UNIVERSITY OF PIRAEUS

School of Information and Communication Technologies

Department of Informatics

Thesis

Thesis Title: Τίτλος Διατριβής:	**CIS Microsoft Windows Server 2019 compliance** Συμμόρφωση των Microsoft Windows Server 2019 με το CIS
Student's name-surname:	**Ioannis Koropiotis**
Father's name:	**Athanasios**
Student's ID No:	**Π15057**
Supervisor:	**Konstantinos Patsakis, Associate Professor**

2024-09

Copyright ©

Εκφώνηση της άσκησης

On a Windows Server 2019 Hardening will be applied based on CIS Benchmark Documents. Also remediation of vulnerabilities will take place in order to protect the system from Cyber Security Threats

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

1 Introduction 16

2 Account Policies 17

2.1 17

2.1.1 Ensure 'Enforce password history' is set to '24 or more password(s)' 17
2.1.2 Ensure 'Maximum password age' is set to '365 or fewer days, but not 0' 18
2.1.3 Ensure 'Minimum password age' is set to '1 or more day(s)' 19
2.1.4 Ensure 'Minimum password length' is set to '14 or more character(s)' 20
2.1.5 Ensure 'Password must meet complexity requirements' is set to 'Enabled' 21
2.1.6 Ensure 'Store passwords using reversible encryption' is set to 'Disabled' 22

2.2 Account Lockout Policy 23

2.2.1 Ensure 'Account lockout duration' is set to '15 or more minute(s)' 23
2.2.2 Ensure 'Account lockout threshold' is set to '5 or fewer invalid logon attempt(s), but not 0' 24
2.2.3 Ensure 'Allow Administrator account lockout' is set to 'Enabled' 25
2.2.4 Ensure 'Reset account lockout counter after' is set to '15 or more minute(s)' 26

3 Local Policies 27

3.1 User Rights Assignment 27

3.1.1 Ensure 'Access Credential Manager as a trusted caller' is set to 'No One' 27
3.1.2 Ensure 'Access this computer from the network' is set to 'Administrators, Authenticated Users, ENTERPRISE DOMAIN CONTROLLERS' 28
3.1.3 Ensure Act as part of the operating system' is set to 'No One' 29
3.1.4 Ensure 'Add workstations to domain' is set to 'Administrators' 30
3.1.5 Ensure Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE' 31
3.1.6 Ensure 'Allow log on locally' is set to 'Administrators' 32
3.1.7 Ensure 'Allow log on through Remote Desktop Services' is set to 'Administrators' ... 33
3.1.8 Ensure Back up files and directories' is set to 'Administrators' 34
3.1.9 Ensure 'Change the system time' is set to 'Administrators, LOCAL SERVICE' 35
3.1.10 Ensure 'Change the time zone' is set to 'Administrators, LOCAL SERVICE' 36
3.1.11 Ensure 'Create a pagefile' is set to 'Administrators' 37
3.1.12 Ensure 'Create a token object' is set to 'No One' 38
3.1.13 Ensure 'Create global objects' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' 39
3.1.14 Ensure Create permanent shared objects' is set to 'No One' 40
3.1.15 Ensure ‘Create symbolic links' is set to 'Administrators' 41
3.1.16 Ensure 'Debug programs' is set to 'Administrators' 42
3.1.17 Ensure ‘Deny access to this computer from the network' to include 'Guests' 43
3.1.18 Ensure 'Deny log on as a batch job' to include 'Guests' 44
3.1.19 Ensure 'Deny log on as a service' to include 'Guests' 45
3.1.20 Ensure 'Deny log on locally' to include 'Guests' 46
3.1.21 Ensure 'Deny log on through Remote Desktop Services' to include 'Guests' 47
3.1.22 Ensure 'Enable computer and user accounts to be trusted for delegation' is set to 'Administrators' 48

3.1.23 Ensure 'Force shutdown from a remote system' is set to 'Administrators' 49
3.1.24 Ensure 'Generate security audits' is set to 'LOCAL SERVICE, NETWORK SERVICE' 50
3.1.25 Ensure 'Impersonate a client after authentication' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' 51
3.1.26 Ensure 'Increase scheduling priority' is set to 'Administrators, Window Manager\Window Manager Group' 52
3.1.27 Ensure 'Load and unload device drivers' is set to 'Administrators' 53
3.1.28 Ensure 'Lock pages in memory' is set to 'No One' 54
3.1.29 Ensure 'Log on as a batch job' is set to 'Administrators' 55
3.1.30 Ensure 'Manage auditing and security log' is set to 'Administrators' 56
3.1.31 Ensure 'Modify an object label' is set to 'No One' 57
3.1.32 Ensure 'Modify firmware environment values' is set to 'Administrators' 58
3.1.33 Ensure 'Perform volume maintenance tasks' is set to 'Administrators' 59
3.1.34 Ensure 'Profile single process' is set to 'Administrators' 60
3.1.35 Ensure 'Profile system performance' is set to 'Administrators, NT SERVICE\WdiServiceHost' 61
3.1.36 Ensure 'Replace a process level token' is set to 'LOCAL SERVICE, NETWORK SERVICE' 62
3.1.37 Ensure 'Restore files and directories' is set to 'Administrators' 63
3.1.38 Ensure 'Shut down the system' is set to 'Administrators' 64
3.1.39 Ensure 'Synchronize directory service data' is set to 'No One' 65
3.1.40 Ensure 'Take ownership of files or other objects' is set to 'Administrators' 66
3.2 Security Options 67
3.2.1 Accounts 67
3.2.1.1 Ensure 'Accounts: Block Microsoft accounts' is set to 'Users can't add or log on with Microsoft accounts' 67
3.2.1.2 Ensure 'Accounts: Guest account status' is set to 'Disabled' 68
3.2.1.3 Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled' 69
3.2.1.4 Configure 'Accounts: Rename administrator account' 70
3.2.1.5 Configure 'Accounts: Rename guest account' 71
3.2.2 Audit 72
3.2.2.1 Ensure 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' is set to 'Enabled' 72
3.2.2.2 Ensure 'Audit: Shut down system immediately if unable to log security audits' is set to 'Disabled' 73
3.2.3 Devices 74
3.2.3.1 Ensure 'Devices: Prevent users from installing printer drivers' is set to 'Enabled' 74
3.2.4 Interactive logon 75
3.2.4.1 Ensure 'Interactive logon: Do not require CTRL+ALT+DEL' is set to 'Disabled' 75
3.2.4.2 Ensure 'Interactive logon: Don't display last signed-in' is set to 'Enabled' 76
3.2.4.3 Ensure 'Interactive logon: Machine inactivity limit' is set to '900 or fewer second(s), but not 0' 77
3.2.4.4 Configure 'Interactive logon: Message text for users attempting to log on' 78
3.2.4.5 Configure 'Interactive logon: Message title for users attempting to log on' 79

3.2.4.6 Ensure 'Interactive logon: Prompt user to change password before expiration' is set to 'between 5 and 14 days' 80
3.2.4.7 Ensure 'Interactive logon: Require Domain Controller Authentication to unlock workstation' is set to 'Enabled' 81
3.2.4.8 Ensure 'Interactive logon: Require Domain Controller Authentication to unlock workstation' is set to 'Enabled' 82
3.2.5 Microsoft network client 83
3.2.5.1 Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled' 83
3.2.5.2 Ensure 'Microsoft network client: Digitally sign communications (if server agrees)' is set to 'Enabled' 84
3.2.5.3 Ensure 'Microsoft network client: Send unencrypted password to third-party SMB servers' is set to 'Disabled' 85
3.2.6 Microsoft network server 86
3.2.6.1 Ensure 'Microsoft network server: Amount of idle time required before suspending session' is set to '15 or fewer minute(s)' 86
3.2.6.2 Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled' 87
3.2.6.3 Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled' 88
3.2.6.4 Ensure 'Microsoft network server: Disconnect clients when logon hours expire' is set to 'Enabled' 89
3.2.6.5 Ensure 'Microsoft network server: Server SPN target name validation level' is set to 'Accept if provided by client' or higher 90
3.2.7 Network access 91
3.2.7.1 Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled' 91
3.2.7.2 Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts' is set to 'Enabled' 92
3.2.7.3 Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled' 93
3.2.7.4 Ensure 'Network access: Do not allow storage of passwords and credentials for network authentication' is set to 'Enabled' 94
3.2.7.5 Ensure 'Network access: Let Everyone permissions apply to anonymous users' is set to 'Disabled' 95
3.2.7.6 Configure 'Network access: Named Pipes that can be accessed anonymously' .. 96
3.2.7.7 Configure 'Network access: Remotely accessible registry paths' is configured ... 97
3.2.7.8 Configure 'Network access: Remotely accessible registry paths and sub-paths' is configured 98
3.2.7.9 Ensure 'Network access: Restrict anonymous access to Named Pipes and Shares' is set to 'Enabled' 99
3.2.7.10 Ensure 'Network access: Restrict clients allowed to make remote calls to SAM' is set to 'Administrators: Remote Access: Allow' 100
3.2.7.11 Ensure 'Network access: Shares that can be accessed anonymously' is set to 'None' 101
3.2.7.12 Ensure 'Network access: Sharing and security model for local accounts' is set to 'Classic - local users authenticate as themselves' 102

3.2.8 Network security 103
3.2.8.1 Ensure 'Network security: Allow Local System to use computer identity for NTLM' is set to 'Enabled' 103
3.2.8.2 Ensure 'Network security: Allow LocalSystem NULL session fallback' is set to 'Disabled' 104
3.2.8.3 Ensure 'Network Security: Allow PKU2U authentication requests to this computer to use online identities' is set to 'Disabled' 105
3.2.8.4 Ensure 'Network security: Configure encryption types allowed for Kerberos' is set to 'AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types' 106
3.2.8.5 Ensure 'Network security: Do not store LAN Manager hash value on next password change' is set to 'Enabled' 107
3.2.8.6 Ensure 'Network security: Force logoff when logon hours expire' is set to 'Enabled' 108
3.2.8.7 Ensure 'Network security: LAN Manager authentication level' is set to 'Send NTLMv2 response only. Refuse LM & NTLM' 109
3.2.8.8 Ensure 'Network security: LDAP client signing requirements' is set to 'Negotiate signing' or higher 110
3.2.8.9 Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' is set to 'Require NTLMv2 session security, Require 128-bit encryption' 111
3.2.8.10 Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require NTLMv2 session security, Require 128-bit encryption' 112
3.2.8.11 Ensure 'Network security: Restrict NTLM: Audit Incoming NTLM Traffic' is set to 'Enable auditing for all accounts' 113
3.2.8.12 Ensure 'Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers' is set to 'Audit all' or higher 114
3.2.9 Shutdown 115
3.2.9.1 Ensure 'Shutdown: Allow system to be shut down without having to log on' is set to 'Disabled' 115
3.2.10 System objects 116
3.2.10.1 Ensure 'System objects: Require case insensitivity for non-Windows subsystems' is set to 'Enabled' 116
3.2.10.2 Ensure 'System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)' is set to 'Enabled' 117
3.2.11 User Account Control 118
3.2.11.1 Ensure 'User Account Control: Admin Approval Mode for the Built-in Administrator account' is set to 'Enabled' 118
3.2.11.2 Ensure 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' is set to 'Prompt for consent on the secure desktop' or higher 119
3.2.11.3 Ensure 'User Account Control: Behavior of the elevation prompt for standard users' is set to 'Automatically deny elevation requests' 120
3.2.11.4 Ensure 'User Account Control: Detect application installations and prompt for elevation' is set to 'Enabled' 121
3.2.11.5 Ensure 'User Account Control: Only elevate UIAccess applications that are installed in secure locations' is set to 'Enabled' 122

3.2.11.6 Ensure 'User Account Control: Run all administrators in Admin Approval Mode' is set to 'Enabled' 123
3.2.11.7 Ensure 'User Account Control: Switch to the secure desktop when prompting for elevation' is set to 'Enabled' 124
3.2.11.8 Ensure 'User Account Control: Virtualize file and registry write failures to per-user locations' is set to 'Enabled' 125
4 System Services 126
4.1 Ensure 'Print Spooler (Spooler)' is set to 'Disabled' 126
5 Windows Defender Firewall with Advanced Security 127
5.1 Private Profile 127
5.1.1 Ensure 'Windows Firewall: Private: Firewall state' is set to 'On (recommended)' ... 127
5.1.2 Ensure 'Windows Firewall: Private: Inbound connections' is set to 'Block (default)' 128
5.1.3 Ensure 'Windows Firewall: Private: Outbound connections' is set to 'Allow (default)' 129
5.1.4 Ensure 'Windows Firewall: Private: Settings: Display a notification' is set to 'No' ... 130
5.1.5 Ensure 'Windows Firewall: Private: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\privatefw.log' 131
5.1.6 Ensure 'Windows Firewall: Private: Logging: Size limit (KB)' is set to '16,384 KB or greater' 132
5.1.7 Ensure 'Windows Firewall: Private: Logging: Log dropped packets' is set to 'Yes' ... 133
5.1.8 Ensure 'Windows Firewall: Private: Logging: Log successful connections' is set to 'Yes' 134
5.2 Private Profile 135
5.2.1 Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)' 135
5.2.2 Ensure 'Windows Firewall: Public: Inbound connections' is set to 'Block (default)' . 136
5.2.3 Ensure 'Windows Firewall: Public: Outbound connections' is set to 'Allow (default)' 137
5.2.4 Ensure 'Windows Firewall: Public: Settings: Display a notification' is set to 'No' 138
5.2.5 Ensure 'Windows Firewall: Public: Settings: Apply local firewall rules' is set to 'No' 139
5.2.6 Ensure 'Windows Firewall: Public: Settings: Apply local connection security rules' is set to 'No' 140
5.2.7 Ensure 'Windows Firewall: Public: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\publicfw.log' 141
5.2.8 Ensure 'Windows Firewall: Public: Logging: Size limit (KB)' is set to '16,384 KB or greater' 142
5.2.9 Ensure 'Windows Firewall: Public: Logging: Log dropped packets' is set to 'Yes' 143
5.2.10 Ensure 'Windows Firewall: Public: Logging: Log successful connections' is set to 'Yes' 144
6 Advanced Audit Policy Configuration 145
6.1 Account Logon 145
6.1.1 Ensure 'Audit Credential Validation' is set to 'Success and Failure' 145
6.1.2 Ensure 'Audit Kerberos Authentication Service' is set to 'Success and Failure' 146
6.1.3 Ensure 'Audit Kerberos Service Ticket Operations' is set to 'Success and Failure' ... 147
6.2 Account Management 148

