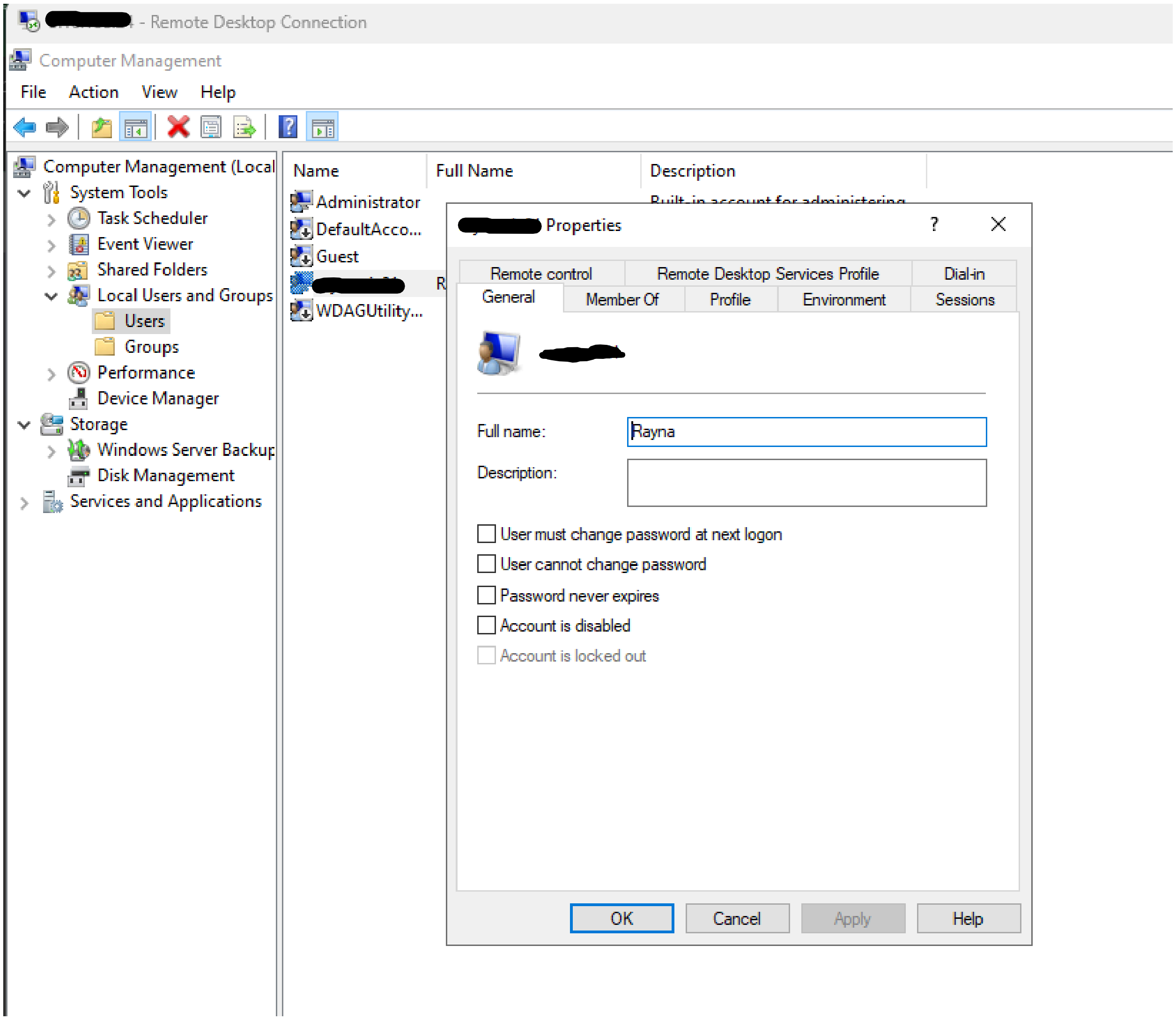
Lab 3 - Windows Server Lockdown

Rayna Campbell

October 15, 2025

1. Create an Account and Set Permissions



[redacted] Properties

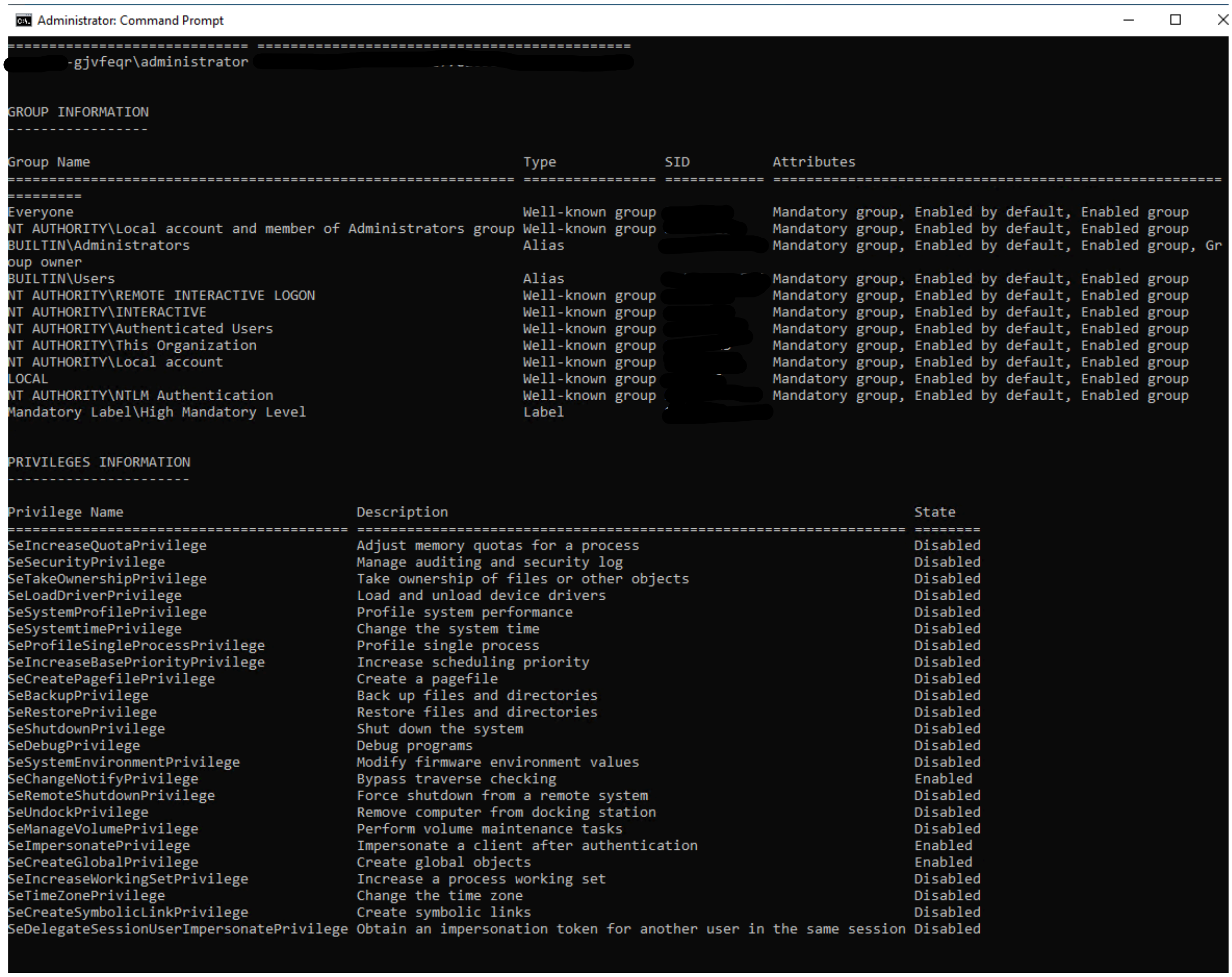
[redacted]

Full name: Rayna

Description:

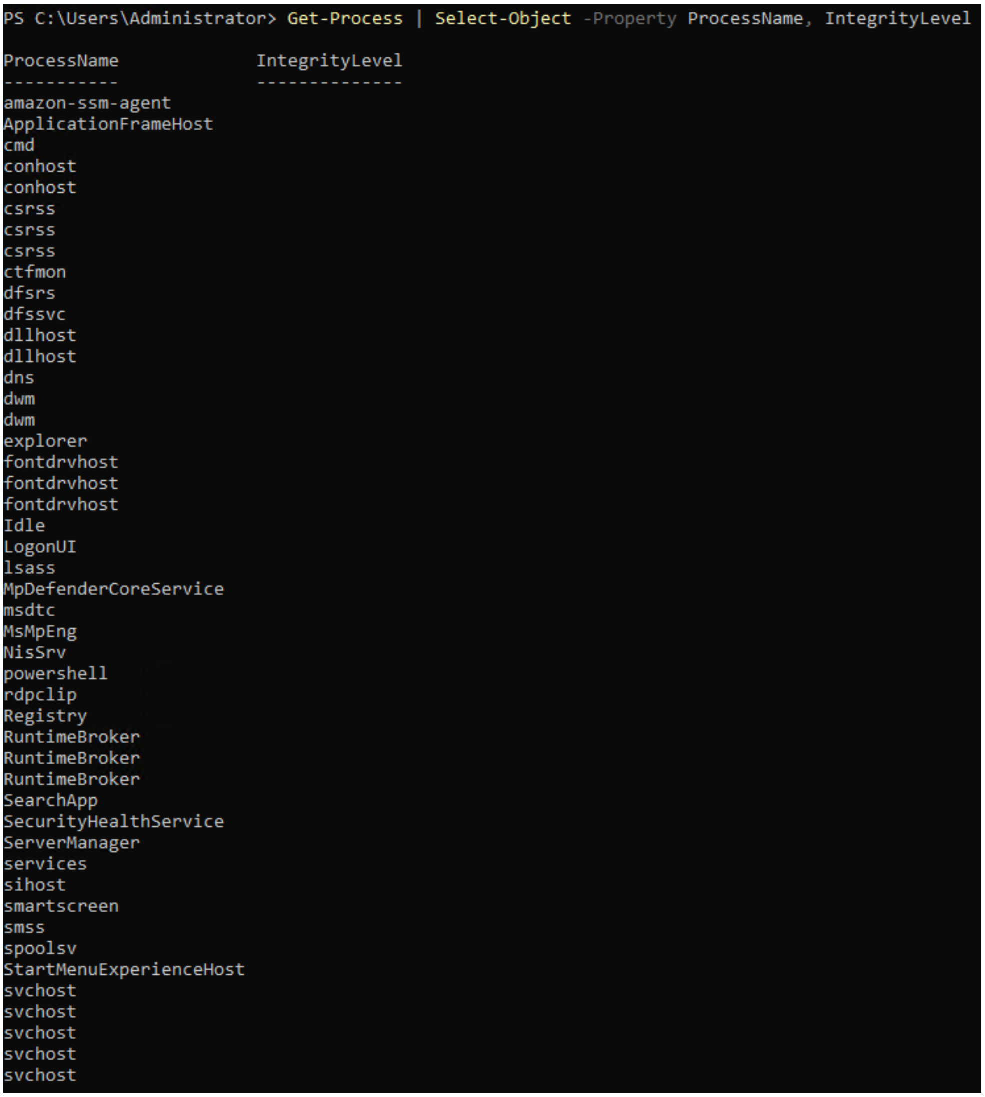
□ User must change password at next logon
□ User cannot change password
□ Password never expires
□ Account is disabled
□ Account is locked out

2. Note SID and Check Integrity Level

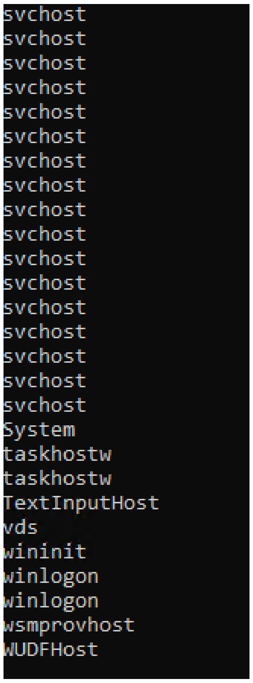


```
=========================== ==========================================
[redacted]-gjvfeqr\administrator [redacted]


GROUP INFORMATION
-----------------

Group Name                                                  Type             SID          Attributes
=========================================================== ================ ============ ==========================================================
========
Everyone                                                    Well-known group [redacted]   Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Local account and member of Administrators group Well-known group [redacted] Mandatory group, Enabled by default, Enabled group
BUILTIN\Administrators                                      Alias            [redacted]   Mandatory group, Enabled by default, Enabled group, Gr
oup owner
BUILTIN\Users                                               Alias            [redacted]   Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\REMOTE INTERACTIVE LOGON                       Well-known group [redacted]   Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\INTERACTIVE                                    Well-known group [redacted]   Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users                            Well-known group [redacted]   Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization                              Well-known group [redacted]   Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Local account                                  Well-known group [redacted]   Mandatory group, Enabled by default, Enabled group
LOCAL                                                       Well-known group [redacted]   Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication                            Well-known group [redacted]   Mandatory group, Enabled by default, Enabled group
Mandatory Label\High Mandatory Level                        Label            [redacted]


PRIVILEGES INFORMATION
----------------------

Privilege Name                            Description                                                        State
========================================= ================================================================== ========
SeIncreaseQuotaPrivilege                  Adjust memory quotas for a process                                 Disabled
SeSecurityPrivilege                       Manage auditing and security log                                   Disabled
SeTakeOwnershipPrivilege                  Take ownership of files or other objects                           Disabled
SeLoadDriverPrivilege                     Load and unload device drivers                                     Disabled
SeSystemProfilePrivilege                  Profile system performance                                         Disabled
SeSystemtimePrivilege                     Change the system time                                             Disabled
SeProfileSingleProcessPrivilege           Profile single process                                             Disabled
SeIncreaseBasePriorityPrivilege           Increase scheduling priority                                       Disabled
SeCreatePagefilePrivilege                 Create a pagefile                                                  Disabled
SeBackupPrivilege                         Back up files and directories                                      Disabled
SeRestorePrivilege                        Restore files and directories                                      Disabled
SeShutdownPrivilege                       Shut down the system                                               Disabled
SeDebugPrivilege                          Debug programs                                                     Disabled
SeSystemEnvironmentPrivilege              Modify firmware environment values                                 Disabled
SeChangeNotifyPrivilege                   Bypass traverse checking                                           Enabled
SeRemoteShutdownPrivilege                 Force shutdown from a remote system                                Disabled
SeUndockPrivilege                         Remove computer from docking station                               Disabled
SeManageVolumePrivilege                   Perform volume maintenance tasks                                   Disabled
SeImpersonatePrivilege                    Impersonate a client after authentication                          Enabled
SeCreateGlobalPrivilege                   Create global objects                                              Enabled
SeIncreaseWorkingSetPrivilege             Increase a process working set                                     Disabled
SeTimeZonePrivilege                       Change the time zone                                               Disabled
SeCreateSymbolicLinkPrivilege             Create symbolic links                                              Disabled
SeDelegateSessionUserImpersonatePrivilege Obtain an impersonation token for another user in the same session Disabled
```

