documents contents from other methods
- **Default value is not configured.**

To configure the policy->Open Local Group Policy editor->Expand User Configuration-> Expand Administrative Templates->Expand Start menu and Taskbar To configure the policy->Open Local

Group Policy editor->Expand User Configuration-> Expand Administrative Templates->Expand Start menu and Taskbar.



To configure Select the options Enable and disabled as shown in the image below:



## References

- <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/account-lockout-threshold>
- <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/maximum-password-age>
- <https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/security-auditing-overview>