6.2.1 Ensure 'Audit Application Group Management' is set to 'Success and Failure' 148
6.2.2 Ensure 'Audit Computer Account Management' is set to include 'Success' 149
6.2.3 Ensure 'Audit Distribution Group Management' is set to include 'Success' 150
6.2.4 Ensure 'Audit Other Account Management Events' is set to include 'Success' 151
6.2.5 Ensure 'Audit Security Group Management' is set to include 'Success' 152
6.2.6 Ensure 'Audit User Account Management' is set to 'Success and Failure' 153
6.3 Detailed Tracking 154
6.3.1 Ensure 'Audit PNP Activity' is set to include 'Success' 154
6.3.2 Ensure 'Audit Process Creation' is set to include 'Success' 155
6.4 DS Access 156
6.4.1 Ensure 'Audit Directory Service Access' is set to include 'Failure' 156
6.4.2 Ensure 'Audit Directory Service Changes' is set to include 'Success' 157
6.5 Logon/Logoff 158
6.5.1 Ensure 'Audit Account Lockout' is set to include 'Failure' 158
6.5.2 Ensure 'Audit Group Membership' is set to include 'Success' 159
6.5.3 Ensure 'Audit Logoff' is set to include 'Success' 160
6.5.4 Ensure 'Audit Logon' is set to 'Success and Failure' 161
6.5.5 Ensure 'Audit Other Logon/Logoff Events' is set to 'Success and Failure' 162
6.5.6 Ensure 'Audit Special Logon' is set to include 'Success' 163
6.6 Object Access 164
6.6.1 Ensure 'Audit Detailed File Share' is set to include 'Failure' 164
6.6.2 Ensure 'Audit File Share' is set to 'Success and Failure' 165
6.6.3 Ensure 'Audit Other Object Access Events' is set to 'Success and Failure' 166
6.6.4 Ensure 'Audit Removable Storage' is set to 'Success and Failure' 167
6.7 Policy Change 168
6.7.1 Ensure 'Audit Audit Policy Change' is set to include 'Success' 168
6.7.2 Ensure 'Audit Authentication Policy Change' is set to include 'Success' 169
6.7.3 Ensure 'Audit Authorization Policy Change' is set to include 'Success' 170
6.7.4 Ensure 'Audit MPSSVC Rule-Level Policy Change' is set to 'Success and Failure' 171
6.7.5 Ensure 'Audit Other Policy Change Events' is set to include 'Failure' 172
6.8 Policy Change 173
6.8.1 Ensure 'Audit Sensitive Privilege Use' is set to 'Success and Failure' 173
6.9 System 174
6.9.1 Ensure 'Audit IPsec Driver' is set to 'Success and Failure' 174
6.9.2 Ensure 'Audit Other System Events' is set to 'Success and Failure' 175
6.9.3 Ensure 'Audit Security State Change' is set to include 'Success' 176
6.9.4 Ensure 'Audit Security System Extension' is set to include 'Success' 177
6.9.5 Ensure 'Audit System Integrity' is set to 'Success and Failure' 178
7 Administrative Templates 179
7.1 Control Panel 179
7.1.1 Personalization 179
7.1.1.1 Ensure 'Prevent enabling lock screen camera' is set to 'Enabled' 179
7.1.1.2 Ensure 'Prevent enabling lock screen slide show' is set to 'Enabled' 180

7.1.2 Regional and Language Options 181
7.1.2.1 Ensure 'Allow users to enable online speech recognition services' is set to 'Disabled' 181
7.1.3 Ensure 'Allow Online Tips' is set to 'Disabled' 182
7.2 MS Security Guide 183
7.2.1 Ensure 'Configure SMB v1 client driver' is set to 'Enabled: Disable driver (recommended)' 183
7.2.2 Ensure 'Configure SMB v1 server' is set to 'Disabled' 184
7.2.3 Ensure 'Enable Structured Exception Handling Overwrite Protection (SEHOP)' is set to 'Enabled' 185
7.2.4 Ensure 'LSA Protection' is set to 'Enabled' 186
7.2.5 Ensure 'WDigest Authentication' is set to 'Disabled' 187
7.3 MSS (Legacy) 188
7.3.1 Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled' 188
7.3.2 Ensure 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled' 189
7.3.3 Ensure 'MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled' 190
7.3.4 Ensure 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' is set to 'Disabled' 191
7.3.5 Ensure 'MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds' is set to 'Enabled: 300,000 or 5 minutes (recommended)' 192
7.3.6 Ensure 'MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers' is set to 'Enabled' 193
7.3.7 Ensure 'MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)' is set to 'Disabled' 194
7.3.8 Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' is set to 'Enabled' 195
7.3.9 Ensure 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)' is set to 'Enabled: 5 or fewer seconds' 196
7.3.10 Ensure 'MSS: (TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted' is set to 'Enabled: 3' 197
7.3.11 Ensure 'MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted' is set to 'Enabled: 3' 198
7.3.12 Ensure 'MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning' is set to 'Enabled: 90% or less' 199
7.4 Network 200
7.4.1 DNS Client 200
7.4.1.1 Ensure 'Turn off multicast name resolution' is set to 'Enabled' 200
7.4.2 Fonts 201
7.4.2.1 Ensure 'Enable Font Providers' is set to 'Disabled' 201
7.4.3 Lanman Workstation 202
7.4.3.1 Ensure 'Enable insecure guest logons' is set to 'Disabled' 202

7.4.4 Link-Layer Topology Discovery 203
7.4.4.1 Ensure 'Turn on Mapper I/O (LLTDIO) driver' is set to 'Disabled' 203
7.4.4.2 Ensure 'Turn on Responder (RSPNDR) driver' is set to 'Disabled' 204
7.4.5 Microsoft Peer-to-Peer Networking Services 205
7.4.5.1 Ensure 'Turn off Microsoft Peer-to-Peer Networking Services' is set to 'Enabled' 205
7.4.6 Network Connections 206
7.4.6.1 Ensure 'Prohibit installation and configuration of Network Bridge on your DNS domain network' is set to 'Enabled' 206
7.4.6.2 Ensure 'Prohibit use of Internet Connection Sharing on your DNS domain network' is set to 'Enabled' 207
7.4.7 Network Provider 208
7.4.7.1 Ensure 'Hardened UNC Paths' is set to 'Enabled, with "Require Mutual Authentication" and "Require Integrity" set for all NETLOGON and SYSVOL shares' 208
7.4.8 Windows Connect Now 209
7.4.8.1 Ensure 'Configuration of wireless settings using Windows Connect Now' is set to 'Disabled' 209
7.4.8.2 Ensure 'Prohibit access of the Windows Connect Now wizards' is set to 'Enabled' 210
7.4.9 Windows Connection Manager 211
7.4.9.1 Ensure 'Minimize the number of simultaneous connections to the Internet or a Windows Domain' is set to 'Enabled: 3 = Prevent Wi-Fi when on Ethernet' 211
7.5 Printers 212
7.5.1 Ensure 'Allow Print Spooler to accept client connections' is set to 'Disabled' 212
7.5.2 Ensure 'Configure Redirection Guard' is set to 'Enabled: Redirection Guard Enabled' 213
7.5.3 Ensure 'Point and Print Restrictions: When installing drivers for a new connection' is set to 'Enabled: Show warning and elevation prompt' 214
7.5.4 Ensure 'Point and Print Restrictions: When updating drivers for an existing connection' is set to 'Enabled: Show warning and elevation prompt' 215
7.6 Start Menu and Taskbar 216
7.6.1 Notifications 216
7.6.1.1 Ensure 'Turn off notifications network usage' is set to 'Enabled' 216
7.7 System 217
7.7.1 Audit Process Creation 217
7.7.1.1 Ensure 'Include command line in process creation events' is set to 'Enabled' .. 217
7.7.2 Credentials Delegation 218
7.7.2.1 Ensure 'Encryption Oracle Remediation' is set to 'Enabled: Force Updated Clients' 218
7.7.2.2 Ensure 'Remote host allows delegation of nonexportable credentials' is set to 'Enabled' 219
7.7.3 Device Guard 220
7.7.3.1 Ensure 'Remote host allows delegation of nonexportable credentials' is set to 'Enabled' 220
7.7.4 Device Installation 221

7.7.4.1 Ensure 'Prevent device metadata retrieval from the Internet' is set to 'Enabled' 221
7.7.5 Early Launch Antimalware 222
7.7.5.1 Ensure 'Boot-Start Driver Initialization Policy' is set to 'Enabled: Good, unknown and bad but critical' 222
7.7.6 Group Policy 223
7.7.6.1 Ensure 'Continue experiences on this device' is set to 'Disabled' 223
7.7.7 Internet Communication Management 224
7.7.7.1 Internet Communication settings 224
7.7.8 Kerberos 237
7.7.8.1 Ensure 'Support device authentication using certificate' is set to 'Enabled: Automatic' 237
7.7.9 Kernel DMA Protection 238
7.7.9.1 Ensure 'Support device authentication using certificate' is set to 'Enabled: Automatic' 238
7.7.10 Locale Services 239
7.7.10.1 Ensure 'Disallow copying of user input methods to the system account for sign-in' is set to 'Enabled' 239
7.7.11 Logon 240
7.7.11.1 Ensure 'Block user from showing account details on sign-in' is set to 'Enabled' 240
7.7.11.2 Ensure 'Do not display network selection UI' is set to 'Enabled' 241
7.7.11.3 Ensure 'Turn off app notifications on the lock screen' is set to 'Enabled' 242
7.7.11.4 Ensure 'Turn on convenience PIN sign-in' is set to 'Disabled' 243
7.7.12 OS Policies 244
7.7.12.1 Ensure 'Allow Clipboard synchronization across devices' is set to 'Disabled' 244
7.7.12.2 Ensure 'Allow upload of User Activities' is set to 'Disabled' 245
7.7.13 Power Management 246
7.7.13.1 Sleep Settings 246
7.7.14 Remote Assistance 250
7.7.14.1 Ensure 'Configure Offer Remote Assistance' is set to 'Disabled' 250
7.7.14.2 Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled' 251
7.7.15 Remote Procedure Call 252
7.7.15.1 Ensure 'Enable RPC Endpoint Mapper Client Authentication' is set to 'Enabled' 252
7.7.15.2 Ensure 'Restrict Unauthenticated RPC clients' is set to 'Enabled: Authenticated' 253
7.7.16 Troubleshooting and Diagnostics 254
7.7.16.1 Microsoft Support Diagnostic Tool 254
7.7.16.2 Windows Performance PerfTrack 255
7.7.17 User Profiles 256
7.7.17.1 Ensure 'Turn off the advertising ID' is set to 'Enabled' 256
7.7.18 Windows Time Service 257
7.7.18.1 Time Providers 257
7.8 Windows Components 259
7.8.1 App Package Deployment 259
7.8.1.1 Ensure 'Allow a Windows app to share application data between users' is set to 'Disabled' 259

7.8.2 App runtime 260
7.8.2.1 Ensure 'Allow Microsoft accounts to be optional' is set to 'Enabled' 260
7.8.3 AutoPlay Policies 261
7.8.3.1 Ensure 'Disallow Autoplay for non-volume devices' is set to 'Enabled' 261
7.8.3.2 Ensure 'Set the default behavior for AutoRun' is set to 'Enabled: Do not execute any autorun commands' 262
7.8.3.3 Ensure 'Turn off Autoplay' is set to 'Enabled: All drives' 263
7.8.4 Biometrics 264
7.8.4.1 Facial Features 264
7.8.5 Camera 265
7.8.5.1 Ensure 'Allow Use of Camera' is set to 'Disabled' 265
7.8.6 Cloud Content 266
7.8.6.1 Ensure 'Turn off Microsoft consumer experiences' is set to 'Enabled' 266
7.8.7 Connect 267
7.8.7.1 Ensure 'Require pin for pairing' is set to 'Enabled: First Time' OR 'Enabled: Always' 267
7.8.8 Credential User Interface 268
7.8.8.1 Ensure 'Do not display the password reveal button' is set to 'Enabled' 268
7.8.8.2 Ensure 'Enumerate administrator accounts on elevation' is set to 'Disabled' ... 269
7.8.9 Credential User Interface 270
7.8.9.1 Ensure 'Configure Authenticated Proxy usage for the Connected User Experience and Telemetry service' is set to 'Enabled: Disable Authenticated Proxy usage' 270
7.8.9.2 Ensure 'Do not show feedback notifications' is set to 'Enabled' 271
7.8.9.3 Ensure 'Toggle user control over Insider builds' is set to 'Disabled' 272
7.8.10 Event Log Service 273
7.8.10.1 Application 273
7.8.10.2 Security 275
7.8.10.3 Setup 277
7.8.10.4 System 279
7.8.11 File Explorer (formerly Windows Explorer) 281
7.8.11.1 Ensure 'Turn off Data Execution Prevention for Explorer' is set to 'Disabled' 281
7.8.11.2 Ensure 'Turn off heap termination on corruption' is set to 'Disabled' 282
7.8.11.3 Ensure 'Turn off shell protocol protected mode' is set to 'Disabled' 283
7.8.12 Location and Sensors 284
7.8.12.1 Ensure 'Turn off shell protocol protected mode' is set to 'Disabled' 284
7.8.13 Messaging 285
7.8.13.1 Ensure 'Allow Message Service Cloud Sync' is set to 'Disabled' 285
7.8.14 Microsoft account 286
7.8.14.1 Ensure 'Block all consumer Microsoft account user authentication' is set to 'Enabled' 286
7.8.15 Microsoft account 287
7.8.15.1 Microsoft Defender Exploit Guard (formerly Windows Defender Exploit Guard) 287
7.8.15.2 Real-time Protection 289
7.8.15.3 Reporting 292
7.8.15.4 Scan 293

7.8.15.5 Ensure 'Configure detection for potentially unwanted applications' is set to 'Enabled: Block' 295
7.8.15.6 Ensure 'Turn off Microsoft Defender AntiVirus' is set to 'Disabled' 296
7.8.16 OneDrive (formerly SkyDrive) 297
7.8.16.1 Ensure 'Prevent the usage of OneDrive for file storage' is set to 'Enabled' 297
7.8.17 Push To Install 298
7.8.17.1 Ensure 'Prevent the usage of OneDrive for file storage' is set to 'Enabled' 298
7.8.18 Remote Desktop Services (formerly Terminal Services) 299
7.8.18.1 Remote Desktop Connection Client 299
7.8.18.2 Remote Desktop Session Host (formerly Terminal Server) 300
7.8.19 RSS Feeds 314
7.8.19.1 Ensure 'Prevent downloading of enclosures' is set to 'Enabled' 314
7.8.20 Search 315
7.8.20.1 Ensure 'Allow Cloud Search' is set to 'Enabled: Disable Cloud Search' 315
7.8.20.2 Ensure 'Allow indexing of encrypted files' is set to 'Disabled' 316
7.8.21 Software Protection Platform 317
7.8.21.1 Ensure 'Turn off KMS Client Online AVS Validation' is set to 'Enabled' 317
7.8.22 Windows Defender SmartScreen 318
7.8.22.1 Explorer 318
7.8.23 Windows Ink Workspace 319
7.8.23.1 Ensure 'Allow suggested apps in Windows Ink Workspace' is set to 'Disabled' . 319
7.8.23.2 Ensure 'Allow Windows Ink Workspace' is set to 'Enabled: On, but disallow access above lock' OR 'Enabled: Disabled' 320
7.8.24 Windows Installer 321
7.8.24.1 Ensure 'Allow user control over installs' is set to 'Disabled' 321
7.8.24.2 Ensure 'Always install with elevated privileges' is set to 'Disabled' 322
7.8.24.3 Ensure 'Prevent Internet Explorer security prompt for Windows Installer scripts' is set to 'Disabled' 323
7.8.25 Windows Logon Options 324
7.8.25.1 Ensure 'Sign-in and lock last interactive user automatically after a restart' is set to 'Disabled' 324
7.8.26 Windows PowerShell 325
7.8.26.1 Ensure 'Turn on PowerShell Script Block Logging' is set to 'Enabled' 325
7.8.26.2 Ensure 'Turn on PowerShell Transcription' is set to 'Enabled' 326
7.8.27 Windows Remote Management (WinRM) 327
7.8.27.1 WinRM Client 327
7.8.27.2 WinRM Service 330
7.8.28 Windows Remote Shell 334
7.8.28.1 Ensure 'Allow Remote Shell Access' is set to 'Disabled' 334
7.8.29 Windows Security (formerly Windows Defender Security Center) 335
7.8.29.1 App and browser protection 335
7.8.30 Windows Update 336
7.8.30.1 Legacy Policies 336
7.8.30.2 Manage end user experience 337
7.8.30.3 Manage updates offered from Windows Update (formerly Defer Windows Updates and Windows Update for Business) 338
8 Administrative Templates (User) 341