3. Check Integrity Level in PowerShell

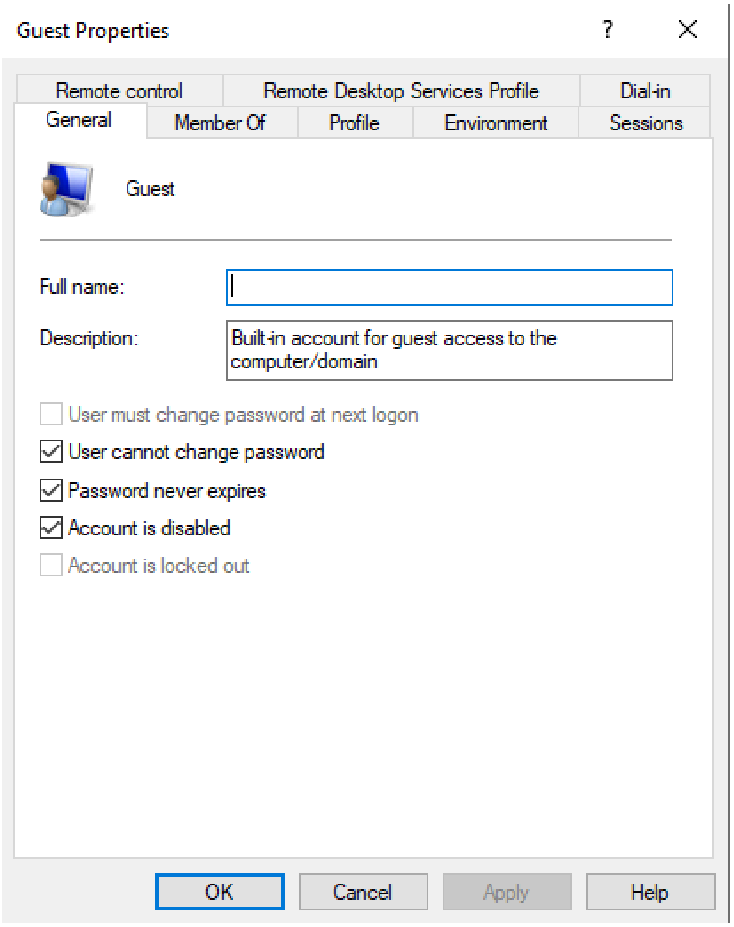


```
PS C:\Users\Administrator> Get-Process | Select-Object -Property ProcessName, IntegrityLevel

ProcessName             IntegrityLevel
-----------             --------------
amazon-ssm-agent
ApplicationFrameHost
cmd
conhost
conhost
csrss
csrss
csrss
ctfmon
dfsrs
dfssvc
dllhost
dllhost
dns
dwm
dwm
explorer
fontdrvhost
fontdrvhost
fontdrvhost
Idle
LogonUI
lsass
MpDefenderCoreService
msdtc
MsMpEng
NisSrv
powershell
rdpclip
Registry
RuntimeBroker
RuntimeBroker
RuntimeBroker
SearchApp
SecurityHealthService
ServerManager
services
sihost
smartscreen
smss
spoolsv
StartMenuExperienceHost
svchost
svchost
svchost
svchost
svchost
```



```
svchost
svchost
svchost
svchost
svchost
svchost
svchost
svchost
svchost
svchost
svchost
svchost
svchost
svchost
svchost
svchost
svchost
System
taskhostw
taskhostw
TextInputHost
vds
wininit
winlogon
winlogon
wsmprovhost
WUDFHost
```

4. Disable Guest Account



Guest Properties

Guest

Full name:

Description: Built-in account for guest access to the computer/domain

□ User must change password at next logon

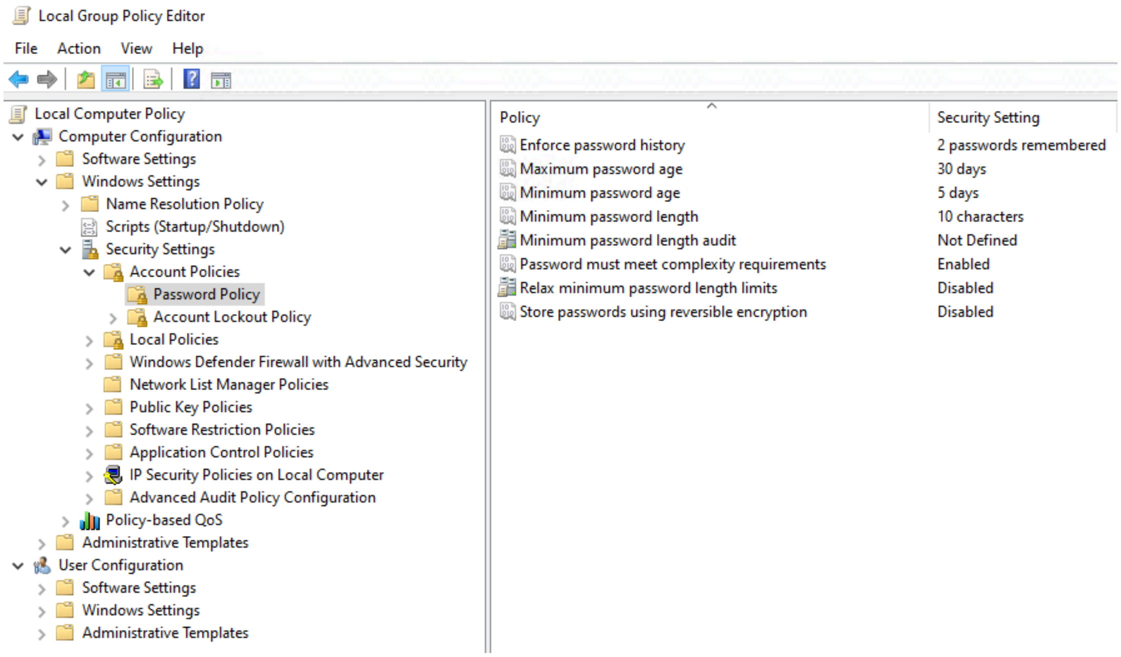
☑ User cannot change password

☑ Password never expires

☑ Account is disabled

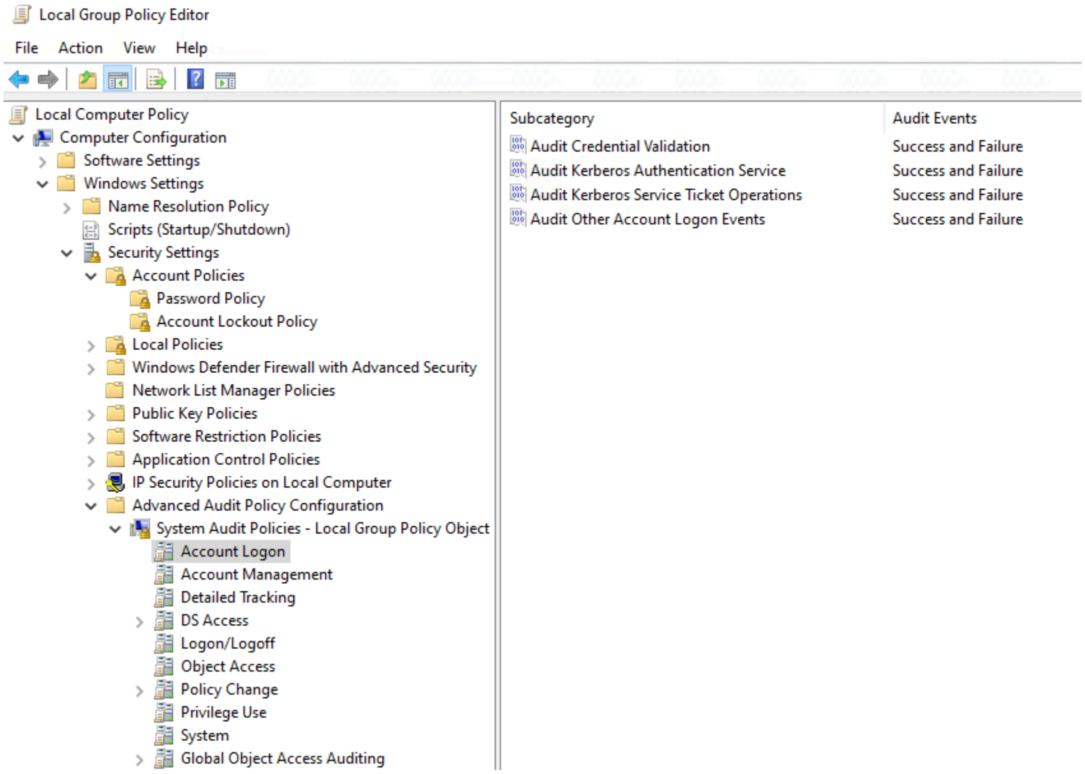
□ Account is locked out

5. Open Group Policy Editor and Set Password Policies

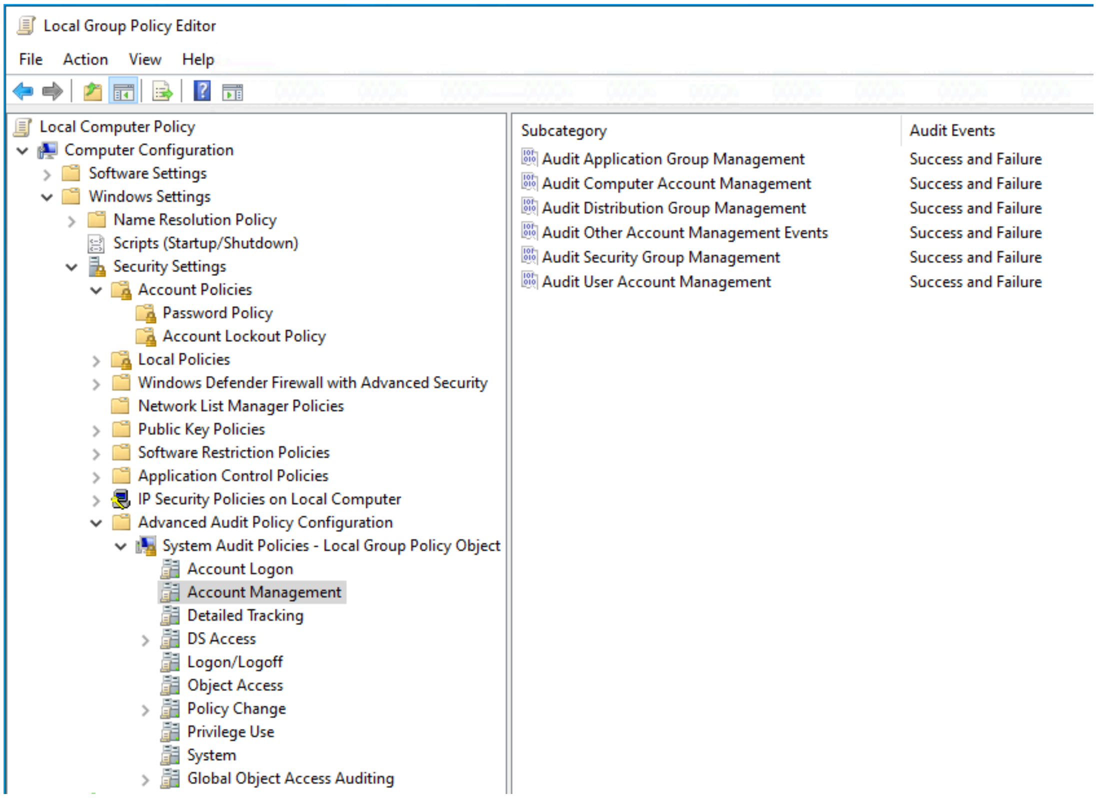


Policy	Security Setting
Enforce password history	2 passwords remembered
Maximum password age	30 days
Minimum password age	5 days
Minimum password length	10 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Enabled
Relax minimum password length limits	Disabled
Store passwords using reversible encryption	Disabled

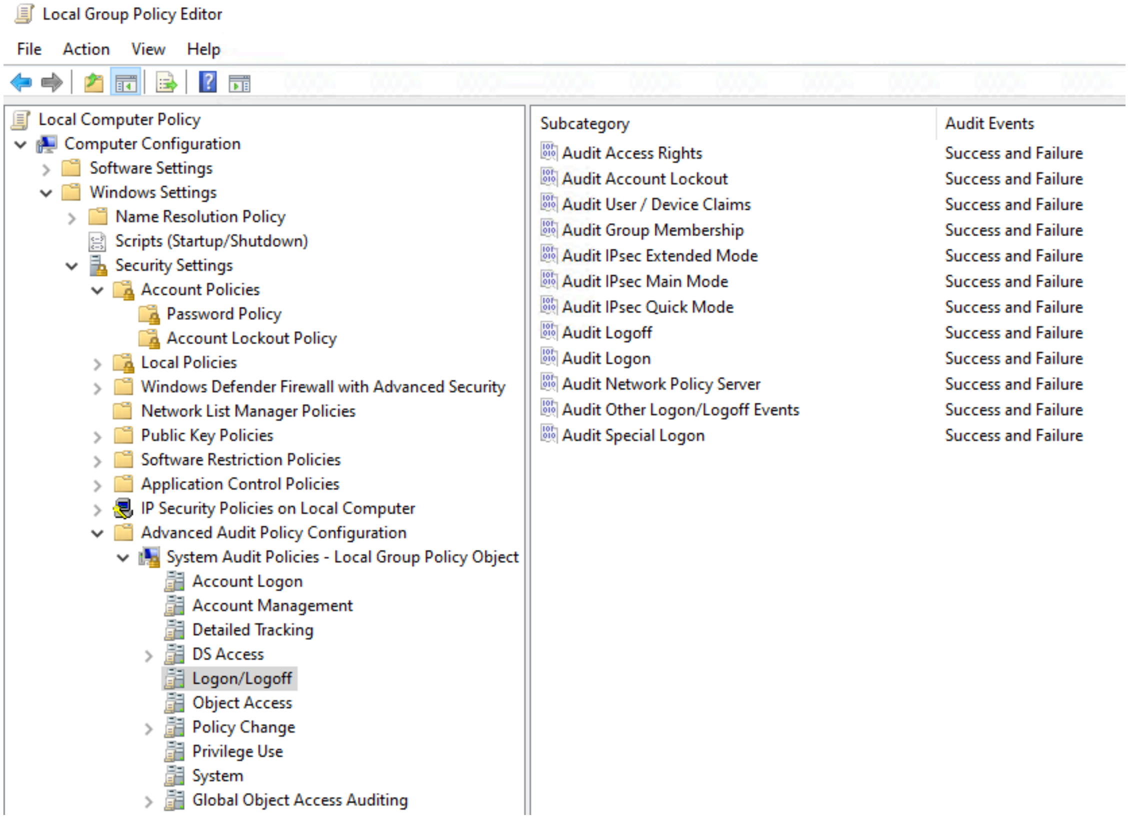
6. Enable Audit for Success and Failures


Local Group Policy Editor
File
Action
View
Help
Local Computer Policy
Computer Configuration
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
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
System Audit Policies - Local Group Policy Object
Account Logon
Account Management
Detailed Tracking
DS Access
Logon/Logoff
Object Access
Policy Change
Privilege Use
System
Global Object Access Auditing

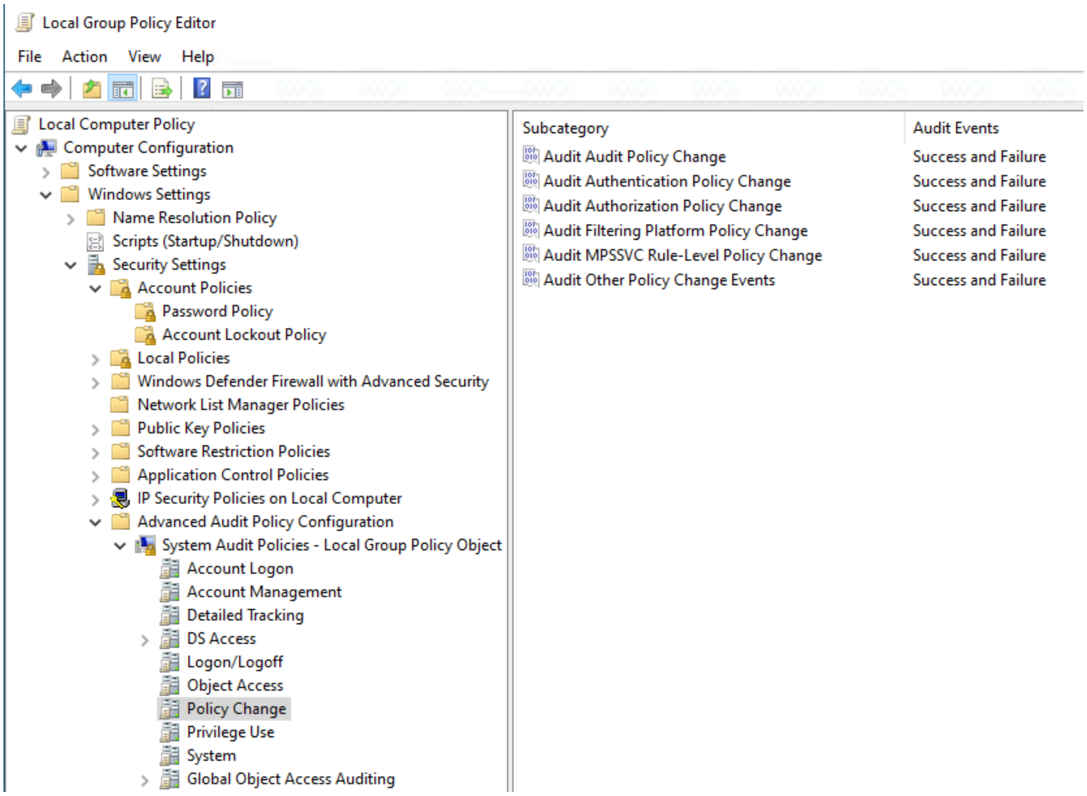
Subcategory	Audit Events
Audit Credential Validation	Success and Failure
Audit Kerberos Authentication Service	Success and Failure
Audit Kerberos Service Ticket Operations	Success and Failure
Audit Other Account Logon Events	Success and Failure