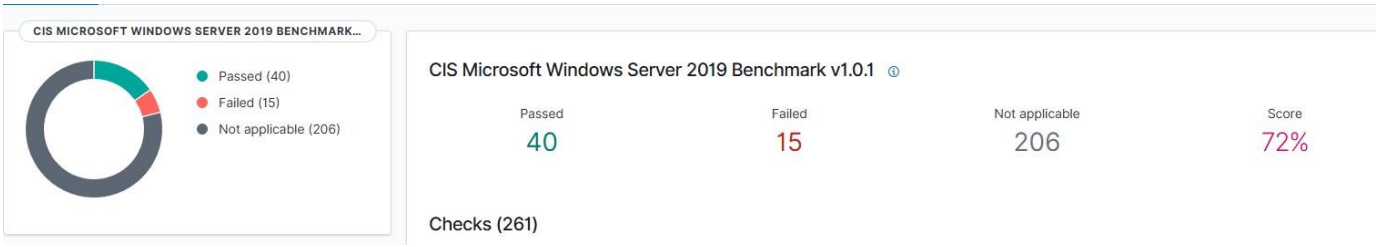
8.1 Control Panel 341
8.1.1 Personalization (formerly Desktop Themes) 341
8.1.1.1 Ensure 'Enable screen saver' is set to 'Enabled' 341
8.2 Start Menu and Taskbar 342
8.2.1 Notifications 342
8.2.1.1 Ensure 'Enable screen saver' is set to 'Enabled' 342
8.3 System 343
8.3.1 Internet Communication Management 343
8.3.1.1 Internet Communication settings 343
8.4 Windows Components 344
8.4.1 Attachment Manager 344
8.4.1.1 Ensure 'Do not preserve zone information in file attachments' is set to 'Disabled' 344
8.4.1.2 Ensure 'Notify antivirus programs when opening attachments' is set to 'Enabled' 345
8.4.2 Cloud Content 346
8.4.2.1 Ensure 'Configure Windows spotlight on lock screen' is set to 'Disabled' 346
8.4.2.2 Ensure 'Do not suggest third-party content in Windows spotlight' is set to 'Enabled' 347
8.4.2.3 Ensure 'Do not use diagnostic data for tailored experiences' is set to 'Enabled' 348
8.4.2.4 Ensure 'Turn off all Windows spotlight features' is set to 'Enabled' 349
8.4.3 Network Sharing 350
8.4.3.1 Ensure 'Prevent users from sharing files within their profile.' is set to 'Enabled' 350
8.4.4 Windows Installer 351
8.4.4.1 Ensure 'Always install with elevated privileges' is set to 'Disabled' 351
8.4.5 Windows Media Player 352
8.4.5.1 Playback 352
9 Conclusion 353

1 Introduction

In today's rapidly evolving digital landscape, securing and fortifying our systems is paramount. For a Windows Server 2019 environment, we will apply hardening measures based on the CIS (Center for Internet Security) Benchmark Documents. These benchmarks offer a comprehensive set of guidelines designed to reduce vulnerabilities and enhance system protection against potential cyber threats.

In addition to implementing these hardening measures, we will undertake remediation efforts to address any identified vulnerabilities. This proactive approach will help safeguard the server from various cybersecurity risks.

To assess the impact of these security enhancements, an initial security score will be presented using the Wazuh security tool. This score will serve as a baseline for evaluating the effectiveness of the applied controls. After the hardening and remediation processes are completed, a final security score will be provided. The comparison between the initial and final scores will demonstrate the improvements in the system's security posture and the effectiveness of the implemented measures.



2 Account Policies

This section outlines the establishment of account policies designed to fortify system security and mitigate potential vulnerabilities within user accounts.

2.1

A robust password policy serves as the foundational defense for safeguarding user accounts. It is imperative that passwords adhere to stringent complexity standards to mitigate the risk of unauthorized access. Moreover, implementing additional measures such as password history tracking, periodic password changes, and automatic lockouts following repeated failed login attempts fortify this critical layer of security against both guessing and brute force attacks.

2.1.1 Ensure 'Enforce password history' is set to '24 or more password(s)'

This policy specifies the minimum number of new, distinct passwords required before an old password can be reused for a user account. The permissible range for this policy is between 0 and 24 passwords. By default, standalone systems allow immediate password reuse (set to 0 passwords), whereas domain-joined systems default to requiring 24 unique passwords before reuse. To ensure the efficacy of this policy, it is advisable to coordinate it with the Minimum password age setting, which discourages users from frequently changing their passwords.

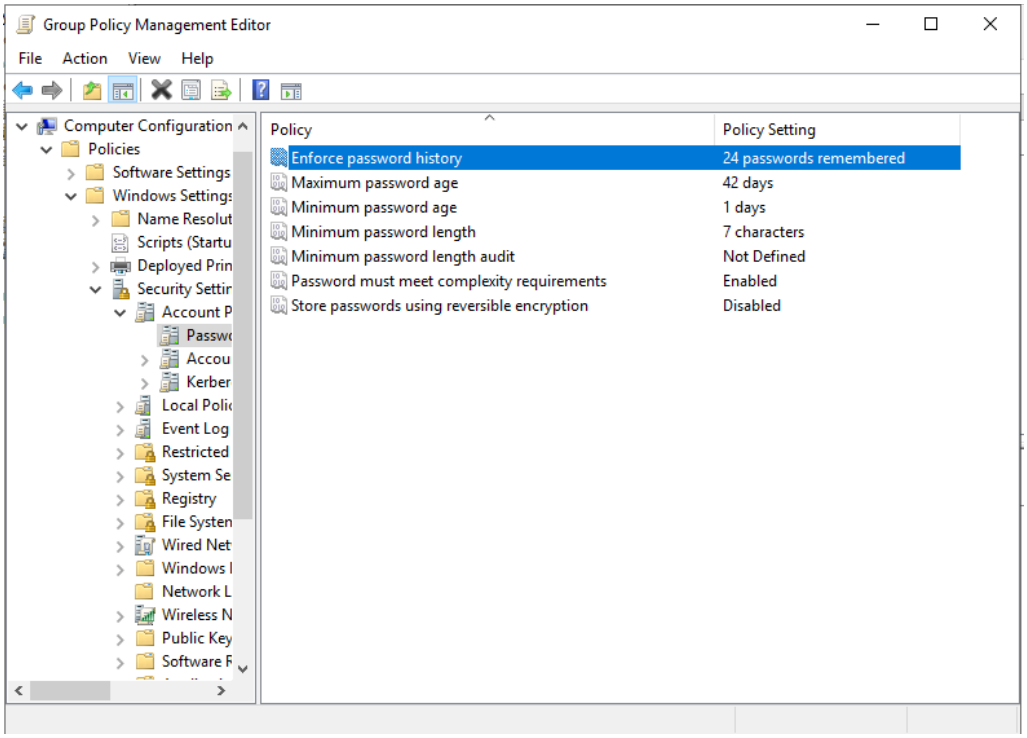


Image 1-Enforce password history

2.1.2 Ensure 'Maximum password age' is set to '365 or fewer days, but not 0'

This policy determines the duration for which a user's password remains valid before it requires renewal. The permissible range for this setting spans from 0 to 999 days. Setting the value to 0 ensures that the password never expires. Regular password changes are recommended as a security measure since it reduces the window of opportunity for attackers to exploit compromised passwords. However, a lower value increases the likelihood of users needing assistance from the help desk either to change their passwords frequently or to recall their current passwords, potentially leading to an increase in support calls.

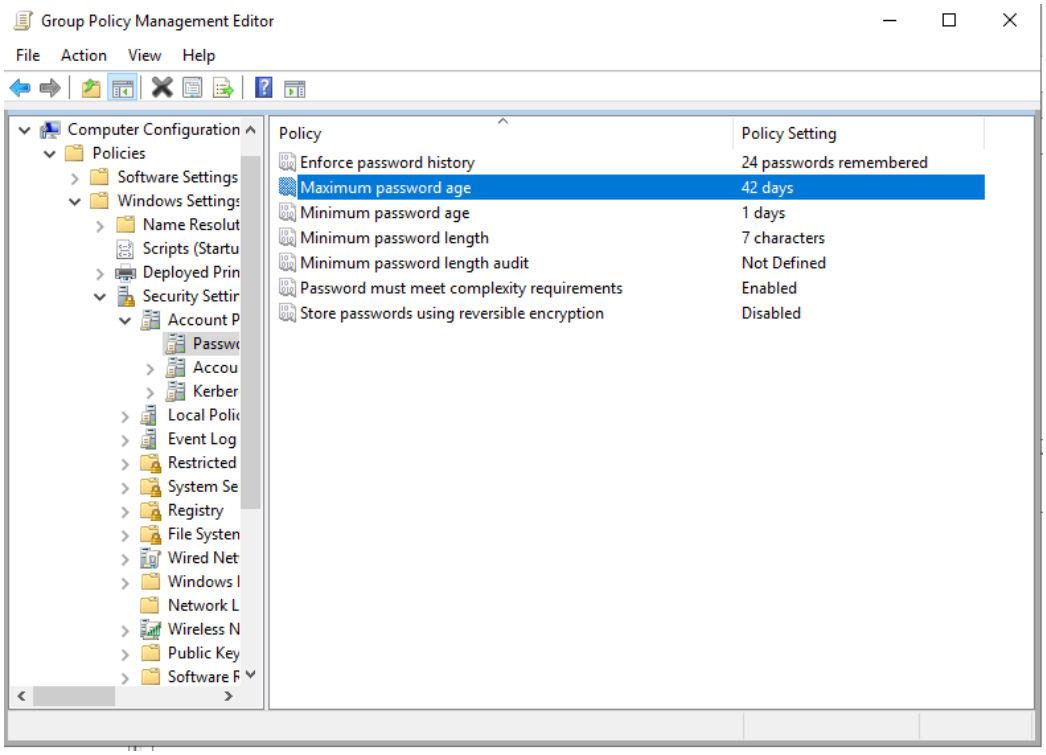


Image 2- Ensure 'Maximum password age' is set to '365 or fewer days'

2.1.3 Ensure 'Minimum password age' is set to '1 or more day(s)'

This policy defines the duration a password must be in use before it can be changed. The permissible range for this setting spans from 1 to 999 days. Alternatively, setting the value to 0 allows immediate password changes. By default, this setting is configured to permit instant password changes.

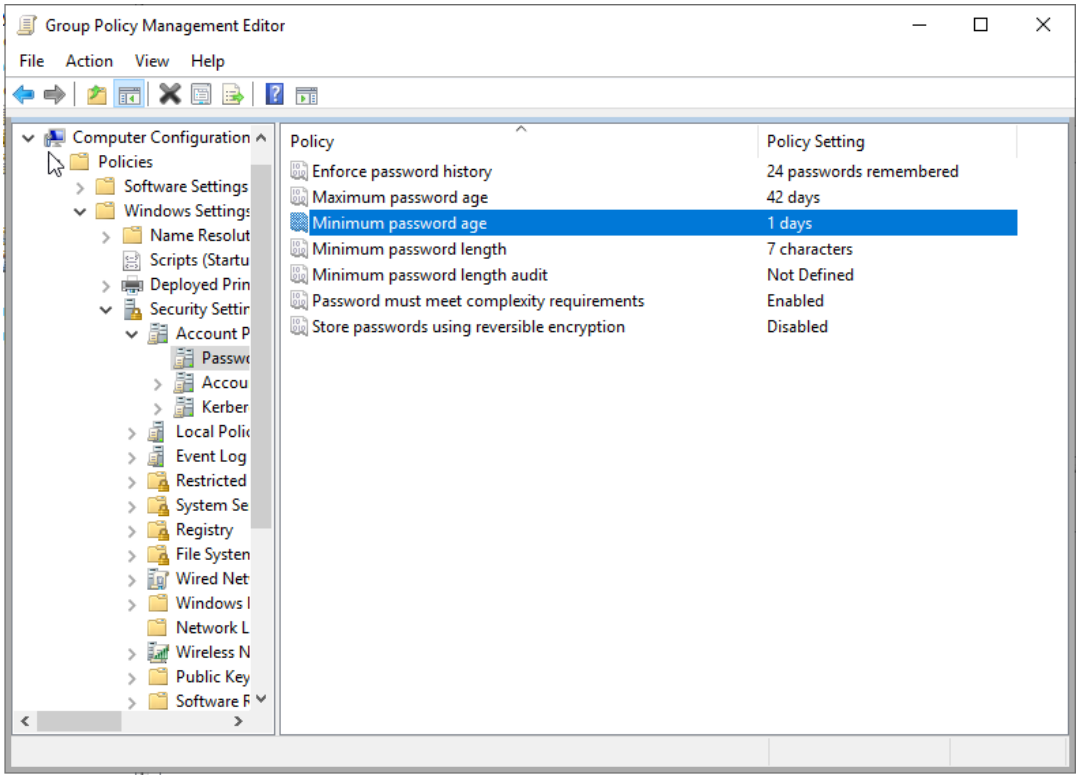


Image 3-Ensure 'Minimum password age' is set to '1 or more day(s)'

2.1.4 Ensure 'Minimum password length' is set to '14 or more character(s)'

This policy determines the minimum number of characters required for a user account password. Various approaches exist for determining the optimal password length within an organization, with some advocating for the use of "passphrases" rather than traditional passwords. In Microsoft Windows 2000 or newer systems, passphrases can be lengthy and may include spaces. For instance, a phrase like "I want to drink a $5 milkshake" constitutes a valid passphrase, offering stronger security compared to shorter strings of random characters while also being easier to recall. It's crucial to educate users on the importance of selecting and maintaining passwords, particularly regarding their length. In enterprise environments, it's recommended to set the Minimum password length to 14 characters, although adjustments should be made based on the specific business requirements of the organization.

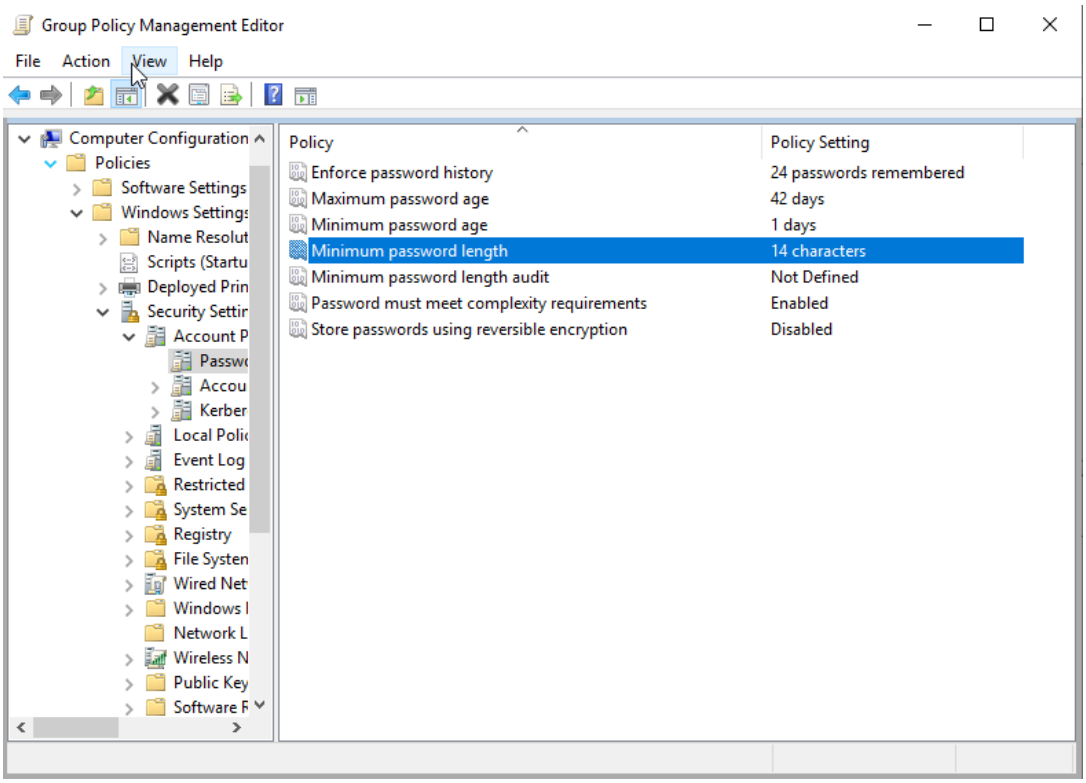


Image 4-Ensure 'Minimum password length' is set to '14 or more character(s)'

2.1.5 Ensure 'Password must meet complexity requirements' is set to 'Enabled'

This policy mandates that all newly created passwords meet basic strength criteria. Passwords must not include the user's account name or consecutive parts of their full name, be at least six characters long, and contain characters from at least three of the following categories: uppercase letters, lowercase letters, digits, and non-alphabetic characters. The complexity of a password increases exponentially with each additional character. For instance, a seven-character lowercase password could be cracked in 133 minutes at a rate of 1,000,000 attempts per second. Properly configuring password settings can significantly impede brute force attacks.