Local Group Policy Editor
File
Action
View
Help
Local Computer Policy
Computer Configuration
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
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
System Audit Policies - Local Group Policy Object
Account Logon
Account Management
Detailed Tracking
DS Access
Logon/Logoff
Object Access
Policy Change
Privilege Use
System
Global Object Access Auditing

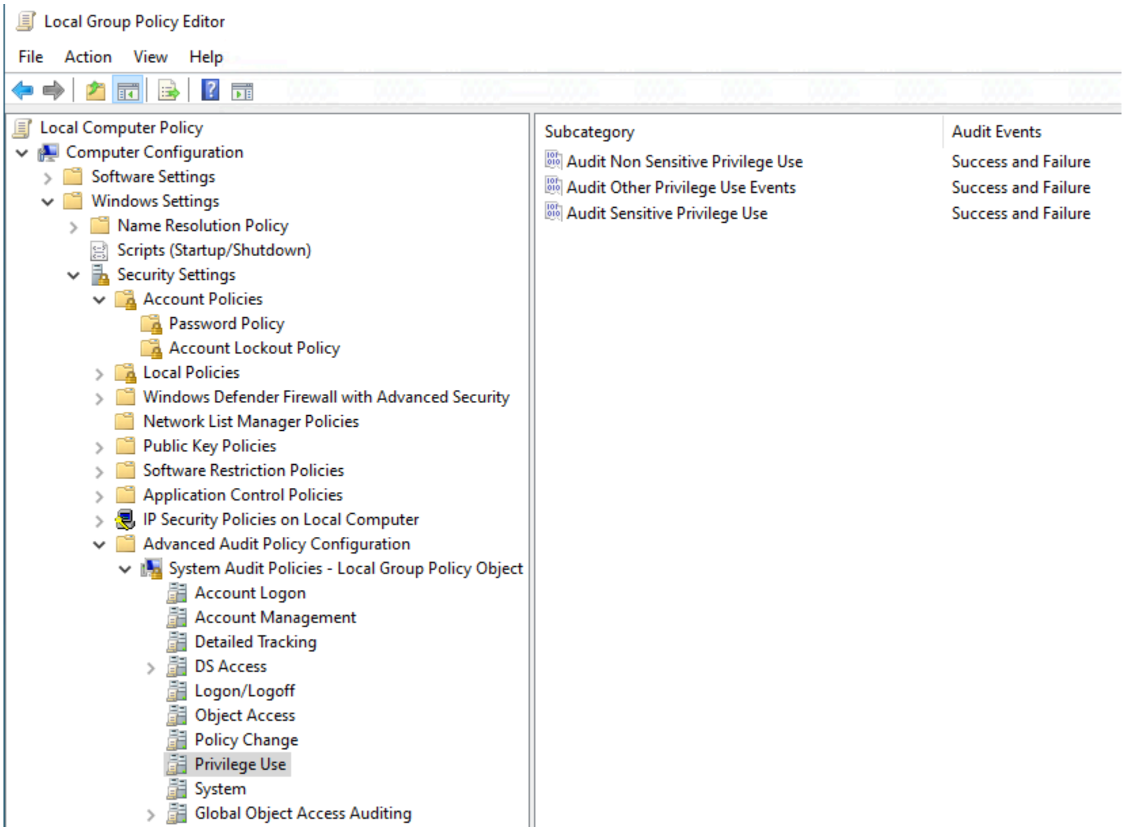
Subcategory	Audit Events
Audit Application Group Management	Success and Failure
Audit Computer Account Management	Success and Failure
Audit Distribution Group Management	Success and Failure
Audit Other Account Management Events	Success and Failure
Audit Security Group Management	Success and Failure
Audit User Account Management	Success and Failure


Local Group Policy Editor
File
Action
View
Help
Local Computer Policy
Computer Configuration
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
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
System Audit Policies - Local Group Policy Object
Account Logon
Account Management
Detailed Tracking
DS Access
Logon/Logoff
Object Access
Policy Change
Privilege Use
System
Global Object Access Auditing

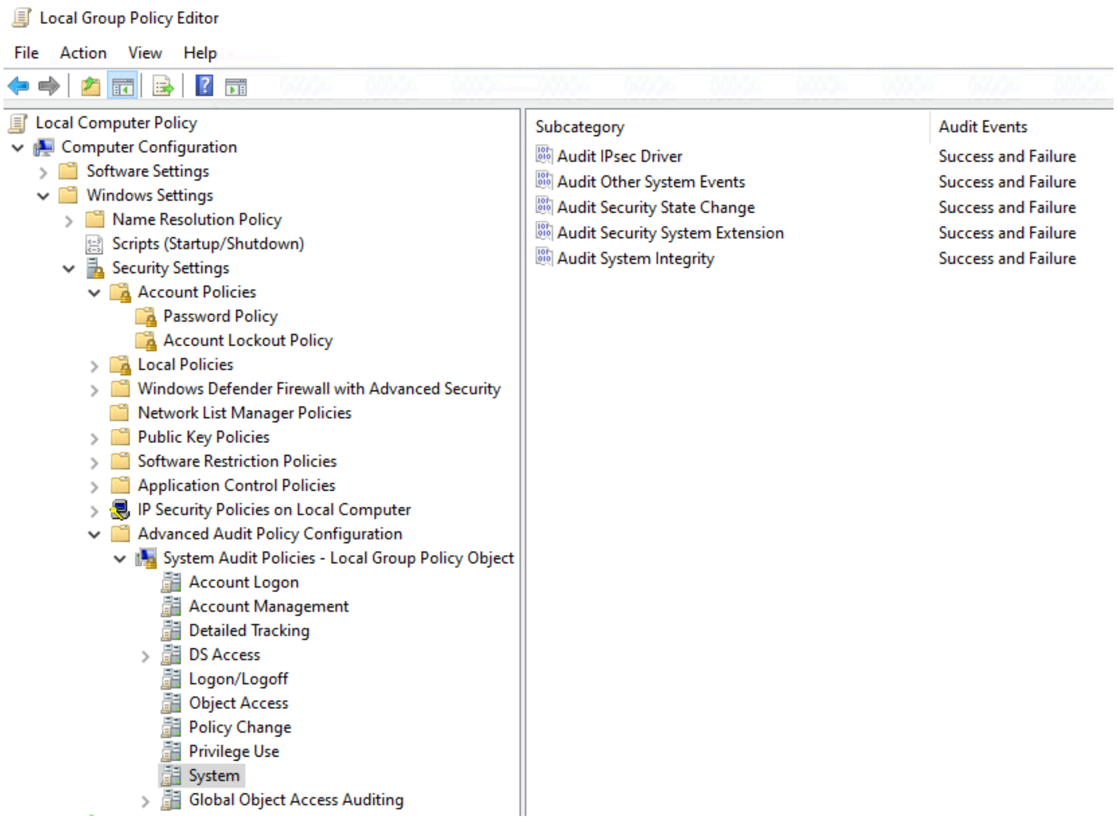
Subcategory	Audit Events
Audit Access Rights	Success and Failure
Audit Account Lockout	Success and Failure
Audit User / Device Claims	Success and Failure
Audit Group Membership	Success and Failure
Audit IPsec Extended Mode	Success and Failure
Audit IPsec Main Mode	Success and Failure
Audit IPsec Quick Mode	Success and Failure
Audit Logoff	Success and Failure
Audit Logon	Success and Failure
Audit Network Policy Server	Success and Failure
Audit Other Logon/Logoff Events	Success and Failure
Audit Special Logon	Success and Failure


Local Group Policy Editor
File
Action
View
Help
Local Computer Policy
Computer Configuration
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
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
System Audit Policies - Local Group Policy Object
Account Logon
Account Management
Detailed Tracking
DS Access
Logon/Logoff
Object Access
Policy Change
Privilege Use
System
Global Object Access Auditing

Subcategory	Audit Events
Audit Audit Policy Change	Success and Failure
Audit Authentication Policy Change	Success and Failure
Audit Authorization Policy Change	Success and Failure
Audit Filtering Platform Policy Change	Success and Failure
Audit MPSSVC Rule-Level Policy Change	Success and Failure
Audit Other Policy Change Events	Success and Failure

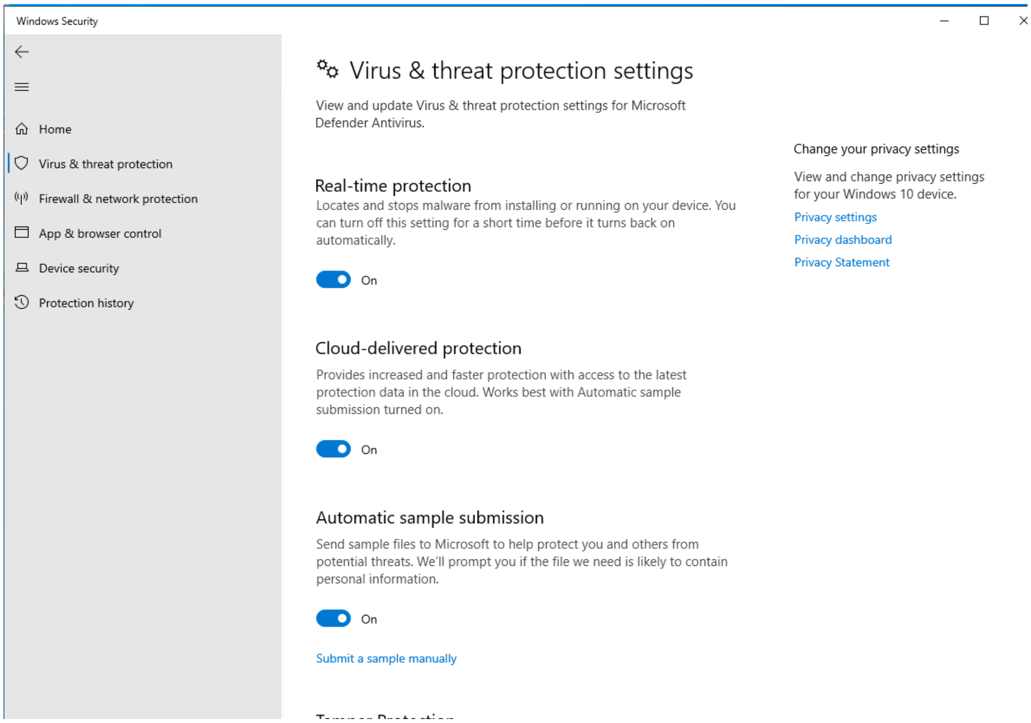

Local Group Policy Editor
File
Action
View
Help
Local Computer Policy
Computer Configuration
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Defender Firewall with Advanced Security
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Computer
Advanced Audit Policy Configuration
System Audit Policies - Local Group Policy Object
Account Logon
Account Management
Detailed Tracking
DS Access
Logon/Logoff
Object Access
Policy Change
Privilege Use
System
Global Object Access Auditing

Subcategory	Audit Events
Audit Non Sensitive Privilege Use	Success and Failure
Audit Other Privilege Use Events	Success and Failure
Audit Sensitive Privilege Use	Success and Failure


Local Group Policy Editor
File
Action
View
Help
Local Computer Policy
Computer Configuration
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
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
System Audit Policies - Local Group Policy Object
Account Logon
Account Management
Detailed Tracking
DS Access
Logon/Logoff
Object Access
Policy Change
Privilege Use
System
Global Object Access Auditing

Subcategory	Audit Events
Audit IPsec Driver	Success and Failure
Audit Other System Events	Success and Failure
Audit Security State Change	Success and Failure
Audit Security System Extension	Success and Failure
Audit System Integrity	Success and Failure

7. Turn on Credential Guard and ATP



Virus & threat protection settings

View and update Virus & threat protection settings for Microsoft Defender Antivirus.

Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

On

Cloud-delivered protection

Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.

On

Automatic sample submission

Send sample files to Microsoft to help protect you and others from potential threats. We'll prompt you if the file we need is likely to contain personal information.

On

Submit a sample manually

Tamper Protection

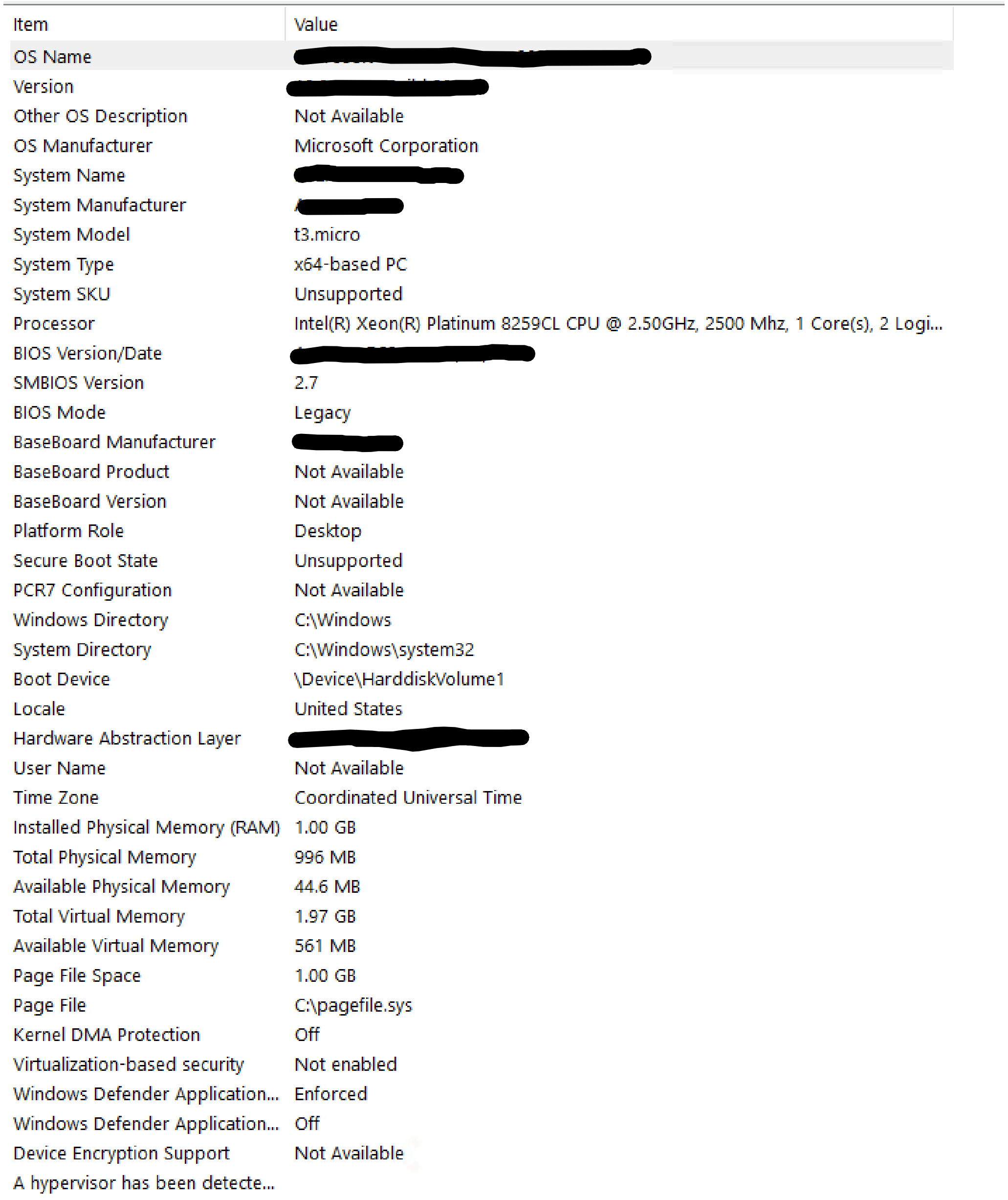
Change your privacy settings

View and change privacy settings for your Windows 10 device.

Privacy settings

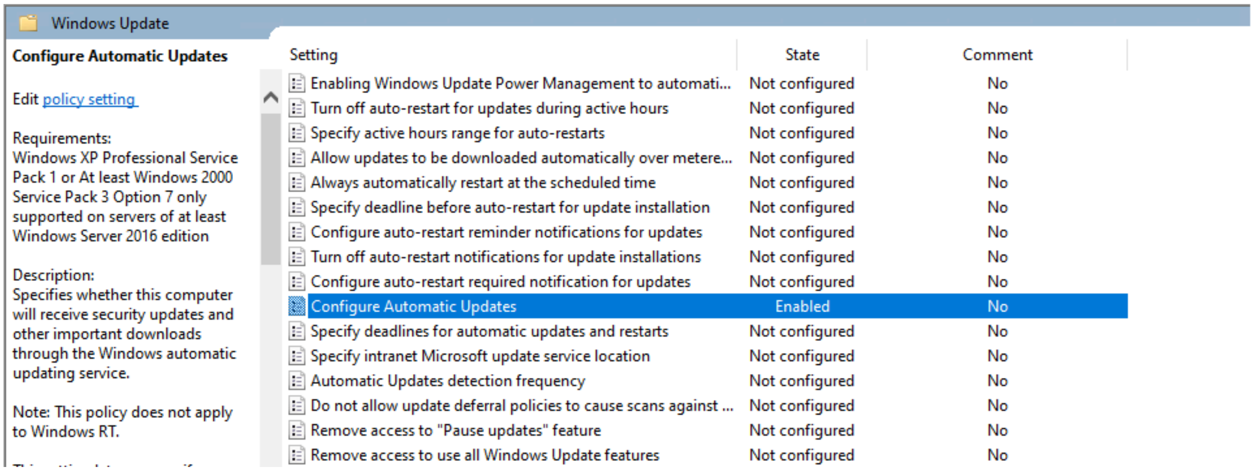
Privacy dashboard

Privacy Statement



Item	Value
OS Name	[redacted]
Version	[redacted]
Other OS Description	Not Available
OS Manufacturer	Microsoft Corporation
System Name	[redacted]
System Manufacturer	[redacted]
System Model	t3.micro
System Type	x64-based PC
System SKU	Unsupported
Processor	Intel(R) Xeon(R) Platinum 8259CL CPU @ 2.50GHz, 2500 Mhz, 1 Core(s), 2 Logi...
BIOS Version/Date	[redacted]
SMBIOS Version	2.7
BIOS Mode	Legacy
BaseBoard Manufacturer	[redacted]
BaseBoard Product	Not Available
BaseBoard Version	Not Available
Platform Role	Desktop
Secure Boot State	Unsupported
PCR7 Configuration	Not Available
Windows Directory	C:\Windows
System Directory	C:\Windows\system32
Boot Device	\Device\HarddiskVolume1
Locale	United States
Hardware Abstraction Layer	[redacted]
User Name	Not Available
Time Zone	Coordinated Universal Time
Installed Physical Memory (RAM)	1.00 GB
Total Physical Memory	996 MB
Available Physical Memory	44.6 MB
Total Virtual Memory	1.97 GB
Available Virtual Memory	561 MB
Page File Space	1.00 GB
Page File	C:\pagefile.sys
Kernel DMA Protection	Off
Virtualization-based security	Not enabled
Windows Defender Application...	Enforced
Windows Defender Application...	Off
Device Encryption Support	Not Available
A hypervisor has been detecte...	

8. Group Policy for Automated Patches



Windows Update

Configure Automatic Updates

Edit policy setting

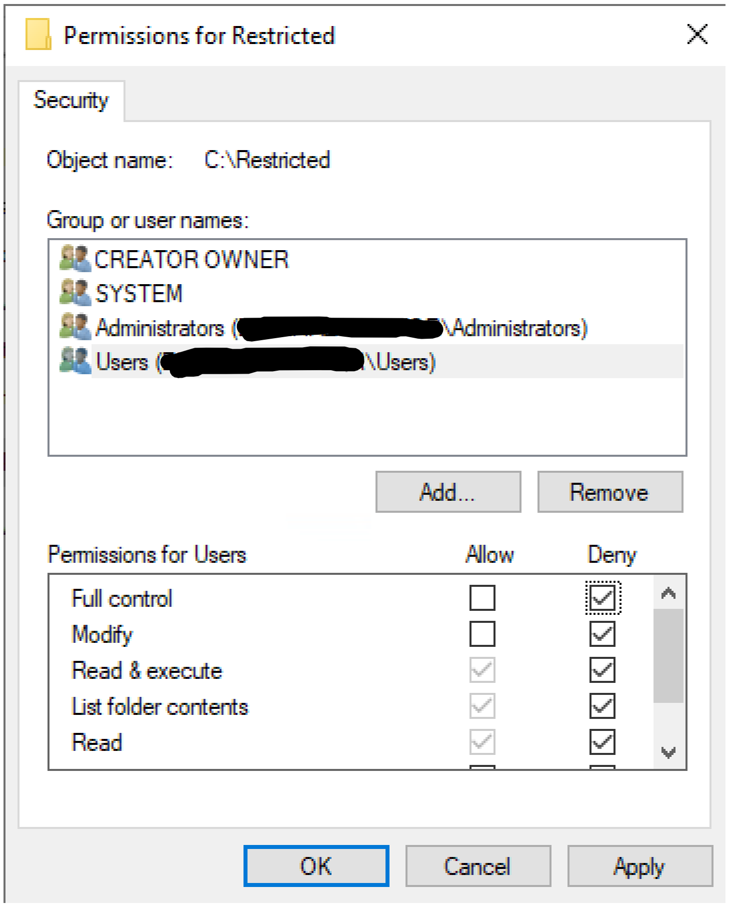
Requirements:
Windows XP Professional Service Pack 1 or At least Windows 2000 Service Pack 3 Option 7 only supported on servers of at least Windows Server 2016 edition

Description:
Specifies whether this computer will receive security updates and other important downloads through the Windows automatic updating service.

Note: This policy does not apply to Windows RT.

Setting	State	Comment
Enabling Windows Update Power Management to automati...	Not configured	No
Turn off auto-restart for updates during active hours	Not configured	No
Specify active hours range for auto-restarts	Not configured	No
Allow updates to be downloaded automatically over metere...	Not configured	No
Always automatically restart at the scheduled time	Not configured	No
Specify deadline before auto-restart for update installation	Not configured	No
Configure auto-restart reminder notifications for updates	Not configured	No
Turn off auto-restart notifications for update installations	Not configured	No
Configure auto-restart required notification for updates	Not configured	No
Configure Automatic Updates	Enabled	No
Specify deadlines for automatic updates and restarts	Not configured	No
Specify intranet Microsoft update service location	Not configured	No
Automatic Updates detection frequency	Not configured	No
Do not allow update deferral policies to cause scans against ...	Not configured	No
Remove access to "Pause updates" feature	Not configured	No
Remove access to use all Windows Update features	Not configured	No

9. Create a Folder and Restrict Permissions



Permissions for Restricted

Security

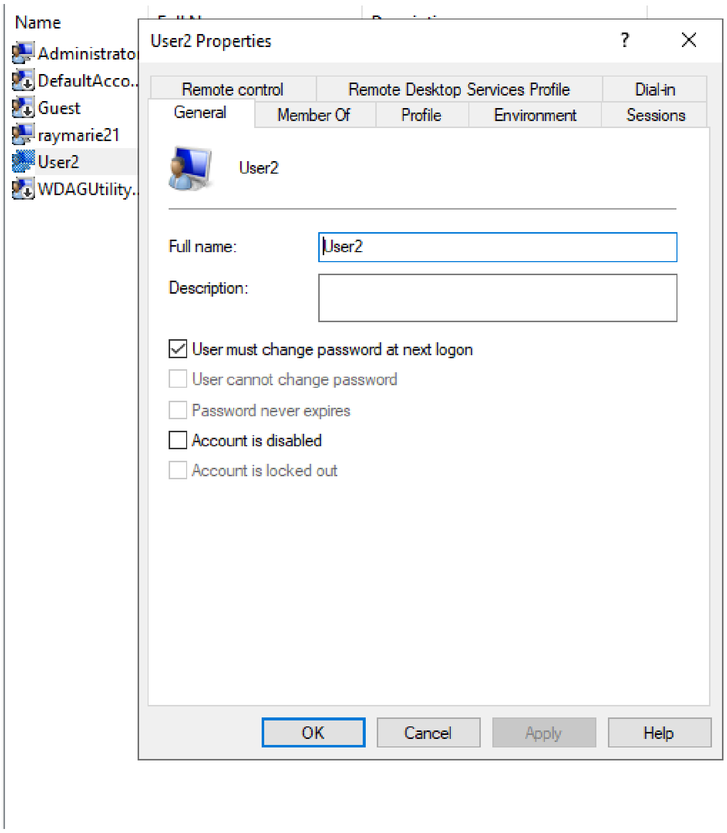
Object name: C:\Restricted

Group or user names:

- CREATOR OWNER
- SYSTEM
- Administrators ([redacted]\Administrators)
- Users ([redacted]\Users)

Permissions for Users	Allow	Deny
Full control	□	☑
Modify	□	☑
Read & execute	☑	☑
List folder contents	☑	☑
Read	☑	☑

10. Create a Local User Account



User2

Full name: User2

Description:

☑ User must change password at next logon

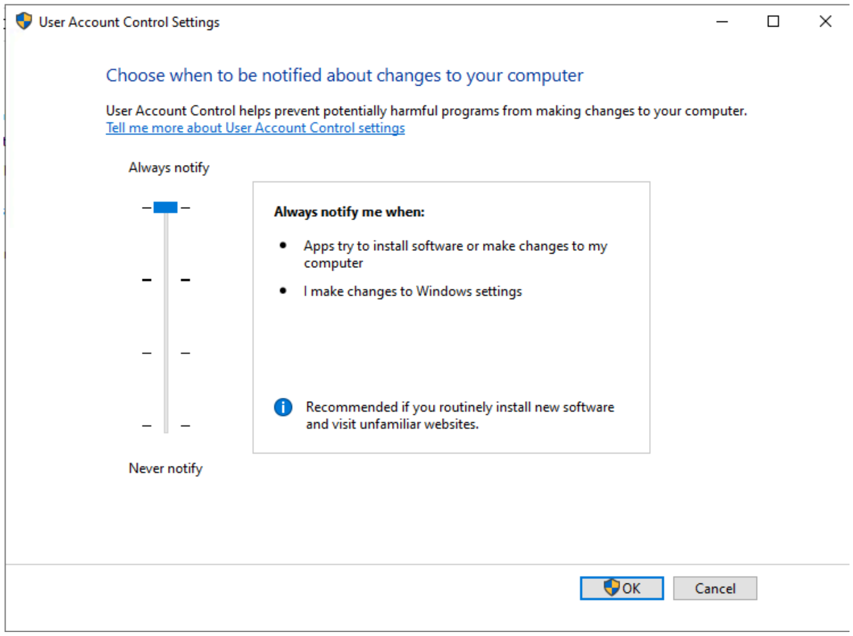
□ User cannot change password

□ Password never expires

□ Account is disabled

□ Account is locked out

11. Change UAC Settings



Choose when to be notified about changes to your computer

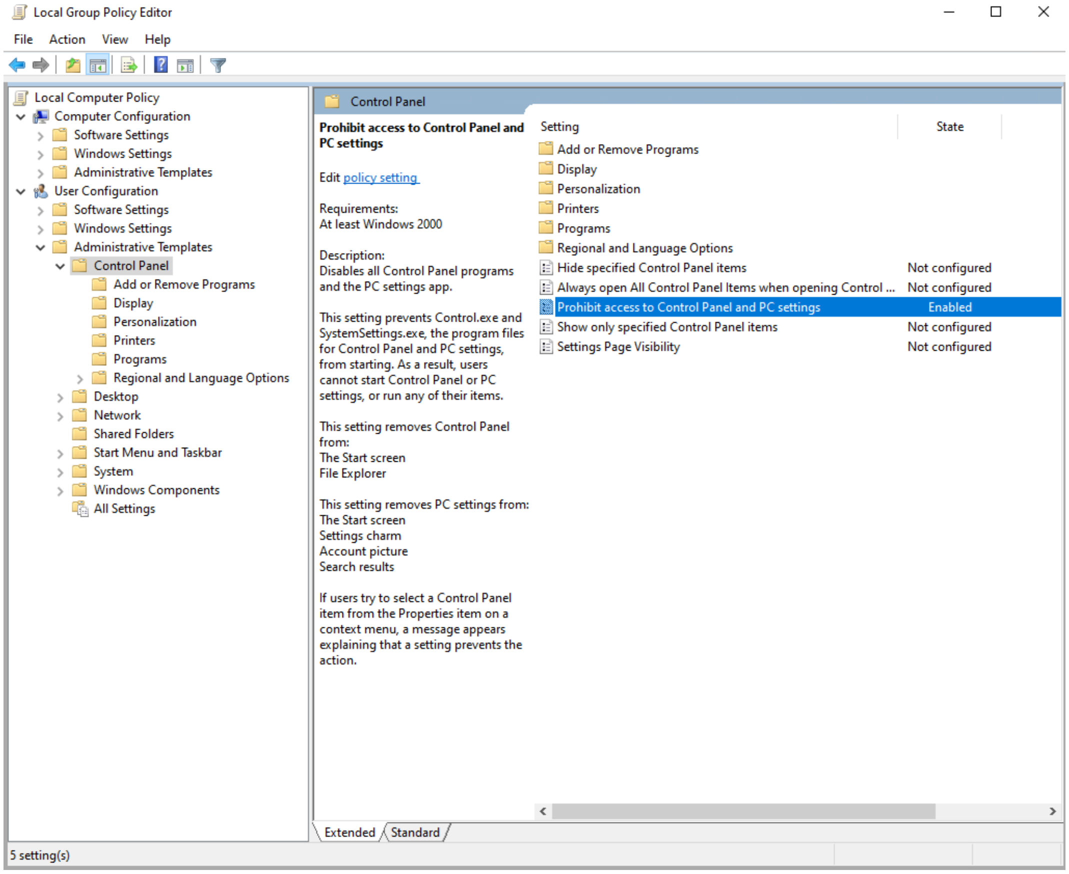
User Account Control helps prevent potentially harmful programs from making changes to your computer.
Tell me more about User Account Control settings

Always notify me when:

- Apps try to install software or make changes to my computer
- I make changes to Windows settings

Recommended if you routinely install new software and visit unfamiliar websites.

12. Moderate Access to Control Panel and Command Prompt, Restrict Software Installations



Prohibit access to Control Panel and PC settings

Edit policy setting

Requirements:
At least Windows 2000

Description:
Disables all Control Panel programs and the PC settings app.