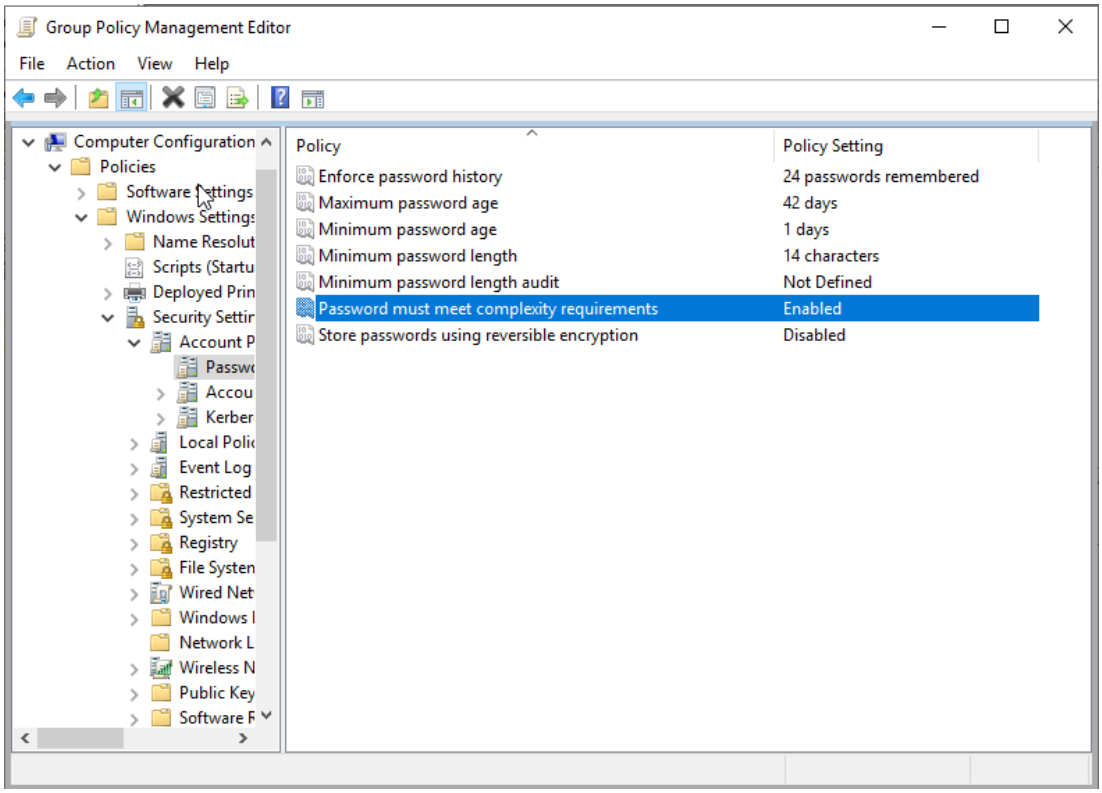


Image 5-Ensure 'Password must meet complexity requirements' is set to 'Enabled'

2.1.6 Ensure 'Store passwords using reversible encryption' is set to 'Disabled'

This policy setting governs whether the operating system stores passwords using reversible encryption. Reversible encryption is used to support certain application protocols that necessitate access to the user's password for authentication. Passwords stored with reversible encryption are essentially equivalent to plaintext versions of the passwords.

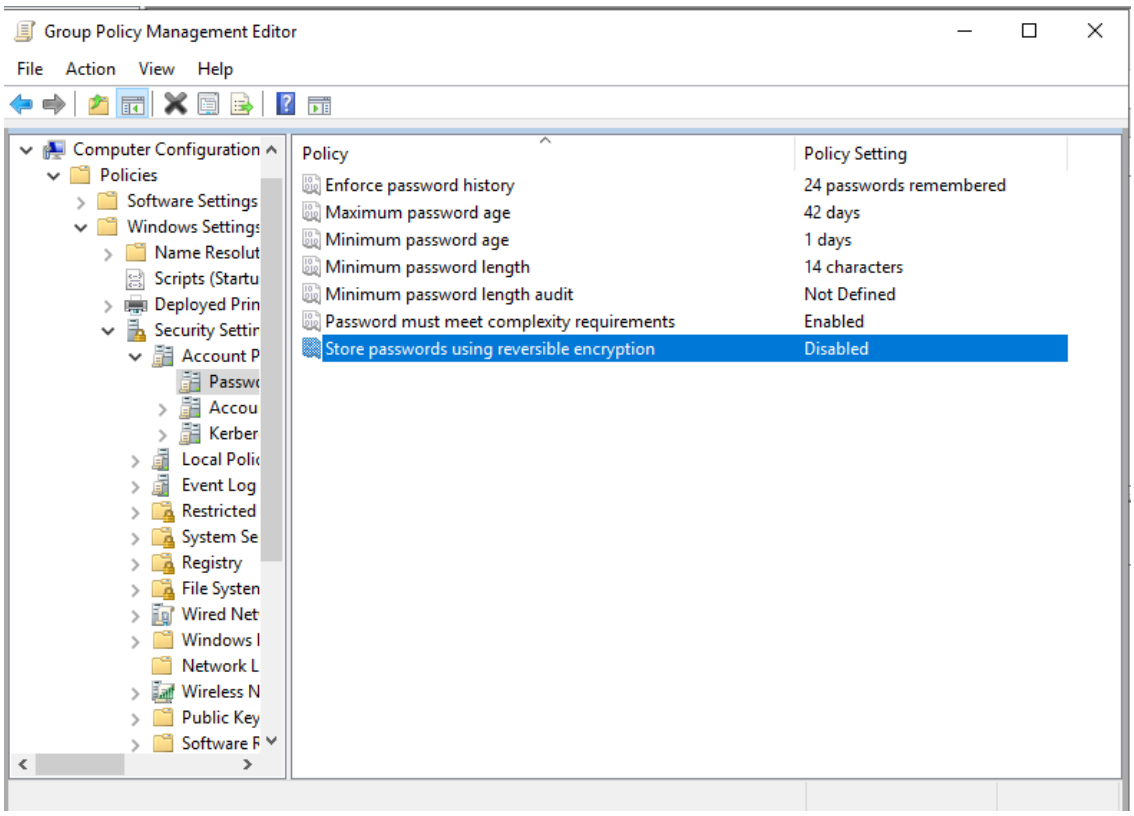


Image 6-Ensure 'Store passwords using reversible encryption' is set to 'Disabled'

2.2 Account Lockout Policy

The Account Lockout Policy in Windows is a vital security feature that prevents unauthorized access to user accounts. It sets thresholds for locking out accounts after a specified number of failed login attempts, deterring brute force attacks.

Administrators can customize settings such as the maximum number of failed attempts allowed, lockout duration, and reset intervals. This flexibility allows for tailored security measures while balancing usability.

When implemented alongside strong password policies and multi-factor authentication, the Account Lockout Policy enhances overall security, safeguarding university data and resources.

2.2.1 Ensure 'Account lockout duration' is set to '15 or more minute(s)'

This policy dictates the duration a locked account remains inaccessible before it automatically unlocks, allowing the user to attempt logging in again. It specifies the number of minutes for which the account stays locked. Setting the value to 0 means the account remains locked until manually unlocked by an administrator.

While setting a high value may seem prudent, it often leads to an increase in help desk calls for unlocking mistakenly locked accounts. Users should be informed about the lock duration, understanding they should only contact the help desk if urgent access to their computer is required.

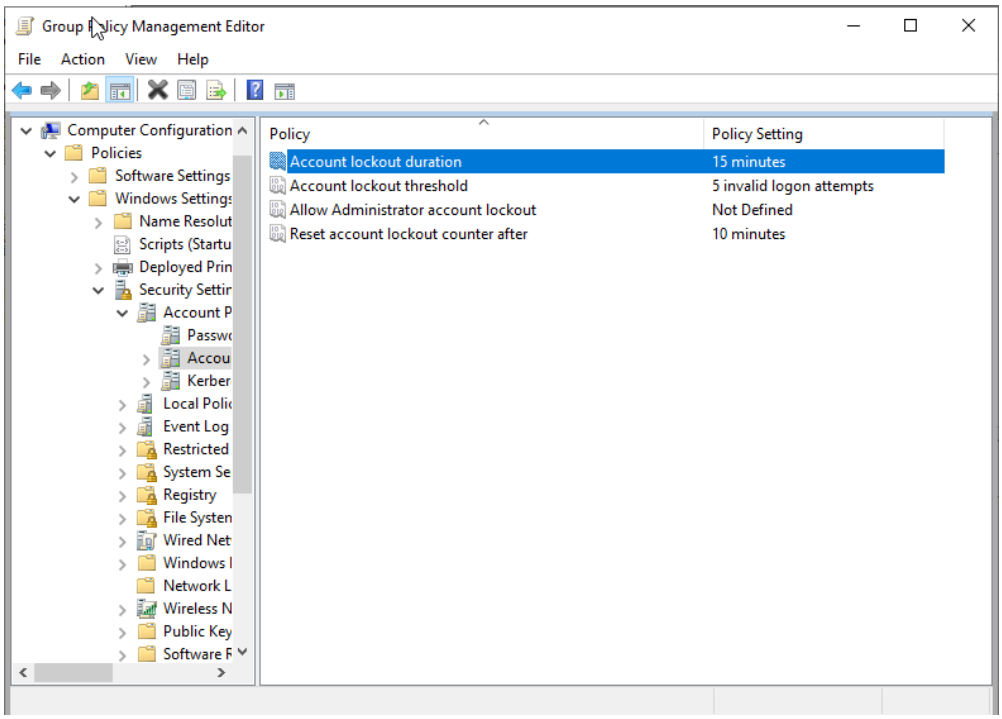


Image 7-Ensure 'Account lockout duration' is set to '15 or more minute(s)'

2.2.2 Ensure 'Account lockout threshold' is set to '5 or fewer invalid logon attempt(s), but not 0'

This policy setting establishes the threshold for failed login attempts before an account is locked. Configuring this policy to 0 does not adhere to standard practices, as it disables the account lockout feature.

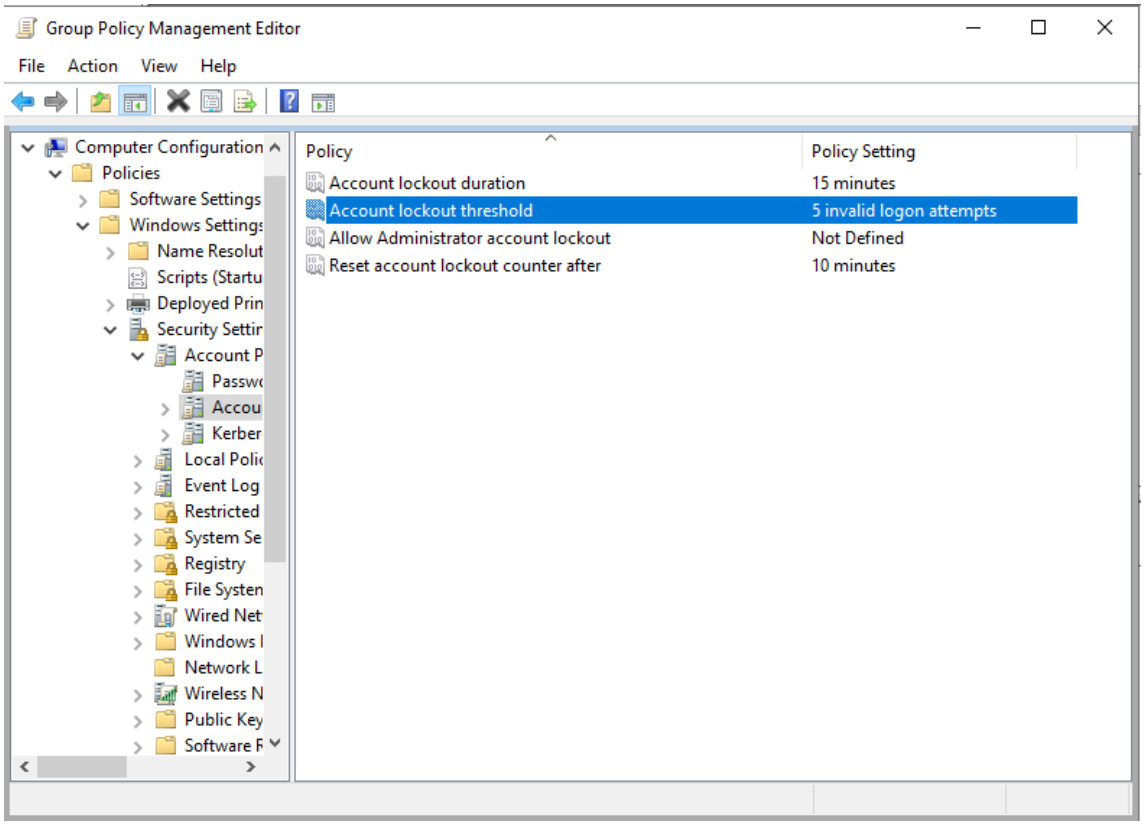


Image 8-Ensure 'Account lockout threshold' is set to '5 or fewer invalid logon attempt(s), but not 0'

2.2.3 Ensure 'Allow Administrator account lockout' is set to 'Enabled'

This policy determines if the built-in Administrator account is affected by the Account Lockout Policy settings, including Account lockout duration, Account lockout threshold, and Reset account lockout counter. By default, the built-in Administrator account is exempt from these controls, ensuring it won't be locked out due to multiple incorrect password attempts.

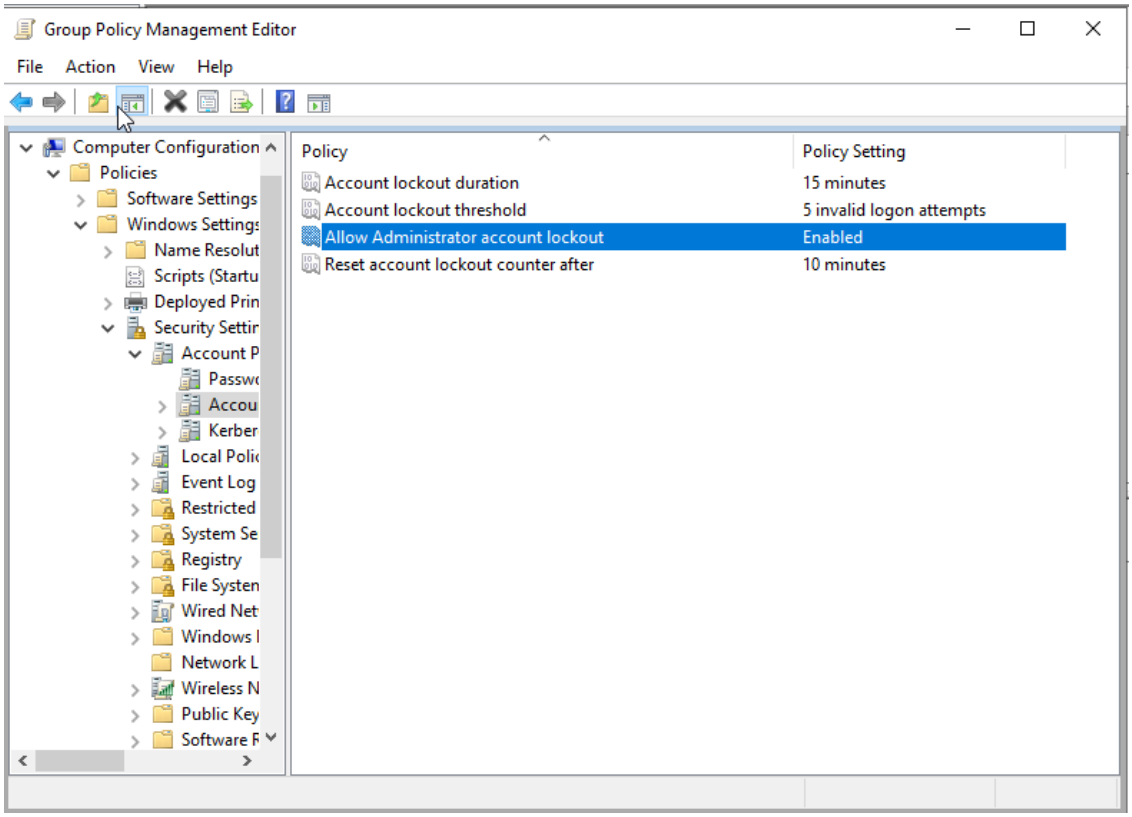


Image 9- Ensure 'Allow Administrator account lockout' is set to 'Enabled'

2.2.4 Ensure 'Reset account lockout counter after' is set to '15 or more minute(s)'

This policy determines the duration before the Account lockout threshold resets to zero. By default, this policy is set to Not Defined. However, if the Account lockout threshold is specified, the reset time must be equal to or less than the Account lockout duration setting.

Leaving this policy at its default value or setting it to an excessively long interval may expose your environment to a Denial of Service (DoS) attack. An attacker could deliberately trigger multiple failed login attempts across all user accounts, resulting in their lockout. Without a defined policy to reset the account lockout, administrators would need to manually unlock accounts. Conversely, configuring a reasonable time value for this policy ensures that users are temporarily locked out until all accounts are automatically unlocked.

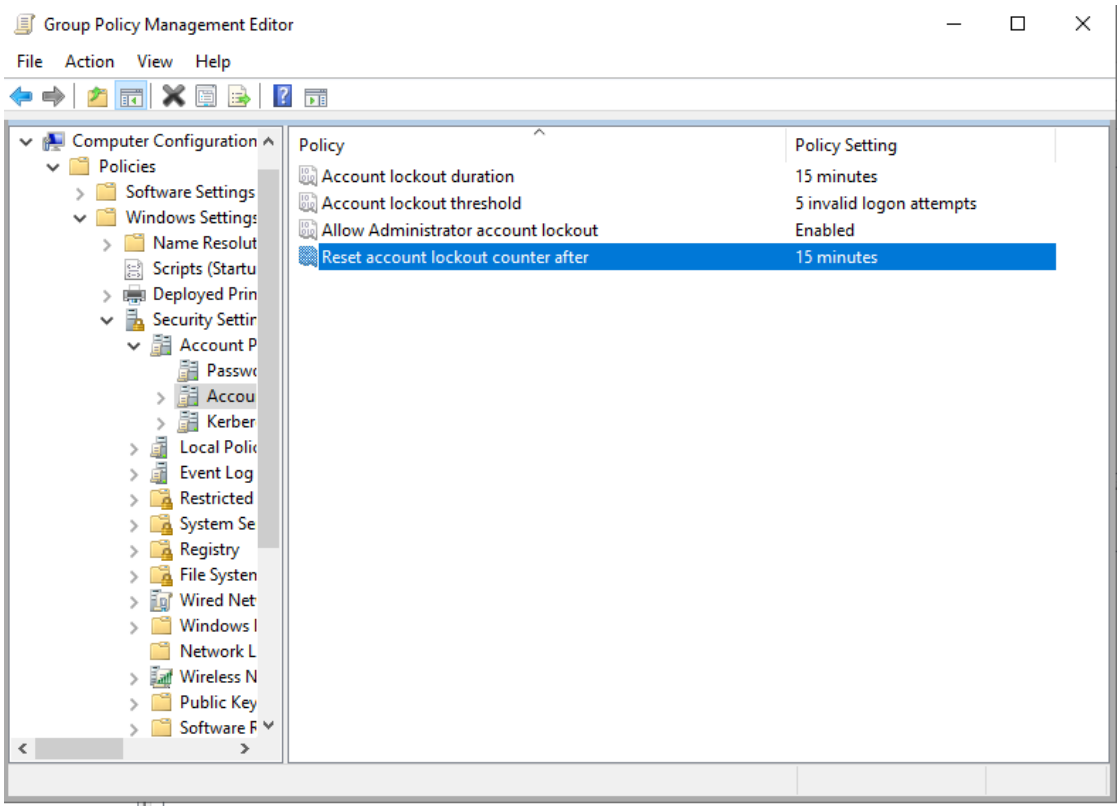


Image 10- Ensure 'Reset account lockout counter after' is set to '15 or more minute(s)'

3 Local Policies

In this section, we'll address local security policies aimed at bolstering the system's defense mechanisms and safeguarding against potential threats at the local level.

3.1 User Rights Assignment

This entails defining user rights assignment to regulate user access and privileges within the system. By specifying user rights, organizations can precisely control user actions and permissions, ensuring adherence to security protocols and regulatory requirements. Through meticulous configuration of user rights assignment, robust access controls are established, promoting system integrity and safeguarding against unauthorized activities or data breaches.

3.1.1 Ensure 'Access Credential Manager as a trusted caller' is set to 'No One'

This security feature is utilized by Credential Manager during Backup and Restore processes. This user right should not be assigned to any accounts except Winlogon. Assigning this user right to other entities could potentially compromise users' saved credentials.

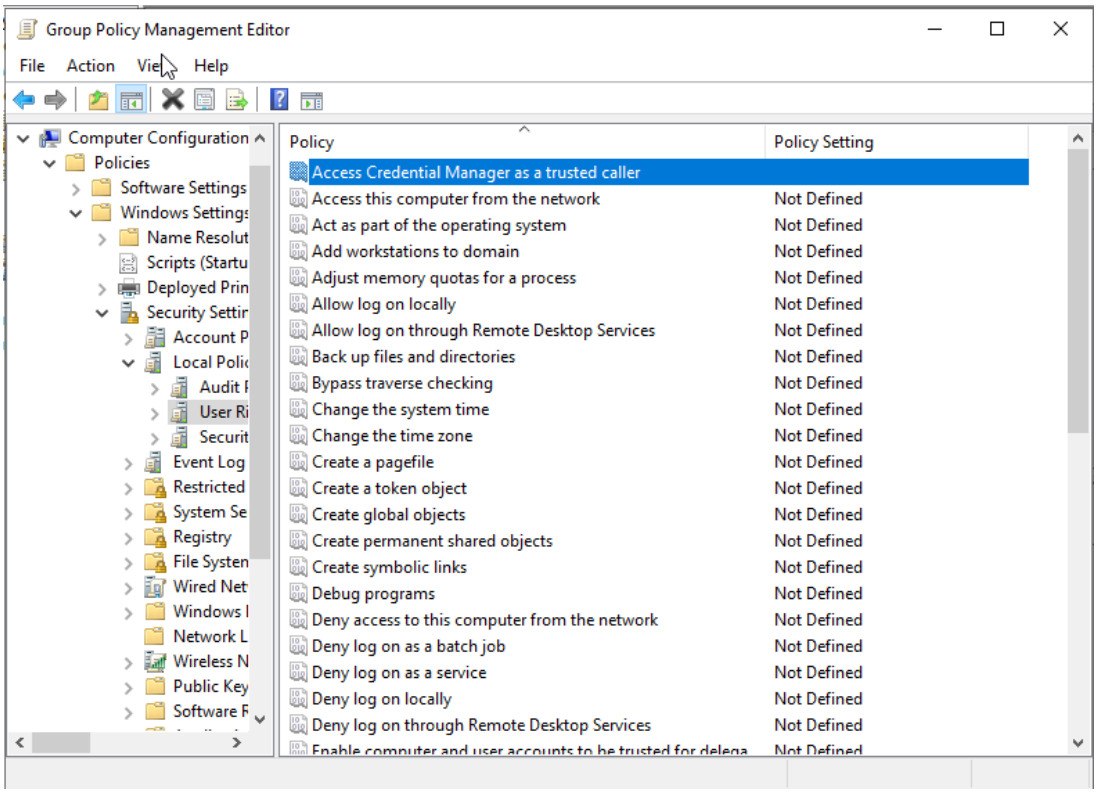


Image 11- Ensure 'Access Credential Manager as a trusted caller' is set to 'No One'

3.1.2 Ensure 'Access this computer from the network' is set to 'Administrators, Authenticated Users, ENTERPRISE DOMAIN CONTROLLERS'

This policy setting enables other network users to establish connections with the computer, which is essential for various network protocols such as Server Message Block (SMB), NetBIOS, Common Internet File System (CIFS), and Component Object Model Plus (COM+).

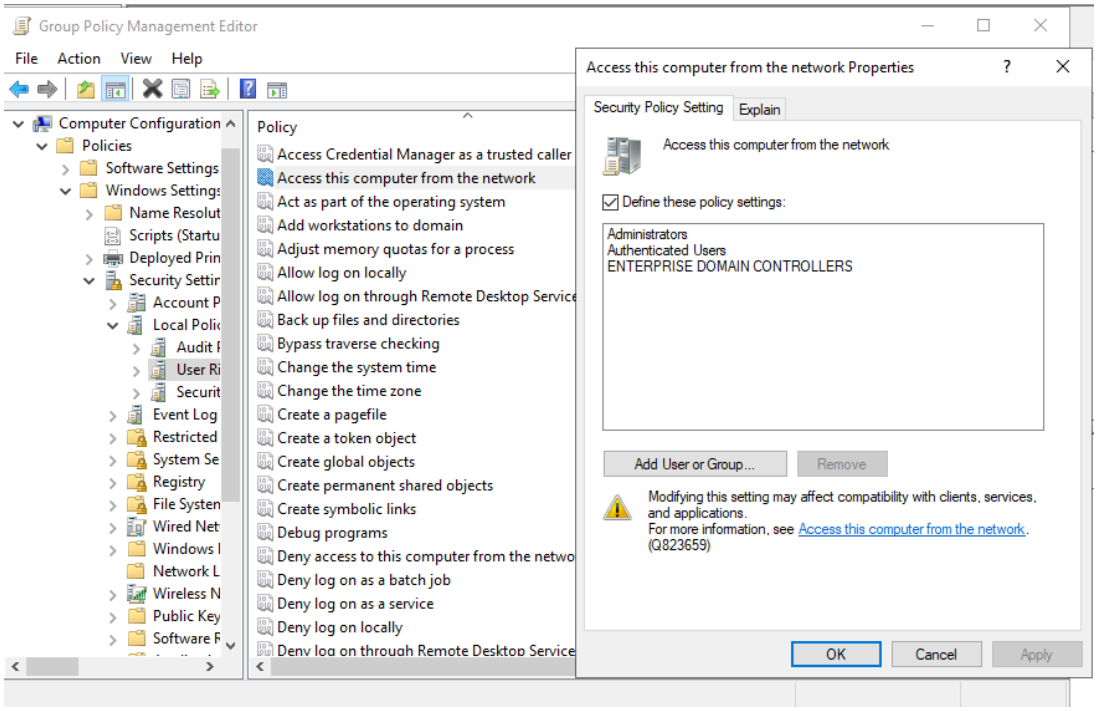


Image 12- Ensure 'Access this computer from the network' is set to 'Administrators, Authenticated Users, ENTERPRISE DOMAIN CONTROLLERS'

3.1.3 Ensure Act as part of the operating system' is set to 'No One'

This policy setting permits a process to take on the identity of any user, thereby acquiring access to the resources authorized for that user.

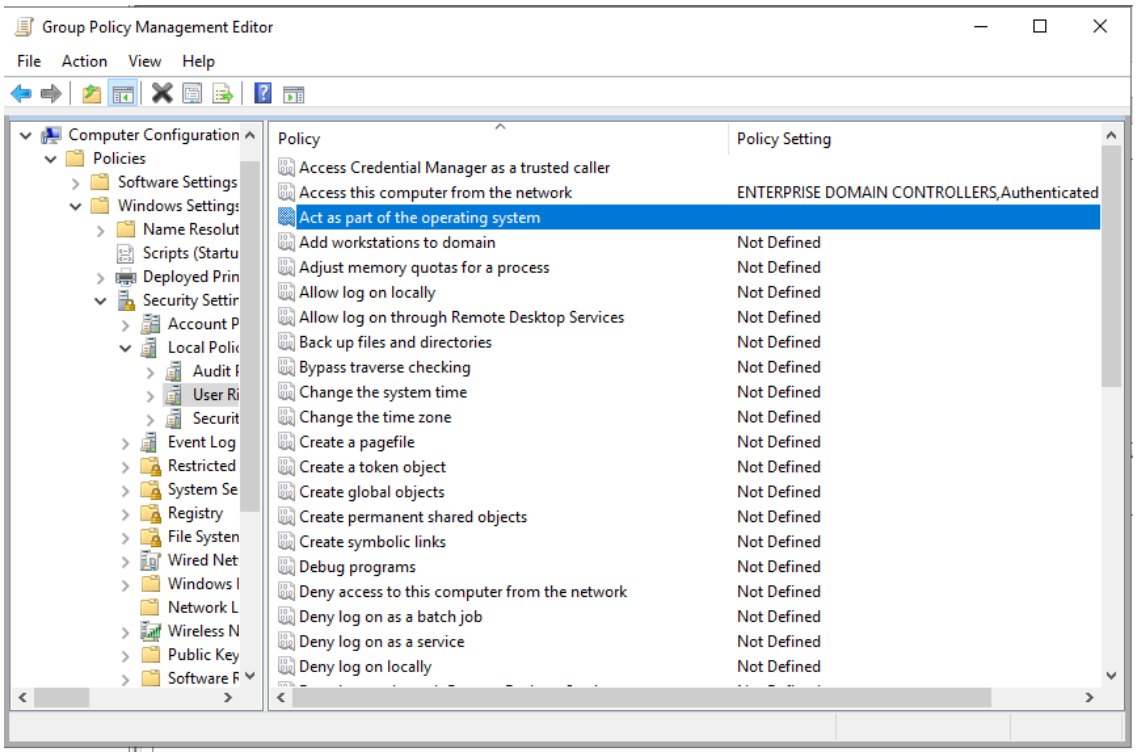


Image 13- Ensure 'Act as part of the operating system' is set to 'No One'

3.1.4 Ensure 'Add workstations to domain' is set to 'Administrators'

This policy determines who can add computer workstations to the domain. It must be assigned in the Default Domain Controller Policy. Users with this right can add up to 10 workstations. However, those with the Create Computer Objects permission can add unlimited computers, regardless of this policy. In Windows networks, a security principal includes users, groups, or computers with assigned security identifiers for resource access. Each computer account in Active Directory functions as a full security principal, capable of authentication and accessing domain resources. However, organizations may want to limit computer additions to maintain consistency in tracking, building, and managing computers. Allowing users to add computers can hinder tracking and management efforts and may lead to unauthorized computer creations that are difficult to trace.