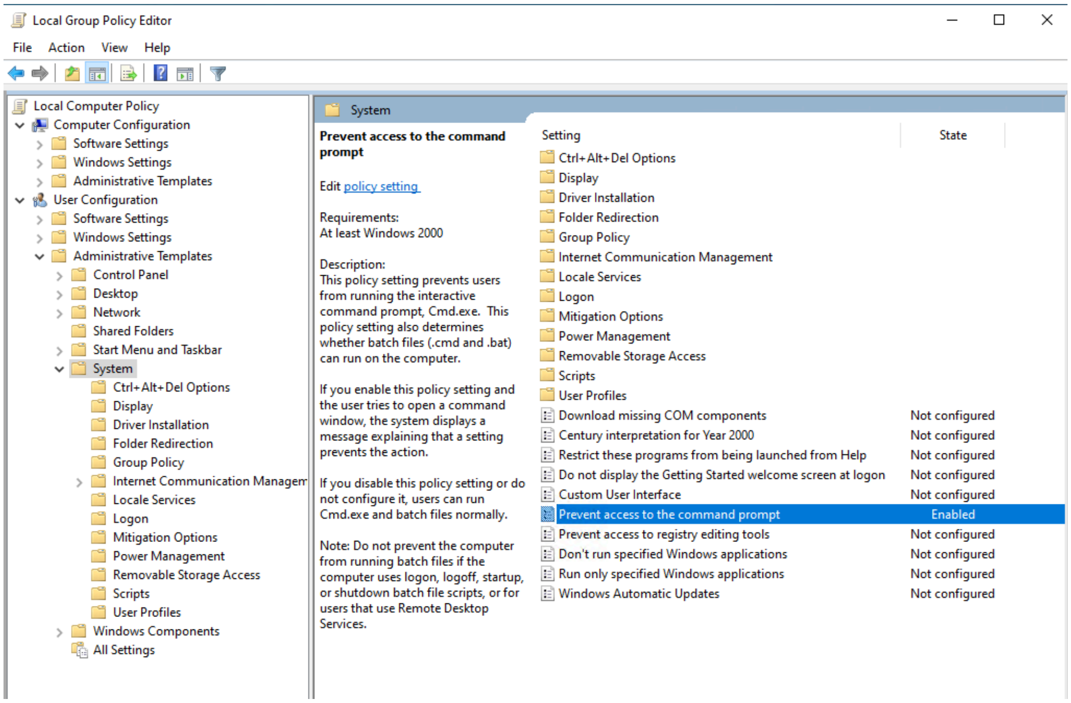
This setting prevents Control.exe and SystemSettings.exe, the program files for Control Panel and PC settings, from starting. As a result, users cannot start Control Panel or PC settings, or run any of their items.

This setting removes Control Panel from:
The Start screen
File Explorer

This setting removes PC settings from:
The Start screen
Settings charm
Account picture
Search results

If users try to select a Control Panel item from the Properties item on a context menu, a message appears explaining that a setting prevents the action.

Setting	State
Add or Remove Programs	
Display	
Personalization	
Printers	
Programs	
Regional and Language Options	
Hide specified Control Panel items	Not configured
Always open All Control Panel Items when opening Control ...	Not configured
Prohibit access to Control Panel and PC settings	Enabled
Show only specified Control Panel items	Not configured
Settings Page Visibility	Not configured



Prevent access to the command prompt

Edit policy setting

Requirements:
At least Windows 2000

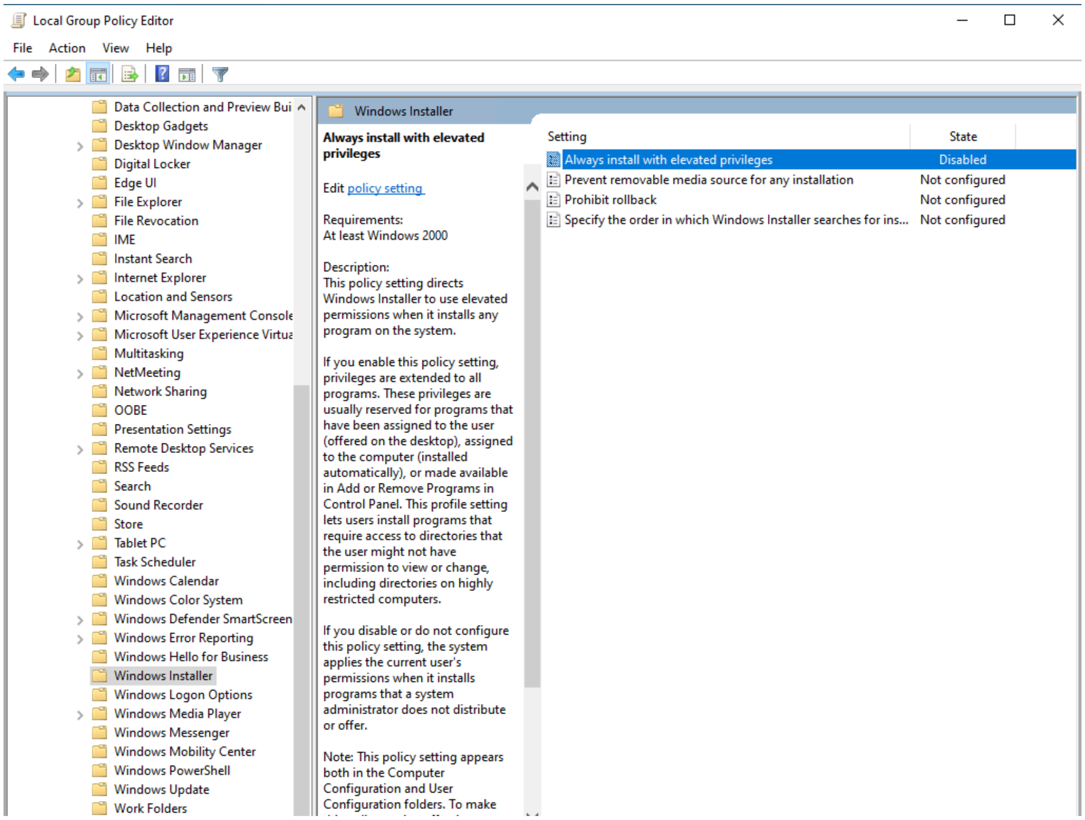
Description:
This policy setting prevents users from running the interactive command prompt, Cmd.exe. This policy setting also determines whether batch files (.cmd and .bat) can run on the computer.

If you enable this policy setting and the user tries to open a command window, the system displays a message explaining that a setting prevents the action.

If you disable this policy setting or do not configure it, users can run Cmd.exe and batch files normally.

Note: Do not prevent the computer from running batch files if the computer uses logon, logoff, startup, or shutdown batch file scripts, or for users that use Remote Desktop Services.

Setting	State
Ctrl+Alt+Del Options	
Display	
Driver Installation	
Folder Redirection	
Group Policy	
Internet Communication Management	
Locale Services	
Logon	
Mitigation Options	
Power Management	
Removable Storage Access	
Scripts	
User Profiles	
Download missing COM components	Not configured
Century interpretation for Year 2000	Not configured
Restrict these programs from being launched from Help	Not configured
Do not display the Getting Started welcome screen at logon	Not configured
Custom User Interface	Not configured
Prevent access to the command prompt	Enabled
Prevent access to registry editing tools	Not configured
Don't run specified Windows applications	Not configured
Run only specified Windows applications	Not configured
Windows Automatic Updates	Not configured



Always install with elevated privileges

Edit policy setting

Requirements:
At least Windows 2000

Description:
This policy setting directs Windows Installer to use elevated permissions when it installs any program on the system.

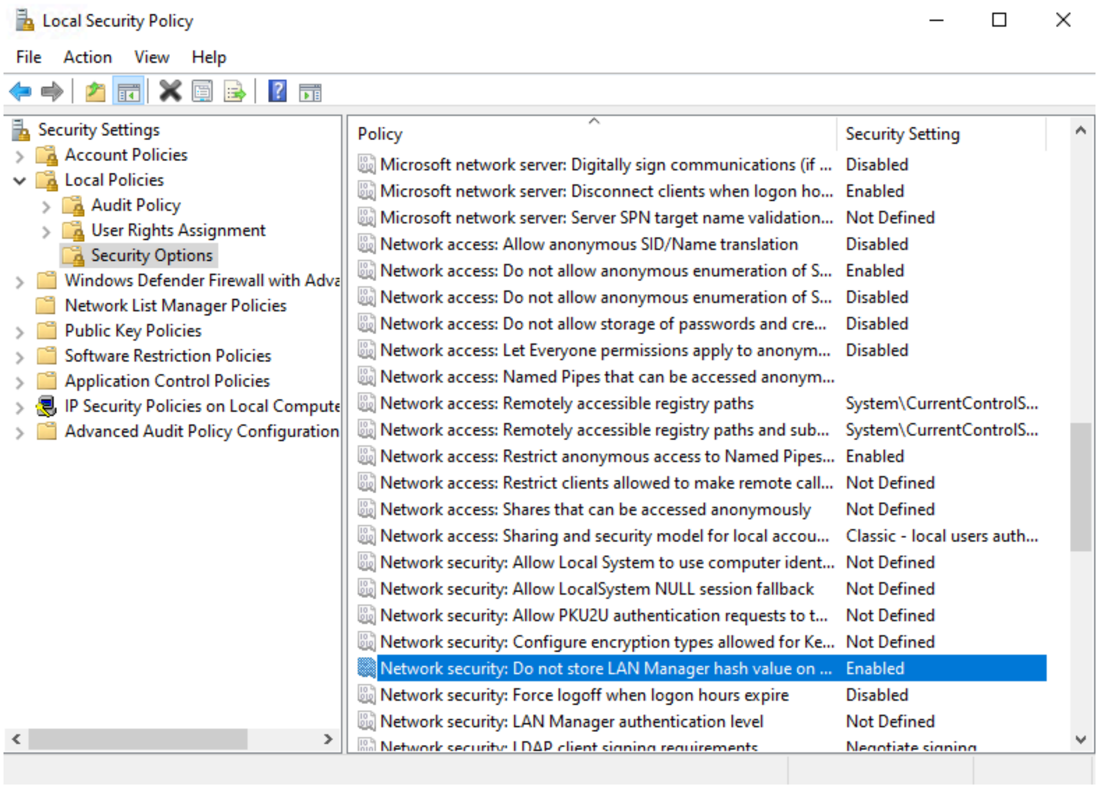
If you enable this policy setting, privileges are extended to all programs. These privileges are usually reserved for programs that have been assigned to the user (offered on the desktop), assigned to the computer (installed automatically), or made available in Add or Remove Programs in Control Panel. This profile setting lets users install programs that require access to directories that the user might not have permission to view or change, including directories on highly restricted computers.

If you disable or do not configure this policy setting, the system applies the current user's permissions when it installs programs that a system administrator does not distribute or offer.

Note: This policy setting appears both in the Computer Configuration and User Configuration folders. To make

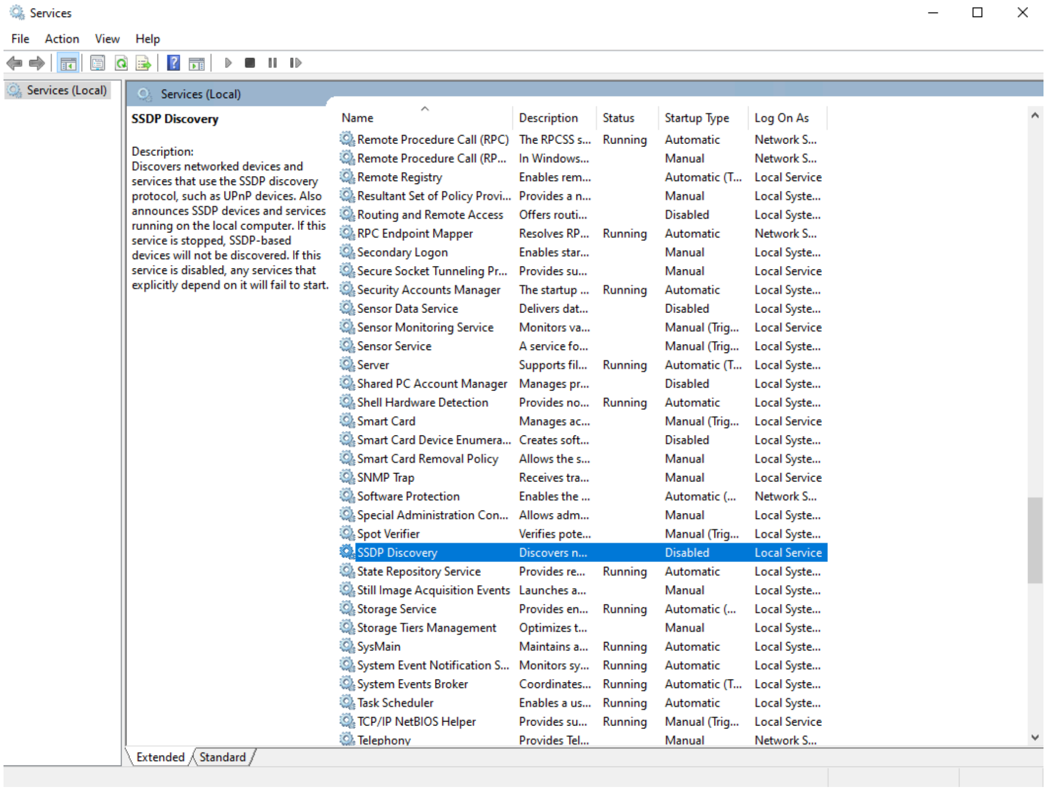
Setting	State
Always install with elevated privileges	Disabled
Prevent removable media source for any installation	Not configured
Prohibit rollback	Not configured
Specify the order in which Windows Installer searches for ins...	Not configured

13. Prevent Storing NetLM Hash


Local Security Policy
File Action View Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Policy	Security Setting
Microsoft network server: Digitally sign communications (if ...	Disabled
Microsoft network server: Disconnect clients when logon ho...	Enabled
Microsoft network server: Server SPN target name validation...	Not Defined
Network access: Allow anonymous SID/Name translation	Disabled
Network access: Do not allow anonymous enumeration of S...	Enabled
Network access: Do not allow anonymous enumeration of S...	Disabled
Network access: Do not allow storage of passwords and cre...	Disabled
Network access: Let Everyone permissions apply to anonym...	Disabled
Network access: Named Pipes that can be accessed anonym...	
Network access: Remotely accessible registry paths	System\CurrentControlS...
Network access: Remotely accessible registry paths and sub...	System\CurrentControlS...
Network access: Restrict anonymous access to Named Pipes...	Enabled
Network access: Restrict clients allowed to make remote call...	Not Defined
Network access: Shares that can be accessed anonymously	Not Defined
Network access: Sharing and security model for local accou...	Classic - local users auth...
Network security: Allow Local System to use computer ident...	Not Defined
Network security: Allow LocalSystem NULL session fallback	Not Defined
Network security: Allow PKU2U authentication requests to t...	Not Defined
Network security: Configure encryption types allowed for Ke...	Not Defined
Network security: Do not store LAN Manager hash value on ...	Enabled
Network security: Force logoff when logon hours expire	Disabled
Network security: LAN Manager authentication level	Not Defined
Network security: LDAP client signing requirements	Negotiate signing