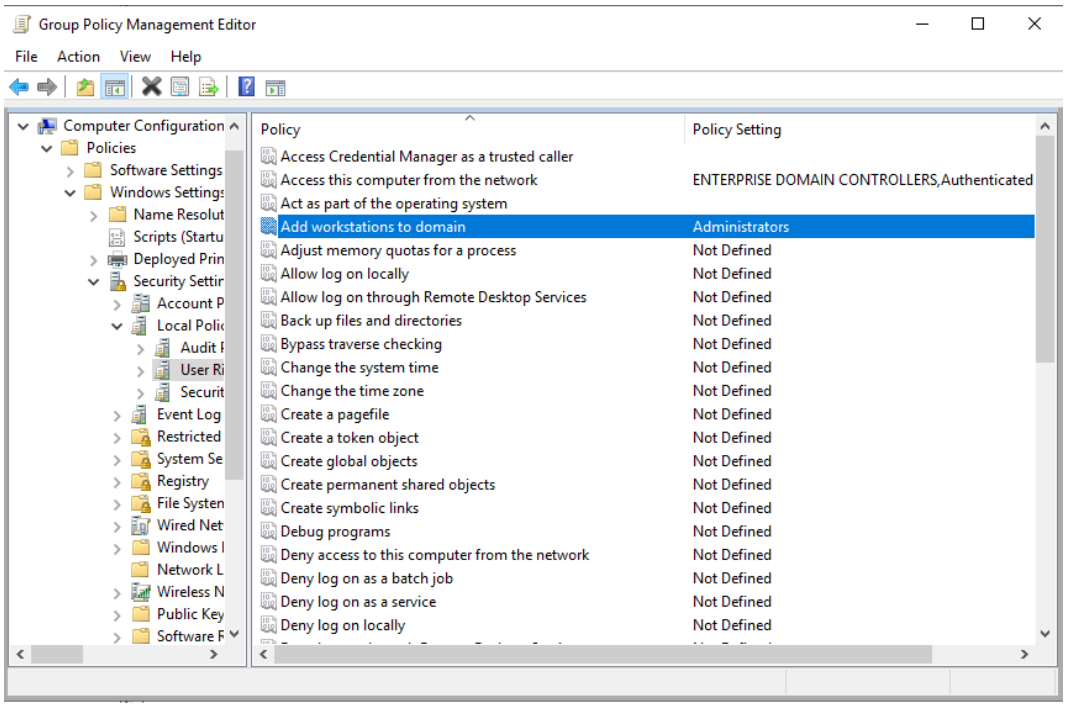


Image 14- Ensure 'Add workstations to domain' is set to 'Administrators'

3.1.5 Ensure Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE'

This policy setting permits a user to modify the maximum memory available to a process. While adjusting memory quotas is valuable for system optimization, it also poses risks. In the hands of unauthorized users, it could potentially be exploited to initiate a denial of service (DoS) attack.

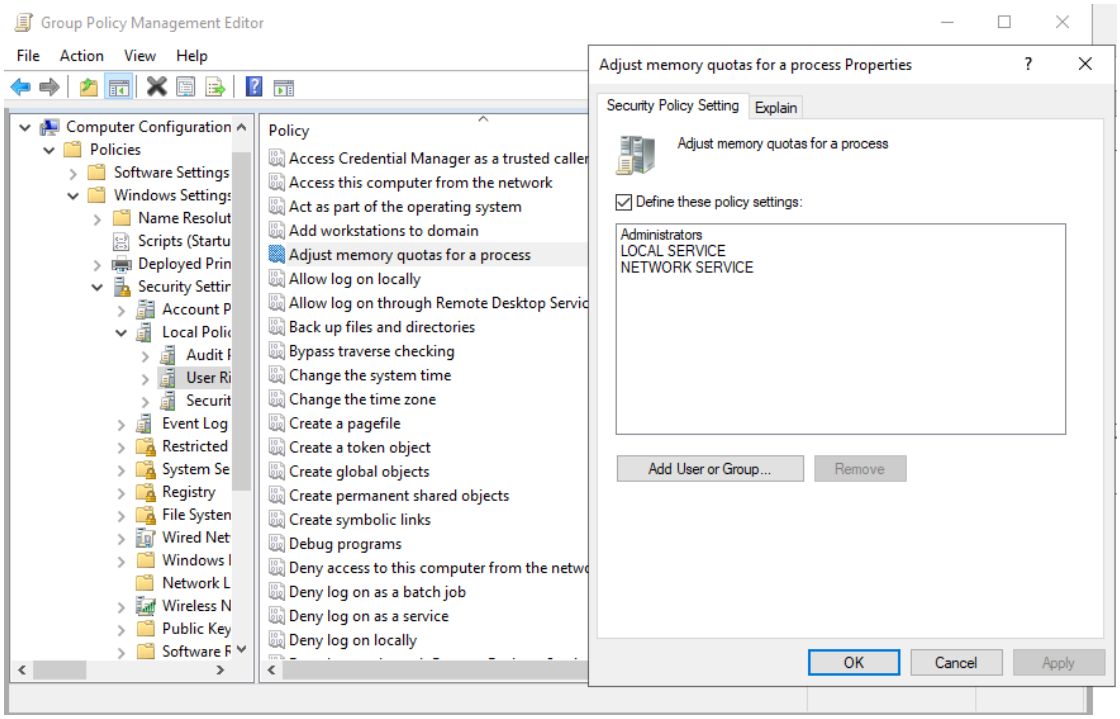


Image 15- Ensure 'Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE'

3.1.6 Ensure 'Allow log on locally' is set to 'Administrators'

This policy setting dictates the users authorized to perform interactive logons on computers within your environment. Such logons, initiated by pressing the CTRL+ALT+DEL key sequence on the client computer keyboard, necessitate this user right. Additionally, users attempting to log on through Terminal Services/Remote Desktop Services or IIS also need this user right.

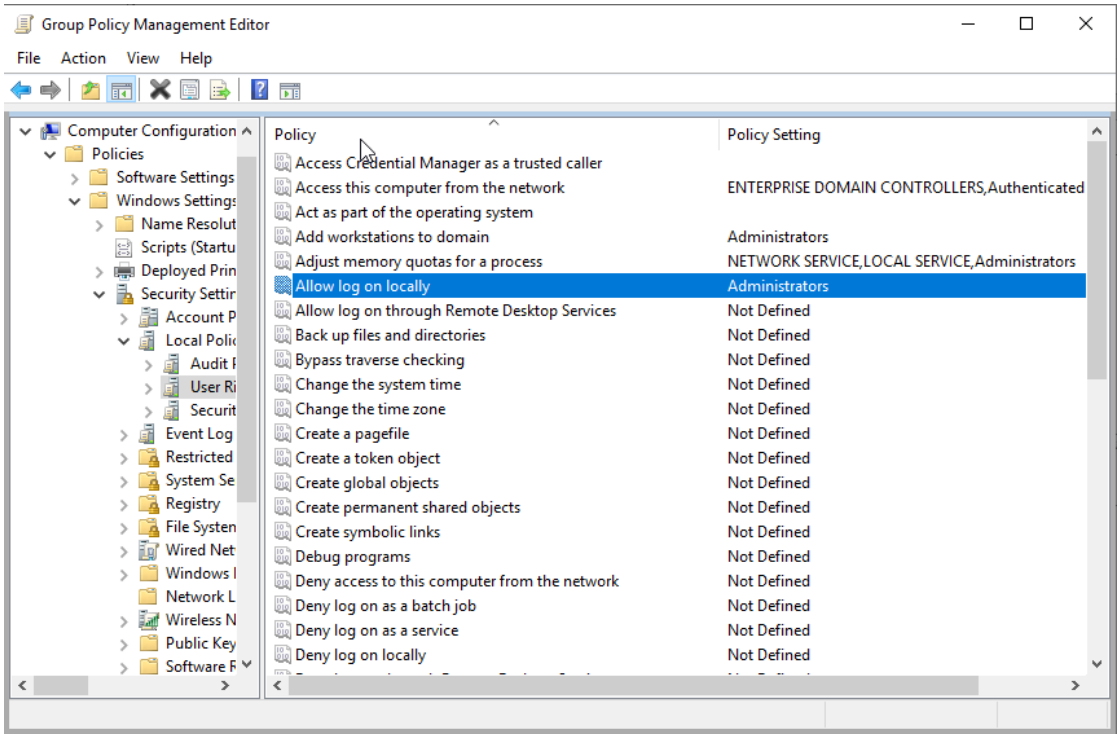


Image 16-Ensure 'Allow log on locally' is set to 'Administrators'

3.1.7 Ensure 'Allow log on through Remote Desktop Services' is set to 'Administrators'

This policy setting determines the users or groups authorized to log on as Remote Desktop Services clients. If Remote Assistance is utilized in your organization's help desk strategy, it's recommended to create a dedicated group and assign this user right through Group Policy. Alternatively, if Remote Assistance isn't utilized, restrict this user right solely to the Administrators group, or utilize the Restricted Groups feature to ensure no user accounts belong to the Remote Desktop Users group. Limiting this user right to the Administrators group, and possibly the Remote Desktop Users group, helps prevent unauthorized users from accessing network computers through the Remote Assistance feature.

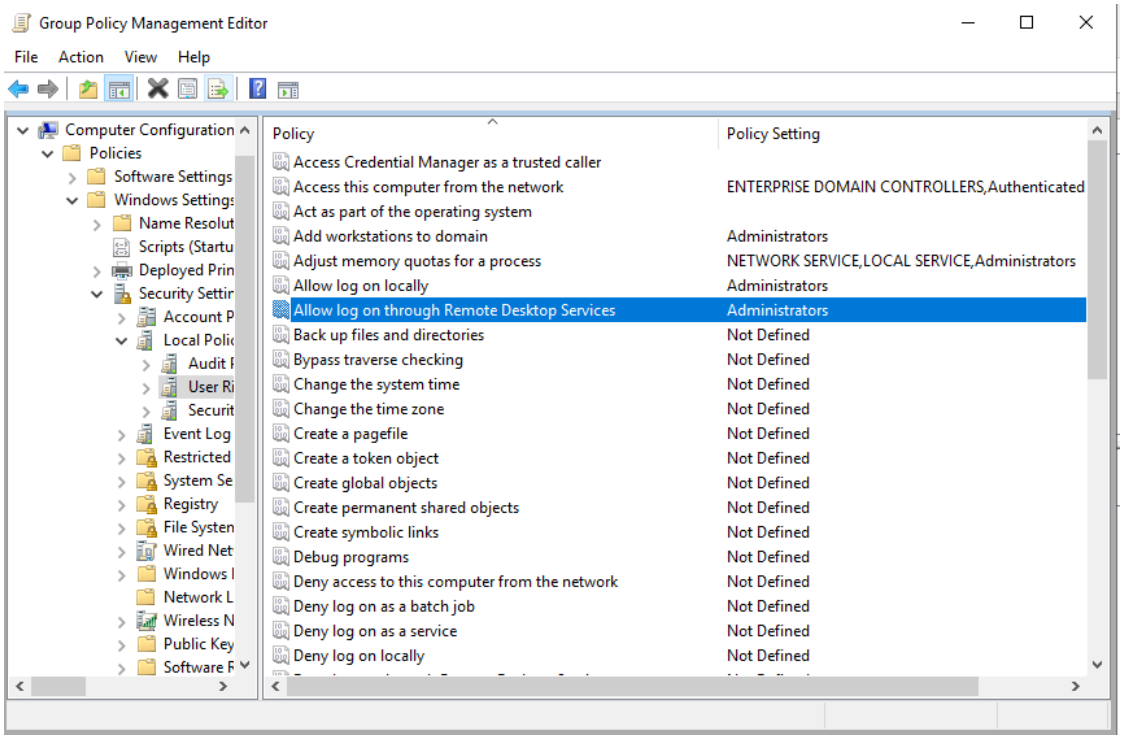


Image 17-Ensure 'Allow log on through Remote Desktop Services' is set to 'Administrators'

3.1.8 Ensure Back up files and directories' is set to 'Administrators'

This policy setting grants users the ability to bypass file and directory permissions for system backup purposes. It becomes active exclusively when an application, like NTBACKUP, seeks to access a file or directory using the NTFS file system backup application programming interface (API). Otherwise, the existing file and directory permissions remain in effect.

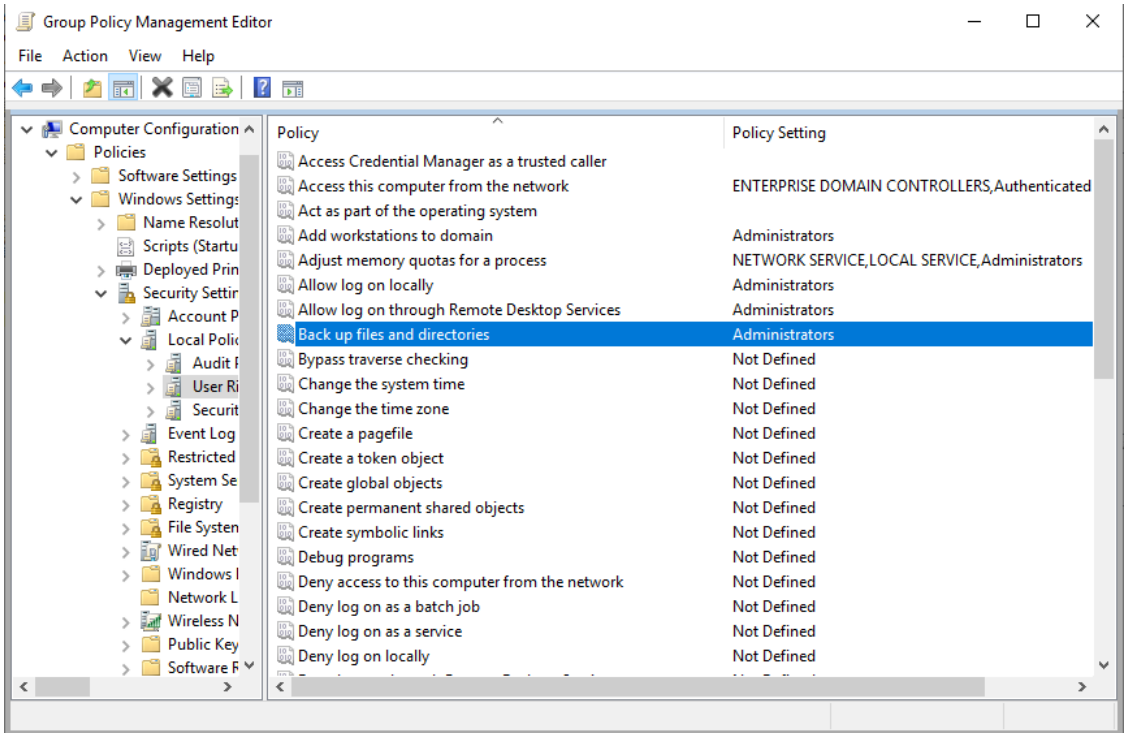


Image 18-Ensure 'Back up files and directories' is set to 'Administrators'

3.1.9 Ensure 'Change the system time' is set to 'Administrators, LOCAL SERVICE'

This policy setting dictates the users and groups authorized to modify the time and date settings on computers within your environment. Users with this user right can influence the timestamps of event logs. Changing a computer's time setting results in event logs displaying the modified time, rather than the actual time when the events took place.

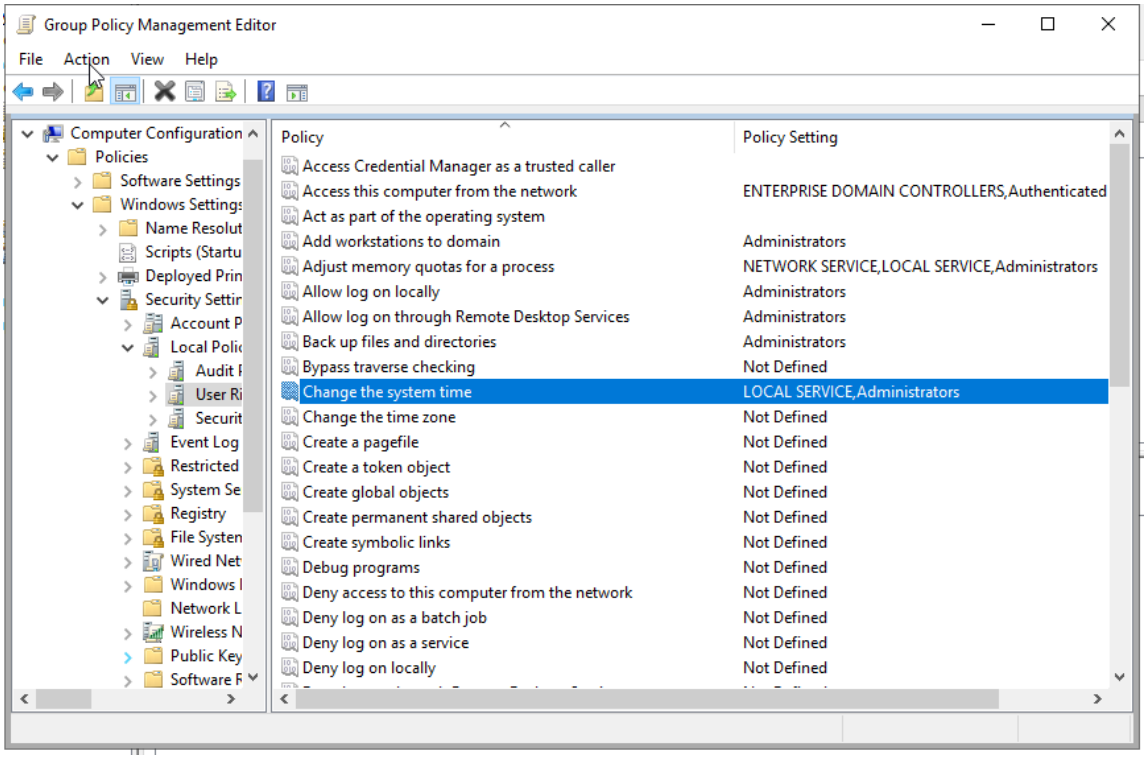


Image 19-Ensure 'Change the system time' is set to 'Administrators, LOCAL SERVICE'

3.1.10 Ensure 'Change the time zone' is set to 'Administrators, LOCAL SERVICE'

This setting determines the users authorized to modify the time zone of the computer. This capability poses minimal risk to the computer and can be beneficial for mobile workers.

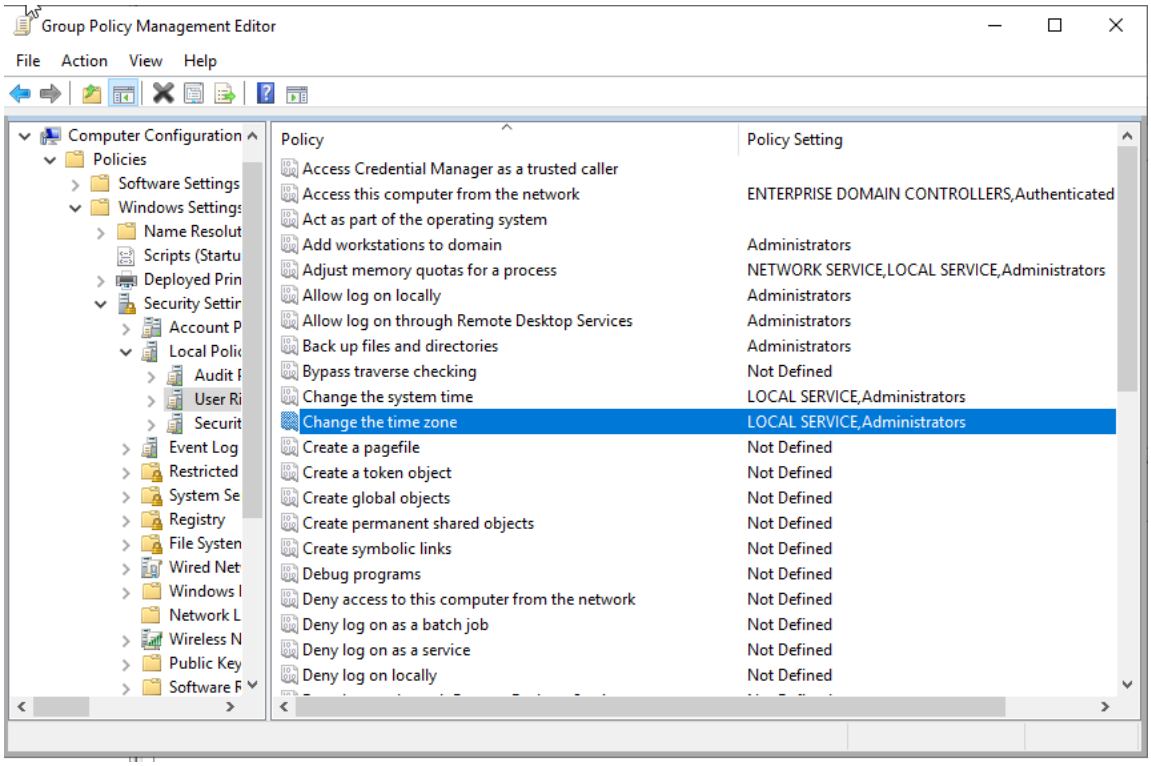


Image 20-Ensure 'Change the time zone' is set to 'Administrators, LOCAL SERVICE'

3.1.11 Ensure 'Create a pagefile' is set to 'Administrators'

This policy setting permits users to adjust the size of the pagefile. However, setting the pagefile size to extremes—either very large or very small—could significantly impact the performance of a compromised computer, potentially exploited by attackers.

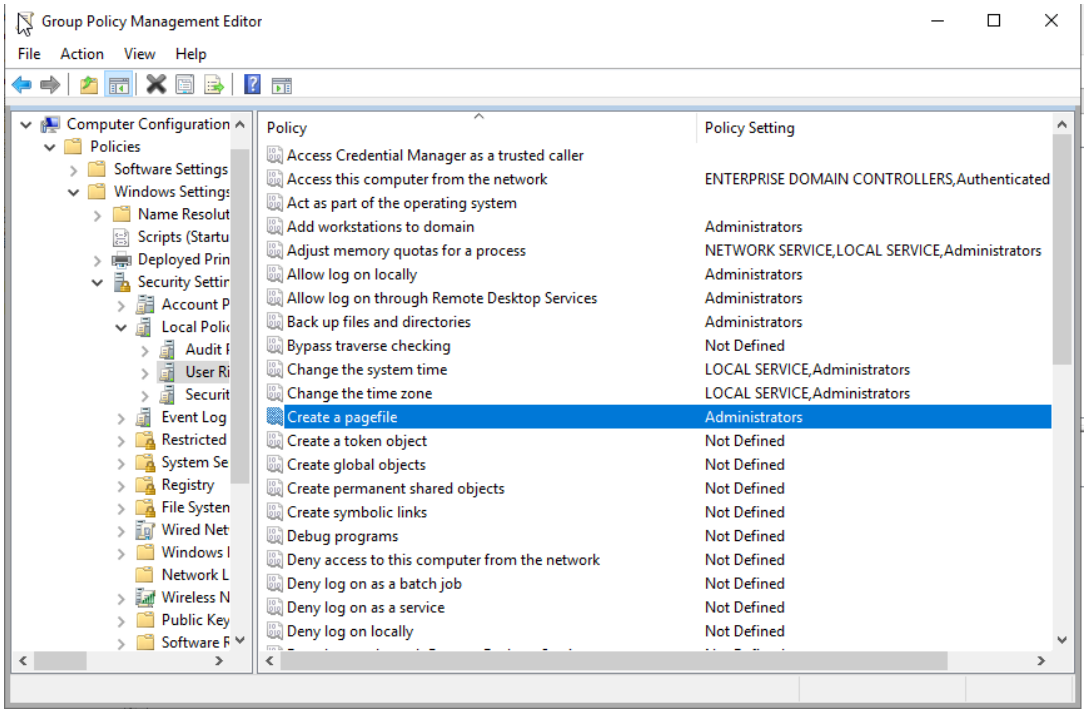


Image 21-Ensure 'Create a pagefile' is set to 'Administrators'

3.1.12 Ensure 'Create a token object' is set to 'No One'

This policy setting permits a process to generate an access token, potentially granting elevated privileges to access sensitive information.

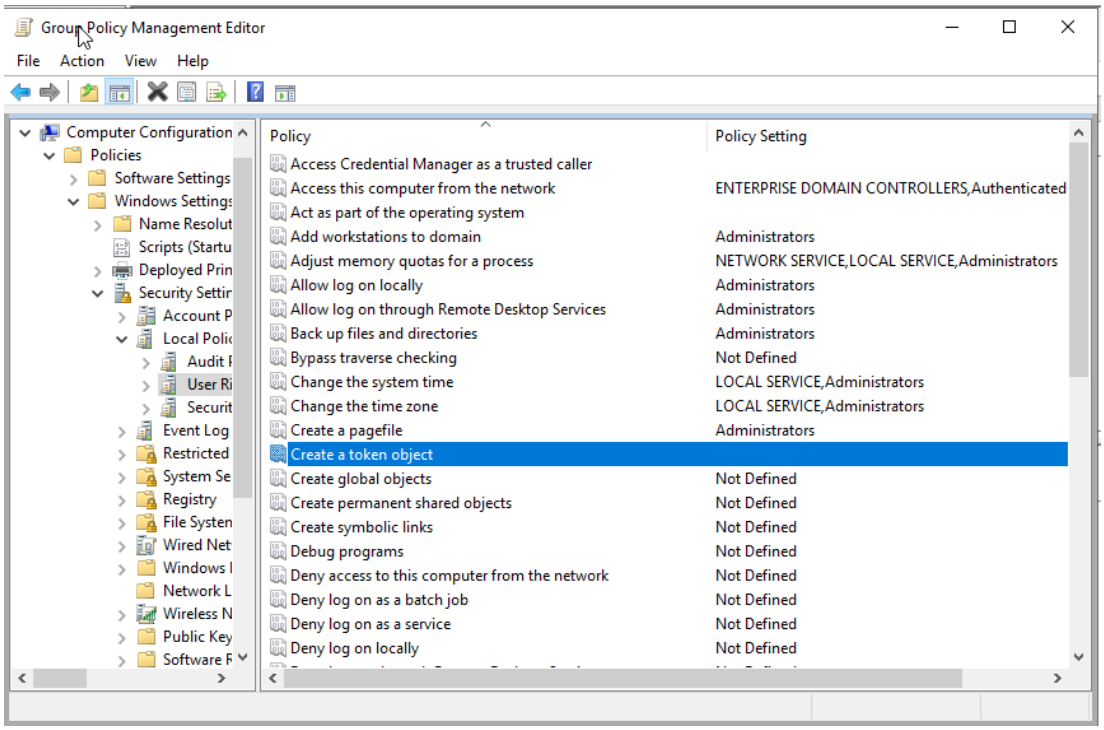


Image 22-Ensure 'Create a token object' is set to 'No One'

3.1.13 Ensure 'Create global objects' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE'

This policy setting governs whether users can generate global objects accessible across all sessions. Without this user right, users can still create objects limited to their own session. Allowing users to create global objects may impact processes in other users' sessions, potentially resulting in issues like application failures or data corruption.

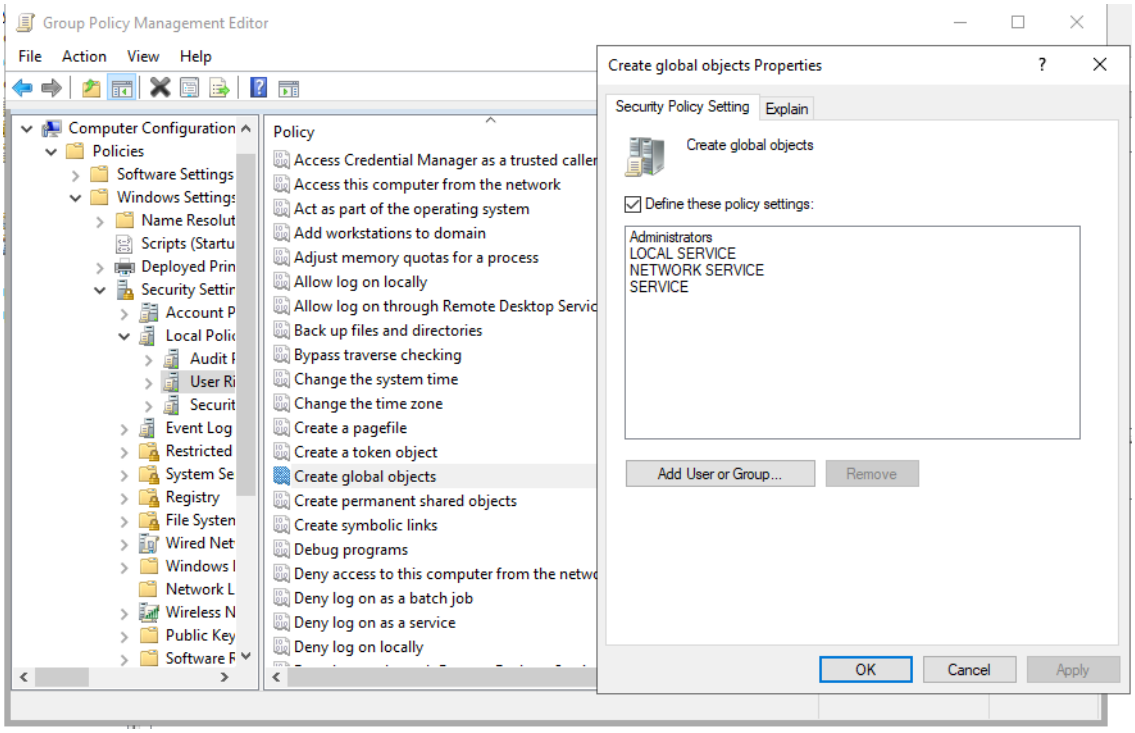


Image 23-Ensure 'Create global objects' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE'

3.1.14 Ensure Create permanent shared objects' is set to 'No One'

This user right is valuable for kernel-mode components that expand the object namespace. However, since components operating in kernel mode automatically possess this user right, it's usually unnecessary to explicitly assign it.