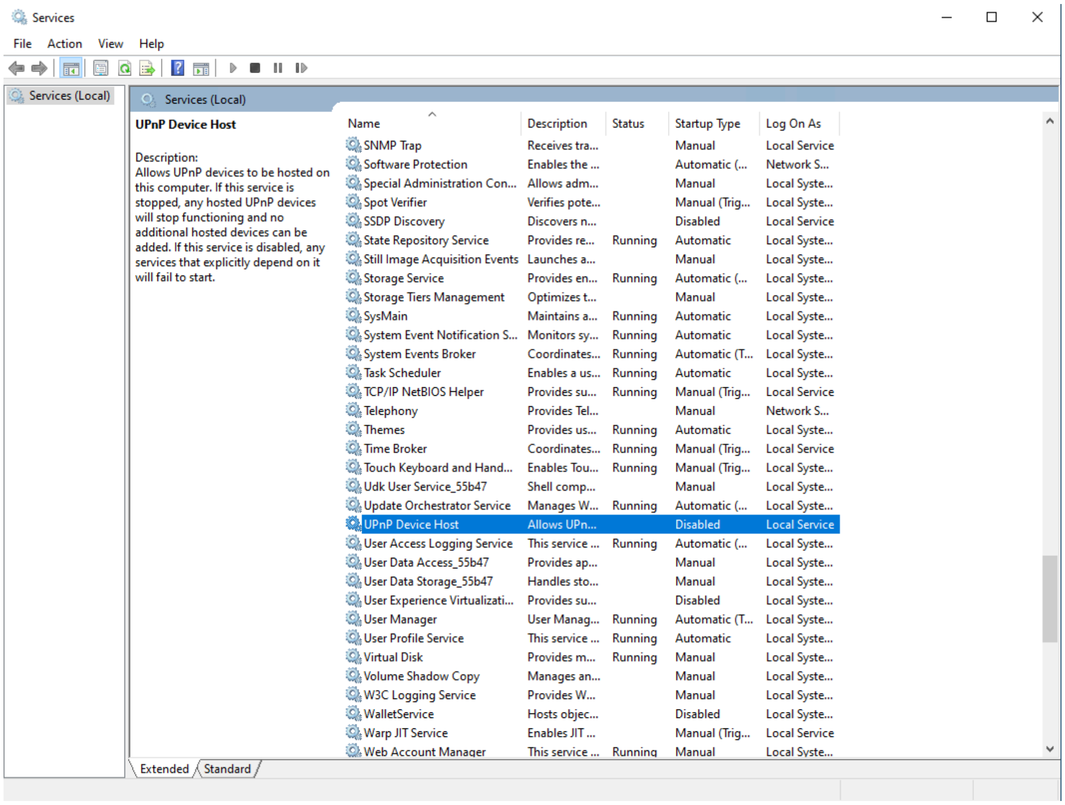
14. Disable FTP, Proxy Services, Telnet, and Universal Plug and Play



SSDP Discovery

Description:
Discovers networked devices and services that use the SSDP discovery protocol, such as UPnP devices. Also announces SSDP devices and services running on the local computer. If this service is stopped, SSDP-based devices will not be discovered. If this service is disabled, any services that explicitly depend on it will fail to start.

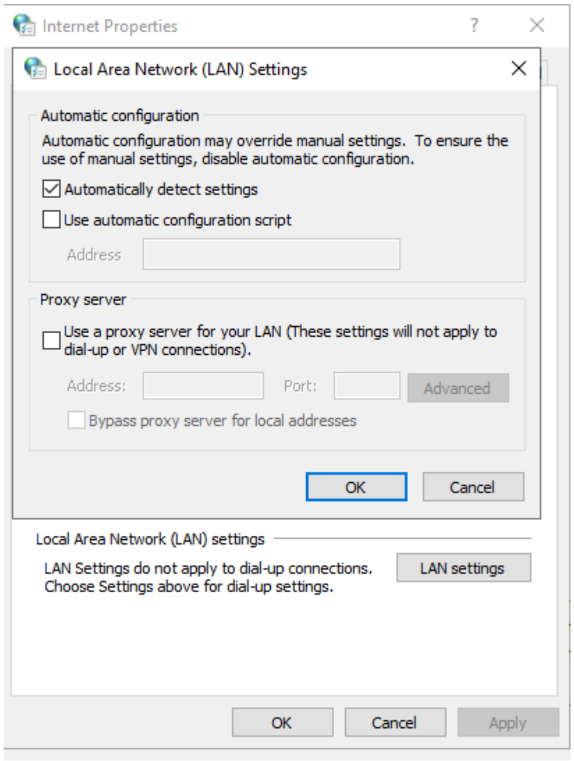
Name	Description	Status	Startup Type	Log On As
Remote Procedure Call (RPC)	The RPCSS s...	Running	Automatic	Network S...
Remote Procedure Call (RP...	In Windows...		Manual	Network S...
Remote Registry	Enables rem...		Automatic (T...	Local Service
Resultant Set of Policy Provi...	Provides a n...		Manual	Local Syste...
Routing and Remote Access	Offers routi...		Disabled	Local Syste...
RPC Endpoint Mapper	Resolves RP...	Running	Automatic	Network S...
Secondary Logon	Enables star...		Manual	Local Syste...
Secure Socket Tunneling Pr...	Provides su...		Manual	Local Service
Security Accounts Manager	The startup ...	Running	Automatic	Local Syste...
Sensor Data Service	Delivers dat...		Disabled	Local Syste...
Sensor Monitoring Service	Monitors va...		Manual (Trig...	Local Service
Sensor Service	A service fo...		Manual (Trig...	Local Syste...
Server	Supports fil...	Running	Automatic (T...	Local Syste...
Shared PC Account Manager	Manages pr...		Disabled	Local Syste...
Shell Hardware Detection	Provides no...	Running	Automatic	Local Syste...
Smart Card	Manages ac...		Manual (Trig...	Local Service
Smart Card Device Enumera...	Creates soft...		Disabled	Local Syste...
Smart Card Removal Policy	Allows the s...		Manual	Local Syste...
SNMP Trap	Receives tra...		Manual	Local Service
Software Protection	Enables the ...		Automatic (...	Network S...
Special Administration Con...	Allows adm...		Manual	Local Syste...
Spot Verifier	Verifies pote...		Manual (Trig...	Local Syste...
SSDP Discovery	Discovers n...		Disabled	Local Service
State Repository Service	Provides re...	Running	Automatic	Local Syste...
Still Image Acquisition Events	Launches a...		Manual	Local Syste...
Storage Service	Provides en...	Running	Automatic (...	Local Syste...
Storage Tiers Management	Optimizes t...		Manual	Local Syste...
SysMain	Maintains a...	Running	Automatic	Local Syste...
System Event Notification S...	Monitors sy...	Running	Automatic	Local Syste...
System Events Broker	Coordinates...	Running	Automatic (T...	Local Syste...
Task Scheduler	Enables a us...	Running	Automatic	Local Syste...
TCP/IP NetBIOS Helper	Provides su...	Running	Manual (Trig...	Local Service
Telephony	Provides Tel...		Manual	Network S...



UPnP Device Host

Description:
Allows UPnP devices to be hosted on this computer. If this service is stopped, any hosted UPnP devices will stop functioning and no additional hosted devices can be added. If this service is disabled, any services that explicitly depend on it will fail to start.

Name	Description	Status	Startup Type	Log On As
SNMP Trap	Receives tra...		Manual	Local Service
Software Protection	Enables the ...		Automatic (...	Network S...
Special Administration Con...	Allows adm...		Manual	Local Syste...
Spot Verifier	Verifies pote...		Manual (Trig...	Local Syste...
SSDP Discovery	Discovers n...		Disabled	Local Service
State Repository Service	Provides re...	Running	Automatic	Local Syste...
Still Image Acquisition Events	Launches a...		Manual	Local Syste...
Storage Service	Provides en...	Running	Automatic (...	Local Syste...
Storage Tiers Management	Optimizes t...		Manual	Local Syste...
SysMain	Maintains a...	Running	Automatic	Local Syste...
System Event Notification S...	Monitors sy...	Running	Automatic	Local Syste...
System Events Broker	Coordinates...	Running	Automatic (T...	Local Syste...
Task Scheduler	Enables a us...	Running	Automatic	Local Syste...
TCP/IP NetBIOS Helper	Provides su...	Running	Manual (Trig...	Local Service
Telephony	Provides Tel...		Manual	Network S...
Themes	Provides us...	Running	Automatic	Local Syste...
Time Broker	Coordinates...	Running	Manual (Trig...	Local Service
Touch Keyboard and Hand...	Enables Tou...	Running	Manual (Trig...	Local Syste...
Udk User Service_55b47	Shell comp...		Manual	Local Syste...
Update Orchestrator Service	Manages W...	Running	Automatic (...	Local Syste...
UPnP Device Host	Allows UPn...		Disabled	Local Service
User Access Logging Service	This service ...	Running	Automatic (...	Local Syste...
User Data Access_55b47	Provides ap...		Manual	Local Syste...
User Data Storage_55b47	Handles sto...		Manual	Local Syste...
User Experience Virtualizati...	Provides su...		Disabled	Local Syste...
User Manager	User Manag...	Running	Automatic (T...	Local Syste...
User Profile Service	This service ...	Running	Automatic	Local Syste...
Virtual Disk	Provides m...	Running	Manual	Local Syste...
Volume Shadow Copy	Manages an...		Manual	Local Syste...
W3C Logging Service	Provides W...		Manual	Local Syste...
WalletService	Hosts objec...		Disabled	Local Syste...
Warp JIT Service	Enables JIT ...		Manual (Trig...	Local Service
Web Account Manager	This service ...	Running	Manual	Local Syste...



Local Area Network (LAN) Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

☑ Automatically detect settings

□ Use automatic configuration script

Address

Proxy server

□ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

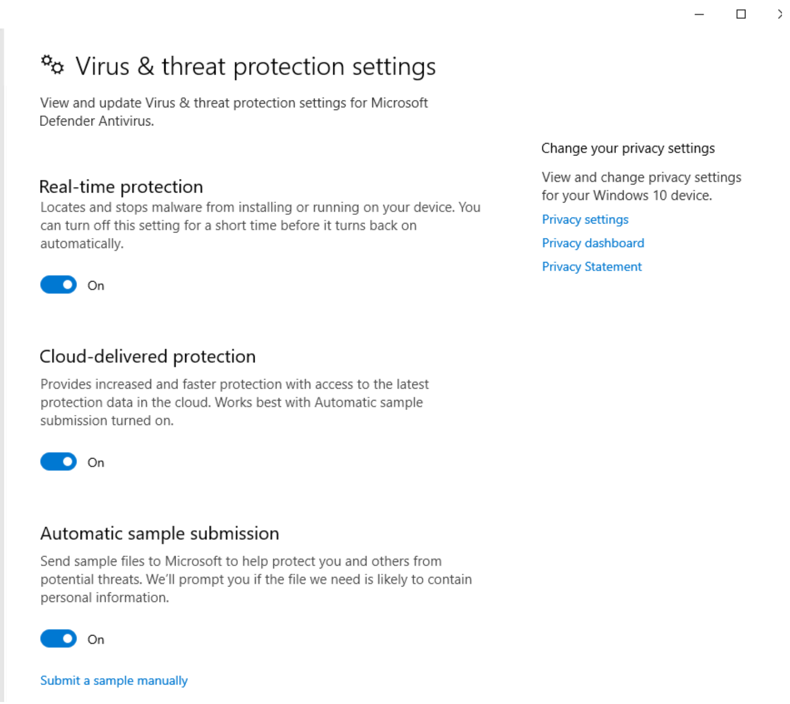
Address: Port:

□ Bypass proxy server for local addresses

Local Area Network (LAN) settings

LAN Settings do not apply to dial-up connections. Choose Settings above for dial-up settings.

15. Windows Defender and Firewall



Virus & threat protection settings

View and update Virus & threat protection settings for Microsoft Defender Antivirus.

Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

● On

Cloud-delivered protection

Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.

● On

Automatic sample submission

Send sample files to Microsoft to help protect you and others from potential threats. We'll prompt you if the file we need is likely to contain personal information.

● On

Submit a sample manually

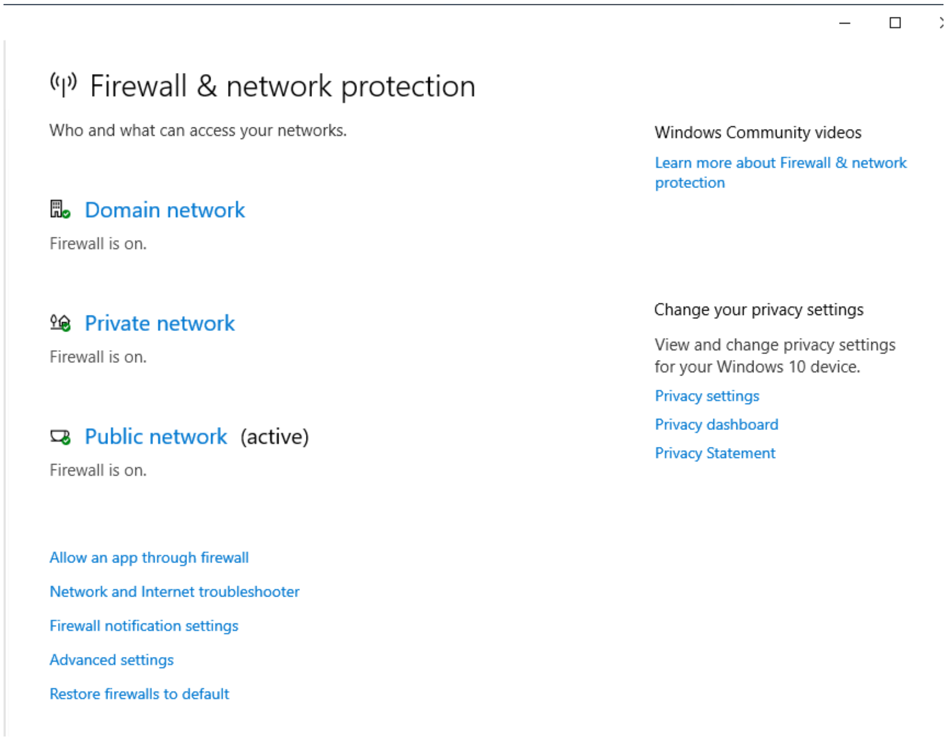
Change your privacy settings

View and change privacy settings for your Windows 10 device.

Privacy settings

Privacy dashboard

Privacy Statement



Firewall & network protection

Who and what can access your networks.

Domain network

Firewall is on.

Private network

Firewall is on.

Public network (active)

Firewall is on.

Allow an app through firewall

Network and Internet troubleshooter

Firewall notification settings

Advanced settings

Restore firewalls to default

Windows Community videos

Learn more about Firewall & network protection

Change your privacy settings

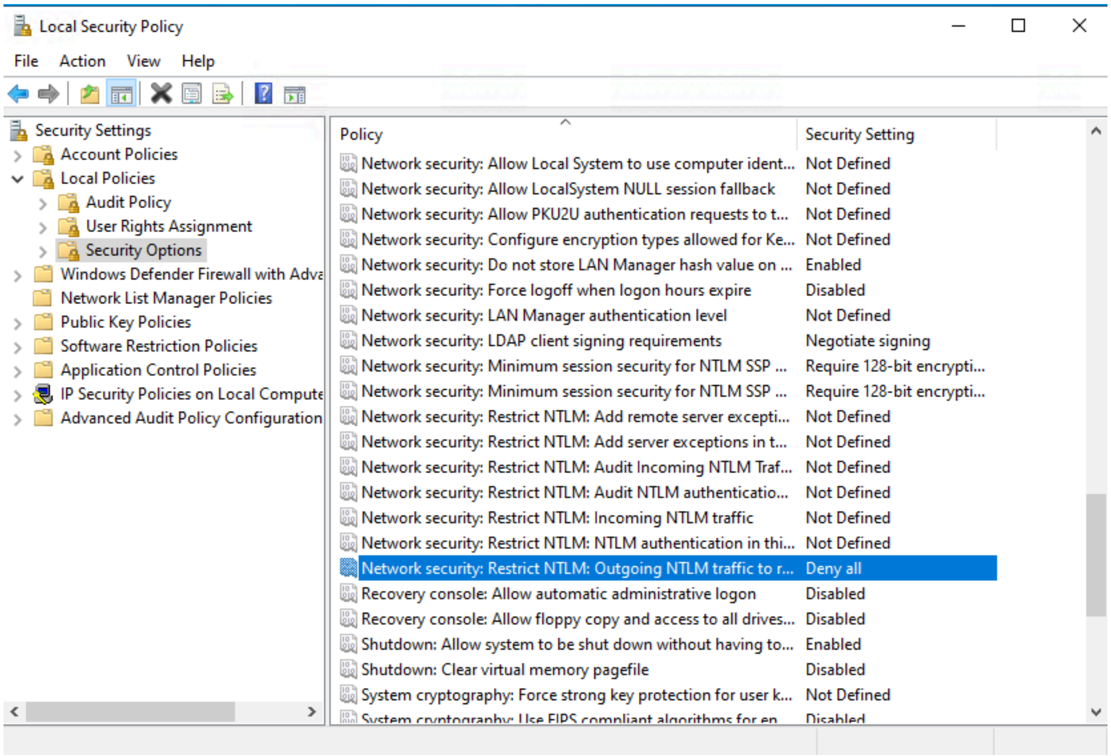
View and change privacy settings for your Windows 10 device.

Privacy settings

Privacy dashboard

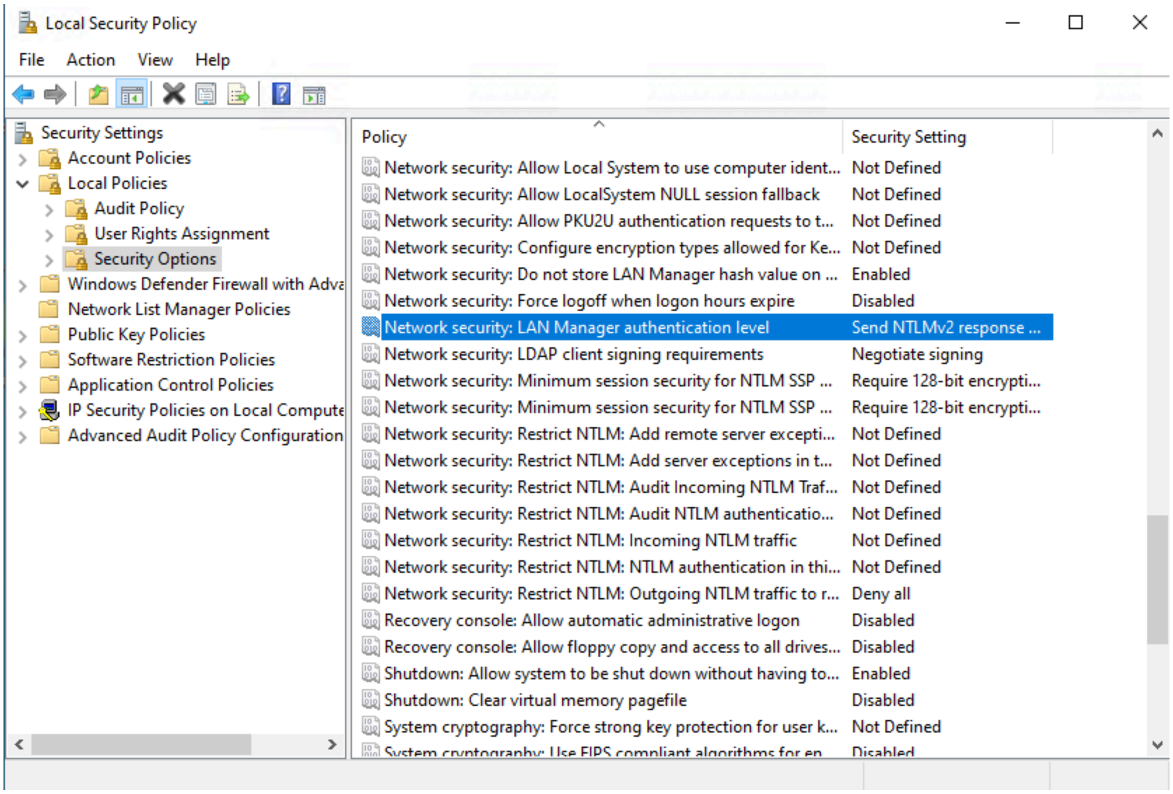
Privacy Statement

16. Disable NTLM, PS 2.0, SMB 1.0

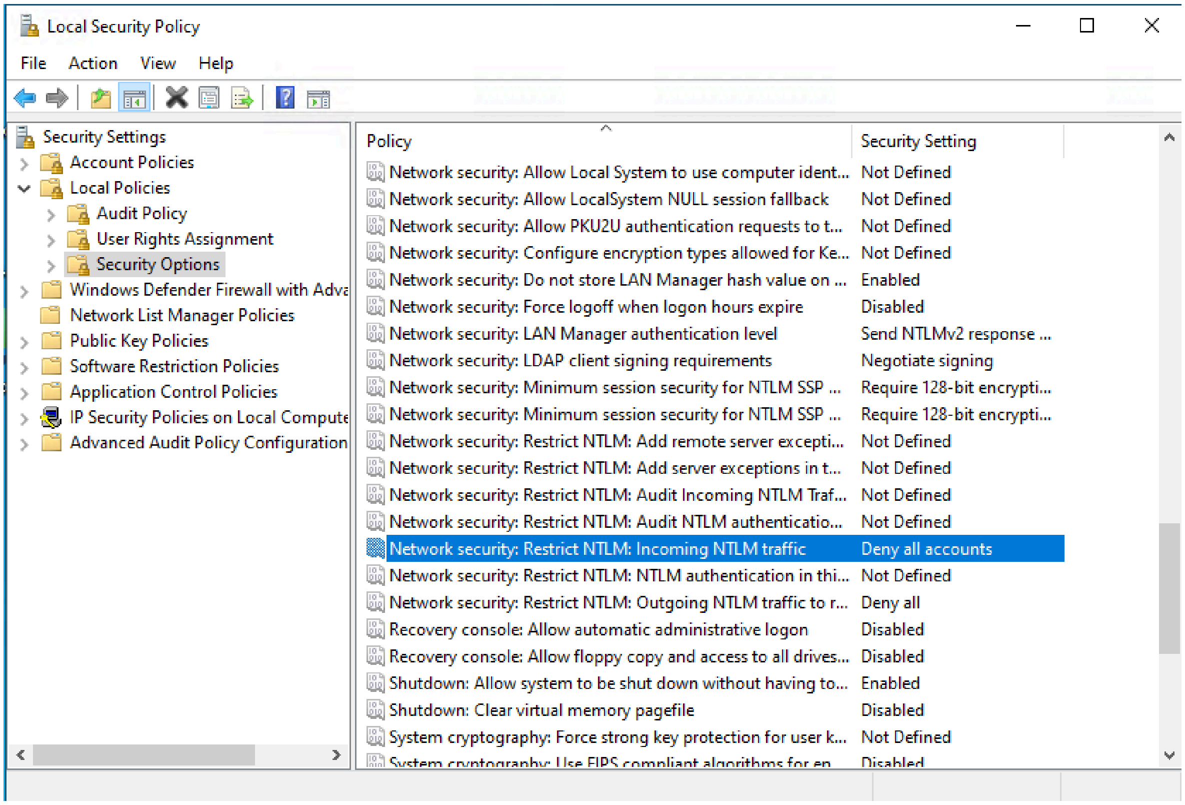


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

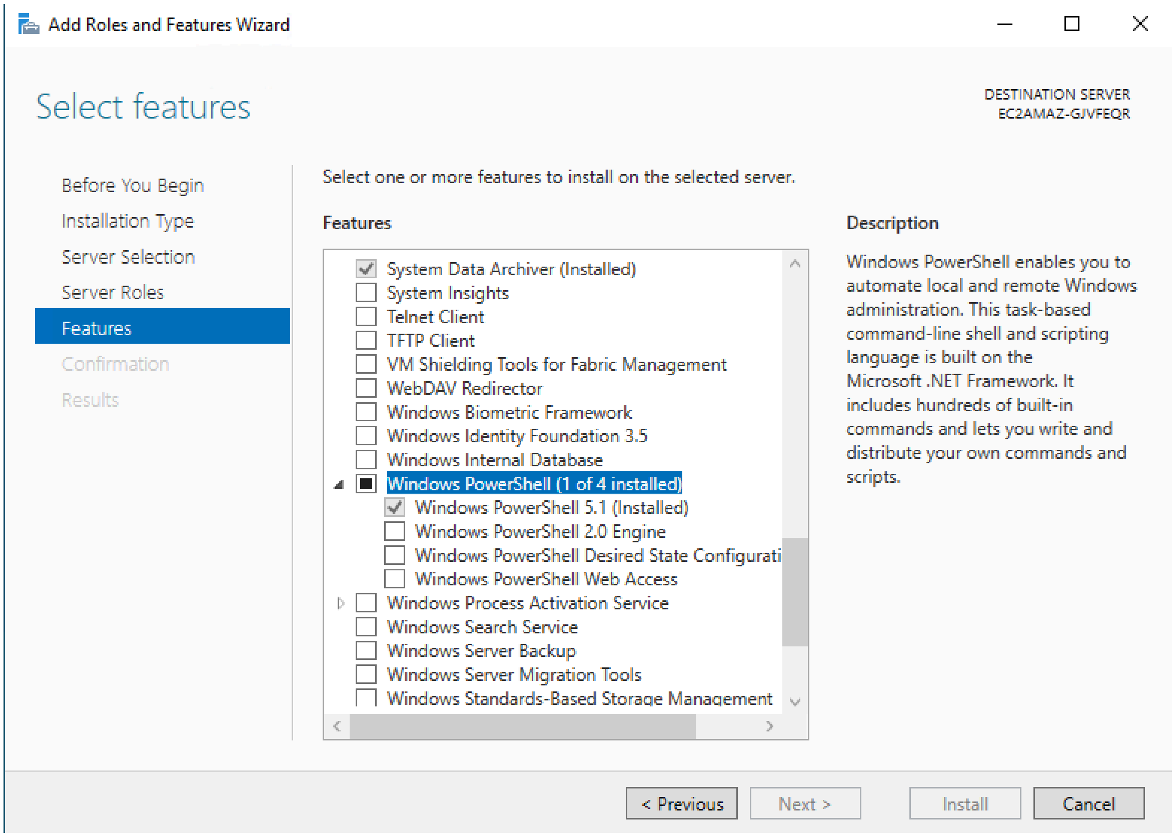
Policy	Security Setting
Network security: Allow Local System to use computer ident...	Not Defined
Network security: Allow LocalSystem NULL session fallback	Not Defined
Network security: Allow PKU2U authentication requests to t...	Not Defined
Network security: Configure encryption types allowed for Ke...	Not Defined
Network security: Do not store LAN Manager hash value on ...	Enabled
Network security: Force logoff when logon hours expire	Disabled
Network security: LAN Manager authentication level	Not Defined
Network security: LDAP client signing requirements	Negotiate signing
Network security: Minimum session security for NTLM SSP ...	Require 128-bit encrypti...
Network security: Minimum session security for NTLM SSP ...	Require 128-bit encrypti...
Network security: Restrict NTLM: Add remote server excepti...	Not Defined
Network security: Restrict NTLM: Add server exceptions in t...	Not Defined
Network security: Restrict NTLM: Audit Incoming NTLM Traf...	Not Defined
Network security: Restrict NTLM: Audit NTLM authenticatio...	Not Defined
Network security: Restrict NTLM: Incoming NTLM traffic	Not Defined
Network security: Restrict NTLM: NTLM authentication in thi...	Not Defined
Network security: Restrict NTLM: Outgoing NTLM traffic to r...	Deny all
Recovery console: Allow automatic administrative logon	Disabled
Recovery console: Allow floppy copy and access to all drives...	Disabled
Shutdown: Allow system to be shut down without having to...	Enabled
Shutdown: Clear virtual memory pagefile	Disabled
System cryptography: Force strong key protection for user k...	Not Defined
System cryptography: Use FIPS compliant algorithms for en...	Disabled


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Policy	Security Setting
Network security: Allow Local System to use computer ident...	Not Defined
Network security: Allow LocalSystem NULL session fallback	Not Defined
Network security: Allow PKU2U authentication requests to t...	Not Defined
Network security: Configure encryption types allowed for Ke...	Not Defined
Network security: Do not store LAN Manager hash value on ...	Enabled
Network security: Force logoff when logon hours expire	Disabled
Network security: LAN Manager authentication level	Send NTLMv2 response ...
Network security: LDAP client signing requirements	Negotiate signing
Network security: Minimum session security for NTLM SSP ...	Require 128-bit encrypti...
Network security: Minimum session security for NTLM SSP ...	Require 128-bit encrypti...
Network security: Restrict NTLM: Add remote server excepti...	Not Defined
Network security: Restrict NTLM: Add server exceptions in t...	Not Defined
Network security: Restrict NTLM: Audit Incoming NTLM Traf...	Not Defined
Network security: Restrict NTLM: Audit NTLM authenticatio...	Not Defined
Network security: Restrict NTLM: Incoming NTLM traffic	Not Defined
Network security: Restrict NTLM: NTLM authentication in thi...	Not Defined
Network security: Restrict NTLM: Outgoing NTLM traffic to r...	Deny all
Recovery console: Allow automatic administrative logon	Disabled
Recovery console: Allow floppy copy and access to all drives...	Disabled
Shutdown: Allow system to be shut down without having to...	Enabled
Shutdown: Clear virtual memory pagefile	Disabled
System cryptography: Force strong key protection for user k...	Not Defined
System cryptography: Use FIPS compliant algorithms for en...	Disabled


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Policy	Security Setting
Network security: Allow Local System to use computer ident...	Not Defined
Network security: Allow LocalSystem NULL session fallback	Not Defined
Network security: Allow PKU2U authentication requests to t...	Not Defined
Network security: Configure encryption types allowed for Ke...	Not Defined
Network security: Do not store LAN Manager hash value on ...	Enabled
Network security: Force logoff when logon hours expire	Disabled
Network security: LAN Manager authentication level	Send NTLMv2 response ...
Network security: LDAP client signing requirements	Negotiate signing
Network security: Minimum session security for NTLM SSP ...	Require 128-bit encrypti...
Network security: Minimum session security for NTLM SSP ...	Require 128-bit encrypti...
Network security: Restrict NTLM: Add remote server excepti...	Not Defined
Network security: Restrict NTLM: Add server exceptions in t...	Not Defined
Network security: Restrict NTLM: Audit Incoming NTLM Traf...	Not Defined
Network security: Restrict NTLM: Audit NTLM authenticatio...	Not Defined
Network security: Restrict NTLM: Incoming NTLM traffic	Deny all accounts
Network security: Restrict NTLM: NTLM authentication in thi...	Not Defined
Network security: Restrict NTLM: Outgoing NTLM traffic to r...	Deny all
Recovery console: Allow automatic administrative logon	Disabled
Recovery console: Allow floppy copy and access to all drives...	Disabled
Shutdown: Allow system to be shut down without having to...	Enabled
Shutdown: Clear virtual memory pagefile	Disabled
System cryptography: Force strong key protection for user k...	Not Defined
System cryptography: Use FIPS compliant algorithms for en...	Disabled



Select features

DESTINATION SERVER
EC2AMAZ-GJVFEQR

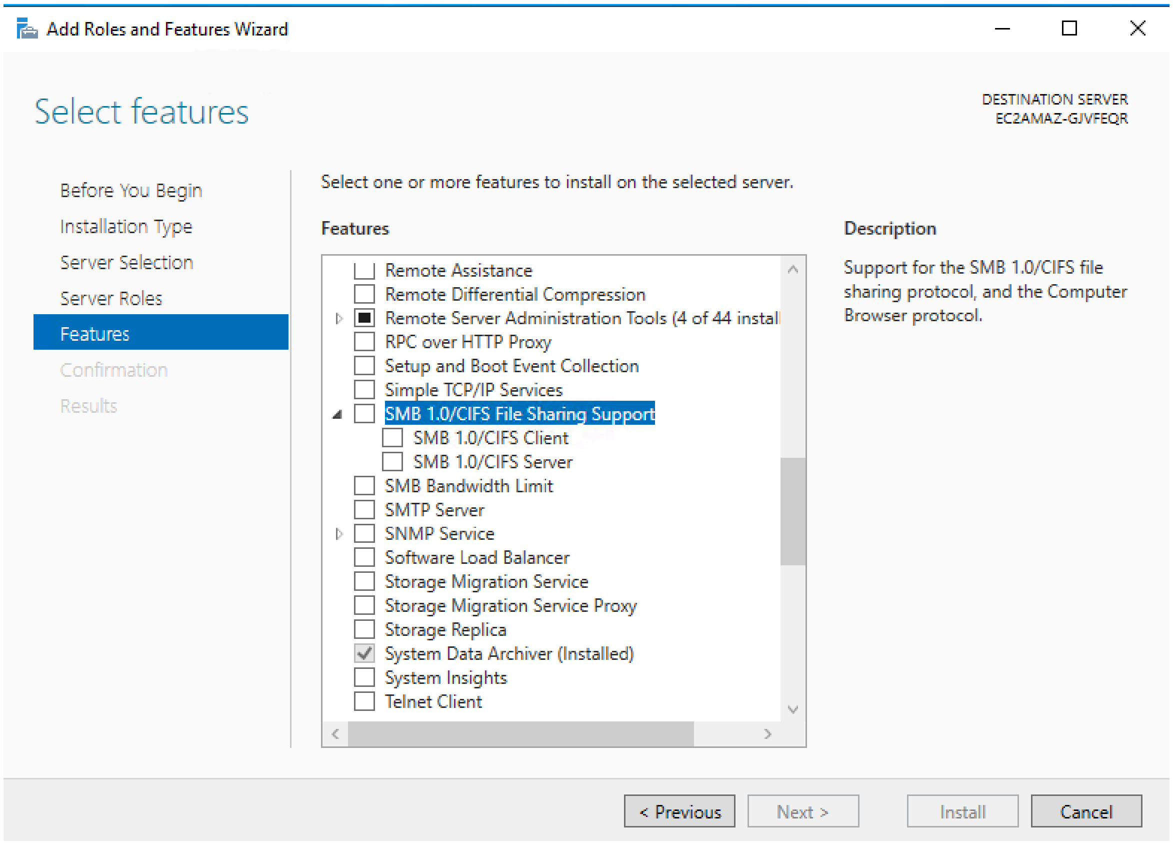
Select one or more features to install on the selected server.

Features

- ☑ System Data Archiver (Installed)
- □ System Insights
- □ Telnet Client
- □ TFTP Client
- □ VM Shielding Tools for Fabric Management
- □ WebDAV Redirector
- □ Windows Biometric Framework
- □ Windows Identity Foundation 3.5
- □ Windows Internal Database
- ■ Windows PowerShell (1 of 4 installed)
  - ☑ Windows PowerShell 5.1 (Installed)
  - □ Windows PowerShell 2.0 Engine
  - □ Windows PowerShell Desired State Configurati
  - □ Windows PowerShell Web Access
- □ Windows Process Activation Service
- □ Windows Search Service
- □ Windows Server Backup
- □ Windows Server Migration Tools
- □ Windows Standards-Based Storage Management

Description

Windows PowerShell enables you to automate local and remote Windows administration. This task-based command-line shell and scripting language is built on the Microsoft .NET Framework. It includes hundreds of built-in commands and lets you write and distribute your own commands and scripts.



Select features

DESTINATION SERVER
EC2AMAZ-GJVFEQR

Select one or more features to install on the selected server.

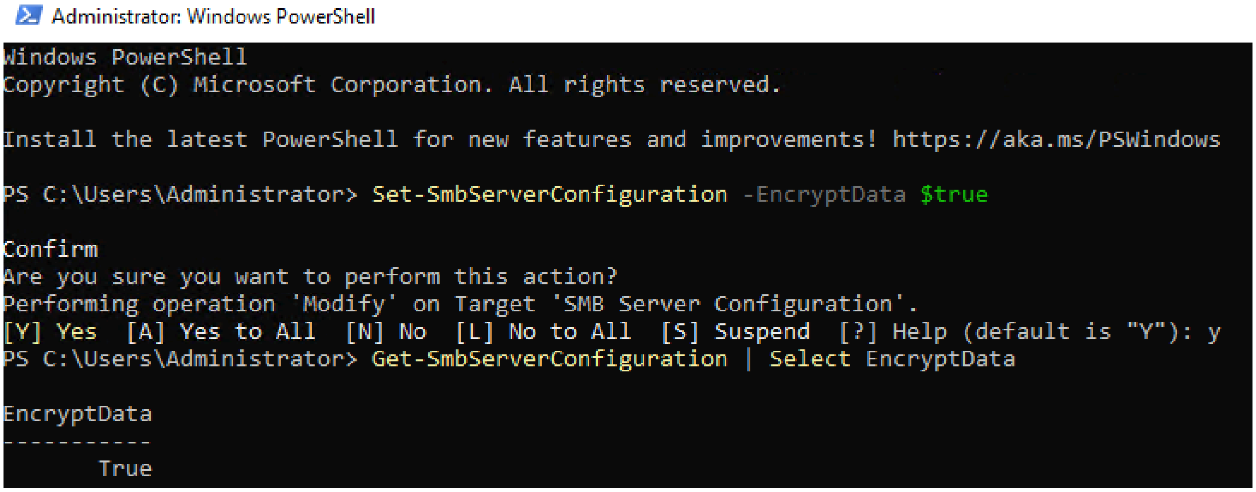
Features

- □ Remote Assistance
- □ Remote Differential Compression
- ■ Remote Server Administration Tools (4 of 44 instal
- □ RPC over HTTP Proxy
- □ Setup and Boot Event Collection
- □ Simple TCP/IP Services
- □ SMB 1.0/CIFS File Sharing Support
  - □ SMB 1.0/CIFS Client
  - □ SMB 1.0/CIFS Server
- □ SMB Bandwidth Limit
- □ SMTP Server
- □ SNMP Service
- □ Software Load Balancer
- □ Storage Migration Service
- □ Storage Migration Service Proxy
- □ Storage Replica
- ☑ System Data Archiver (Installed)
- □ System Insights
- □ Telnet Client

Description

Support for the SMB 1.0/CIFS file sharing protocol, and the Computer Browser protocol.

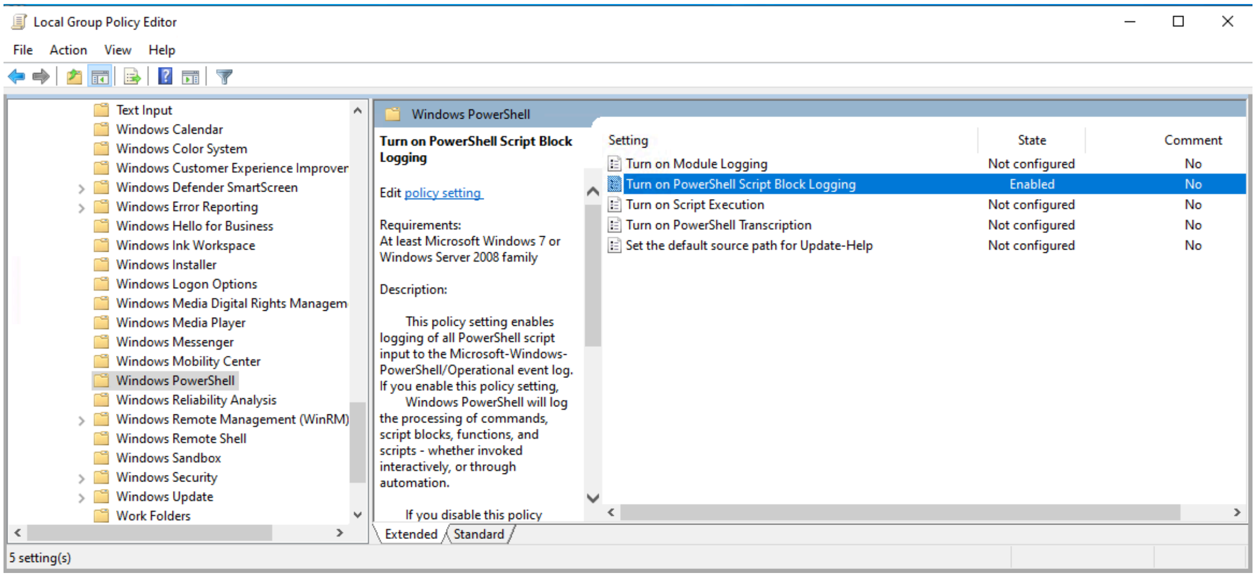
17. Enable SMB Encryption



Administrator: Windows PowerShell

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Administrator> Set-SmbServerConfiguration -EncryptData $true

Confirm
Are you sure you want to perform this action?
Performing operation 'Modify' on Target 'SMB Server Configuration'.
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): y
PS C:\Users\Administrator> Get-SmbServerConfiguration | Select EncryptData

EncryptData
-----------
       True
```

18. Enable PS Logging and Disable PS 2.0



Turn on PowerShell Script Block Logging

Edit policy setting

Requirements:
At least Microsoft Windows 7 or Windows Server 2008 family

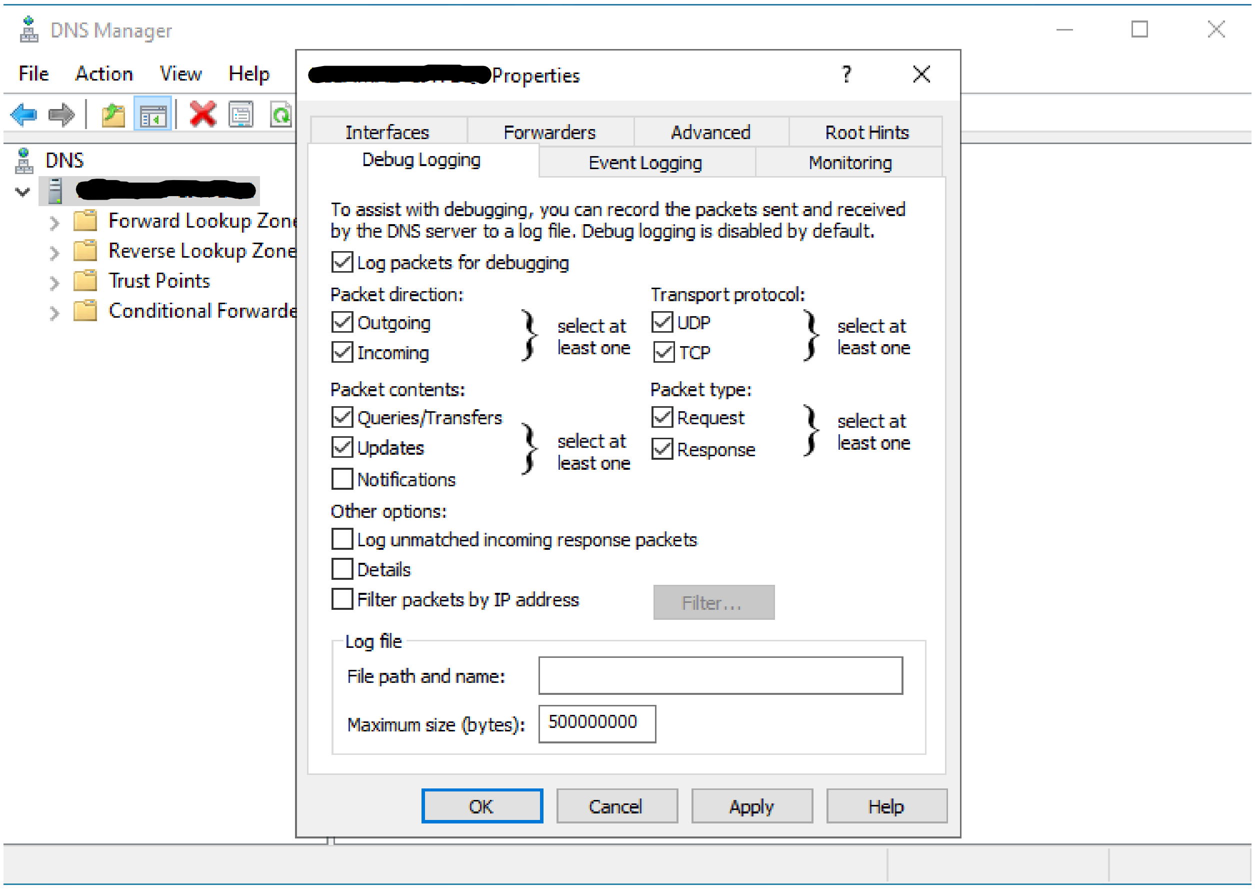
Description:

This policy setting enables logging of all PowerShell script input to the Microsoft-Windows-PowerShell/Operational event log. If you enable this policy setting, Windows PowerShell will log the processing of commands, script blocks, functions, and scripts - whether invoked interactively, or through automation.

If you disable this policy

Setting	State	Comment
Turn on Module Logging	Not configured	No
Turn on PowerShell Script Block Logging	Enabled	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

19. Monitor DNS Logs



[redacted] Properties

To assist with debugging, you can record the packets sent and received by the DNS server to a log file. Debug logging is disabled by default.

☑ Log packets for debugging

Packet direction:
☑ Outgoing
☑ Incoming
} select at least one

Transport protocol:
☑ UDP
☑ TCP
} select at least one

Packet contents:
☑ Queries/Transfers
☑ Updates
□ Notifications
} select at least one

Packet type:
☑ Request
☑ Response
} select at least one

Other options:
□ Log unmatched incoming response packets
□ Details
□ Filter packets by IP address

Log file
File path and name:
Maximum size (bytes): 500000000

1. The system becomes protected from unintended modifications through the implementation of specific user accounts which receive restricted permissions.

2. The SID and integrity level combination enables users to verify their privileges and maintain their operations within their designated security limits.

3. The PowerShell integrity level check verifies that running processes maintain their correct security restrictions while preventing them from accessing elevated permissions.

4. The Guest account becomes unavailable to attackers because disabling it eliminates their default entry point which enhances server access control.

5. The implementation of strong password policies requires users to generate complex passwords which they must update frequently to minimize password-based security threats.

6. The system logs both successful and failed user events through audit success and failure events which enables real-time detection of suspicious activities and unauthorized access attempts.

7. The combination of Credential Guard and ATP protects sensitive login credentials and identifies sophisticated threats to prevent credential theft attacks.

8. The automated update system of the server maintains continuous access to security patches which minimizes the number of system vulnerabilities caused by outdated software.

9. The restriction of folder permissions ensures that authorized personnel maintain exclusive access to sensitive files which protects against unauthorized data access and modification.

10. The creation of a local user account with defined permissions enables better access control because each user receives only the necessary permissions for their work tasks.

11. The modification of UAC settings requires users to confirm important system changes which stops both malware and unauthorized users from making unauthorized system modifications.

12. Users cannot modify essential system settings or install dangerous software because the system blocks their access to Control Panel and Command Prompt and software installation functions.

13. The system becomes more secure because disabling NetLM hash value storage makes it impossible for attackers to retrieve or crack passwords when the system gets compromised.

14. The removal of FTP and Telnet and Proxy and UPnP services from the system eliminates potential entry points which attackers could use to penetrate the server.

15. The system becomes more secure through Windows Defender and Firewall which defend against malware and block unauthorized network traffic.

16. The removal of outdated communication protocols NTLM and PS 2.0 and SMB 1.0 prevents attackers from using old security weaknesses to exploit the system.

17. SMB encryption activation protects data transfers between systems because it prevents unauthorized parties from intercepting or modifying sensitive information.

18. PowerShell logging becomes enabled for auditing purposes while PS 2.0 gets disabled because it lacks modern security features that the current version provides.

19. The monitoring of DNS logs enables organizations to detect abnormal network traffic and identify malicious domain queries which allows for swift security response actions.