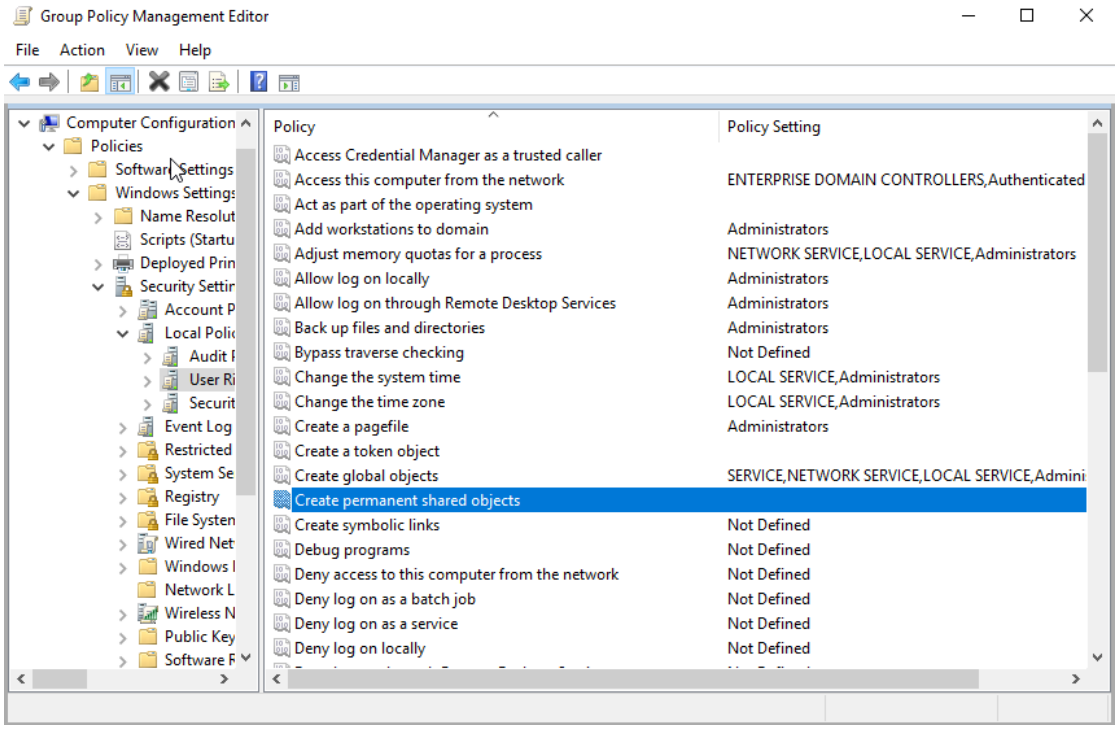


Image 24-Ensure 'Create permanent shared objects' is set to 'No One'

3.1.15 Ensure ‘Create symbolic links' is set to 'Administrators'

This policy setting governs which users have the ability to create symbolic links. In Windows Vista, symbolic links introduce a new way to access existing NTFS file system objects, like files and folders. Symbolic links act as pointers, similar to shortcuts, directing to another file system object, which could be a file, folder, shortcut, or another symbolic link. Unlike shortcuts, which are exclusive to the Windows shell, symbolic links are a feature of the NTFS file system, accessible to all programs and applications.

However, because symbolic links can potentially introduce security vulnerabilities in applications not designed to use them, it's crucial to restrict the privilege of creating them to trusted users. By default, only Administrators have this capability.

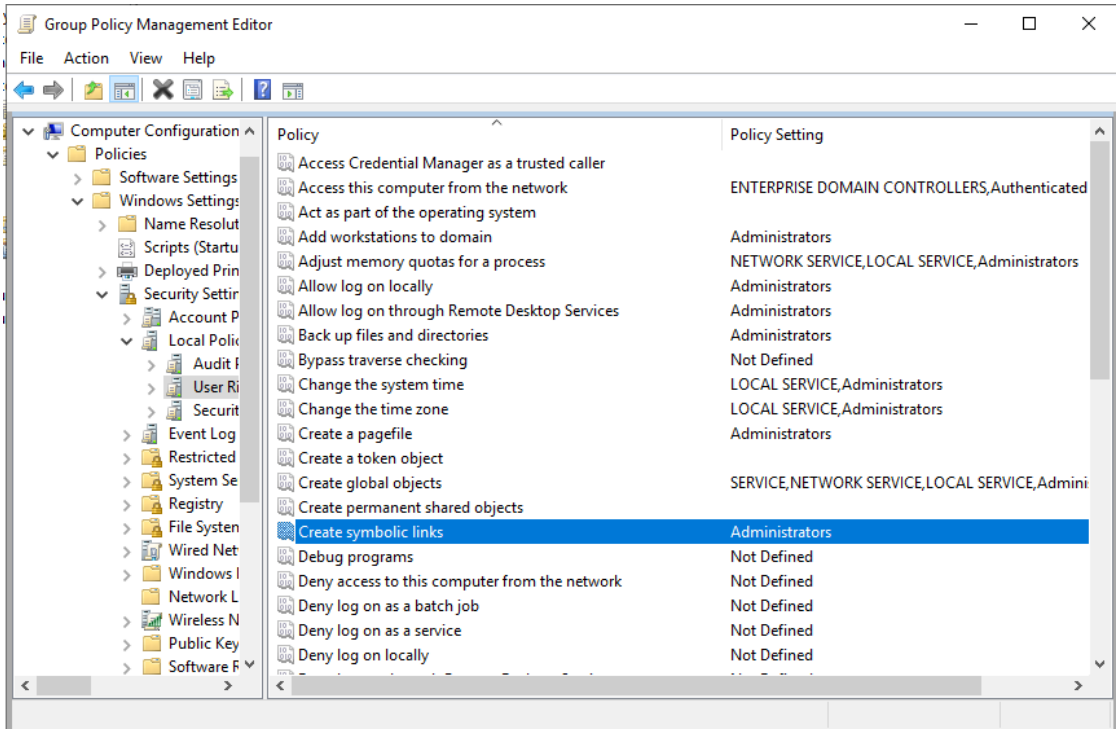


Image 25-Ensure 'Create symbolic links' is set to 'Administrators'

3.1.16 Ensure 'Debug programs' is set to 'Administrators'

This policy setting dictates which user accounts possess the privilege to connect a debugger to any process or the kernel, granting full access to sensitive and crucial operating system elements. While developers debugging their own applications do not require this user right, those debugging new system components will need it.

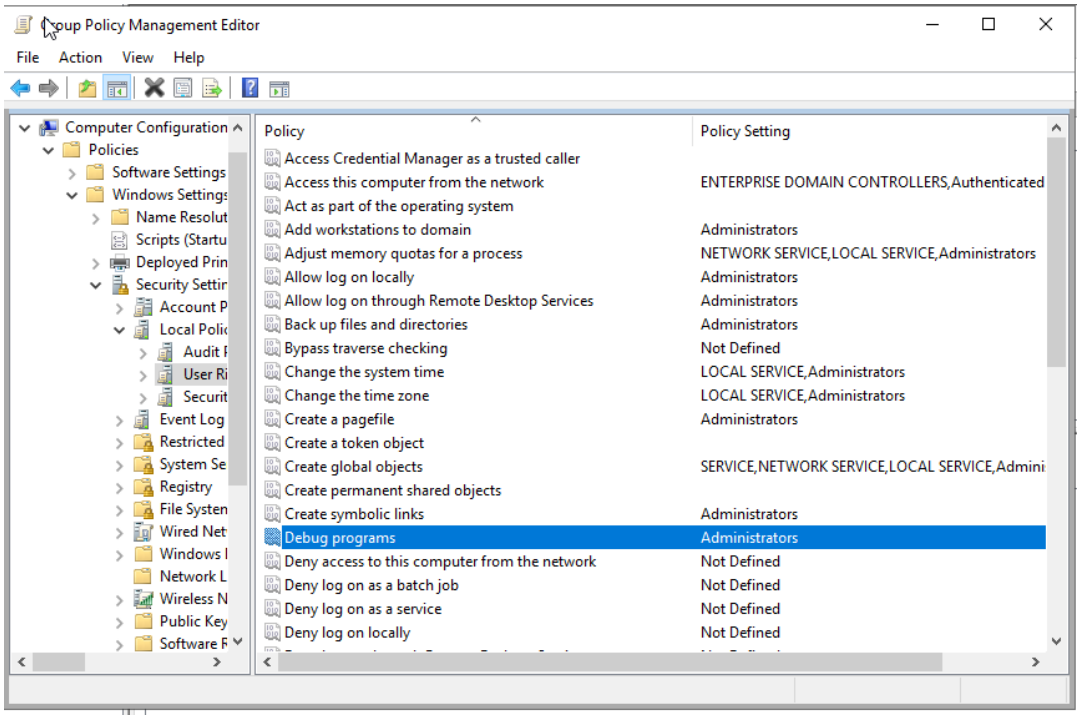


Image 26-Ensure 'Debug programs' is set to 'Administrators'

3.1.17 Ensure ‘Deny access to this computer from the network' to include 'Guests'

This policy setting blocks users from remotely connecting to a computer over the network, preventing potential unauthorized access and modification of data. In highly secure environments, remote access to computer data should be unnecessary, with file sharing handled via network servers instead. If an account is subject to both policies, this user right takes precedence over the "Access this computer from the network" user right.

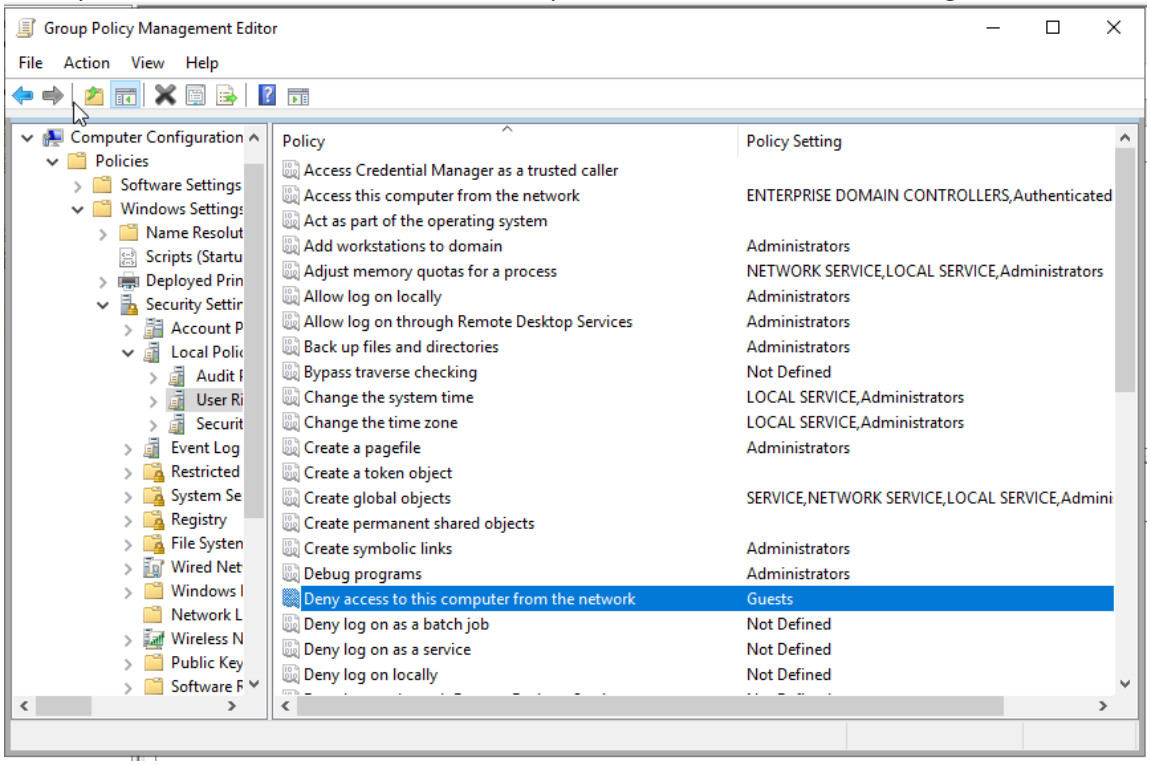


Image 27-Ensure 'Deny access to this computer from the network' to include 'Guests'

3.1.18 Ensure 'Deny log on as a batch job' to include 'Guests'

This policy setting specifies which accounts are prohibited from logging on to the computer as a batch job. A batch job refers to a batch-queue facility rather than a batch (.bat) file. Accounts using the Task Scheduler to plan tasks require this user right. This right overrides the "Log on as a batch job" user right, which could otherwise permit accounts to schedule jobs that excessively use system resources, potentially leading to a Denial of Service (DoS) situation. Not granting this user right to the recommended accounts can pose a security risk.

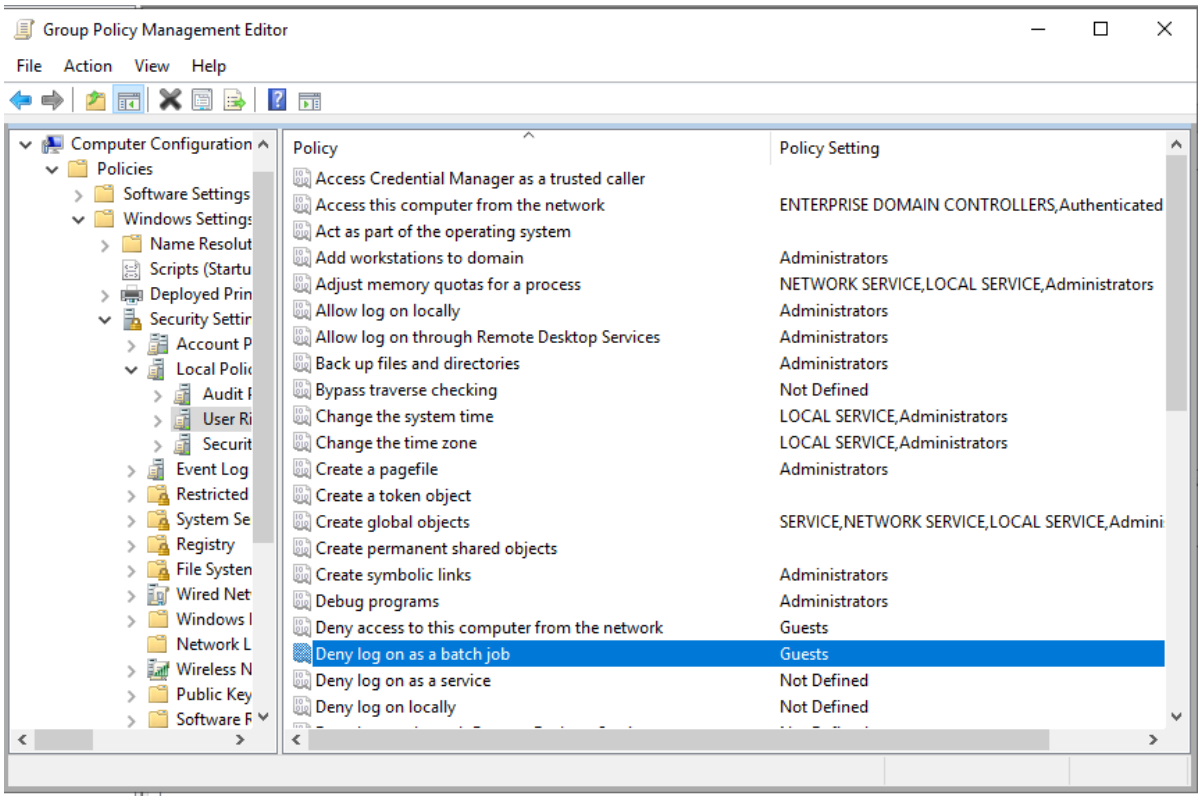


Image 28-Ensure 'Deny log on as a batch job' to include 'Guests'

3.1.19 Ensure 'Deny log on as a service' to include 'Guests'

This security setting specifies which service accounts are prevented from registering a process as a service, overriding the "Log on as a service" user right if an account is subject to both policies. It is recommended to include Guests in this setting. Note that this setting does not apply to the System, Local Service, or Network Service accounts. The rationale is that accounts with the ability to log on as a service could configure and start unauthorized services, such as keyloggers or other malicious software. However, this risk is somewhat mitigated by the fact that only users with administrative privileges can install and configure services, and an attacker with such access could configure the service to run with the System account. The impact of assigning the "Deny log on as a service" user right to specific accounts is that services may not start, potentially resulting in a Denial of Service (DoS) condition.

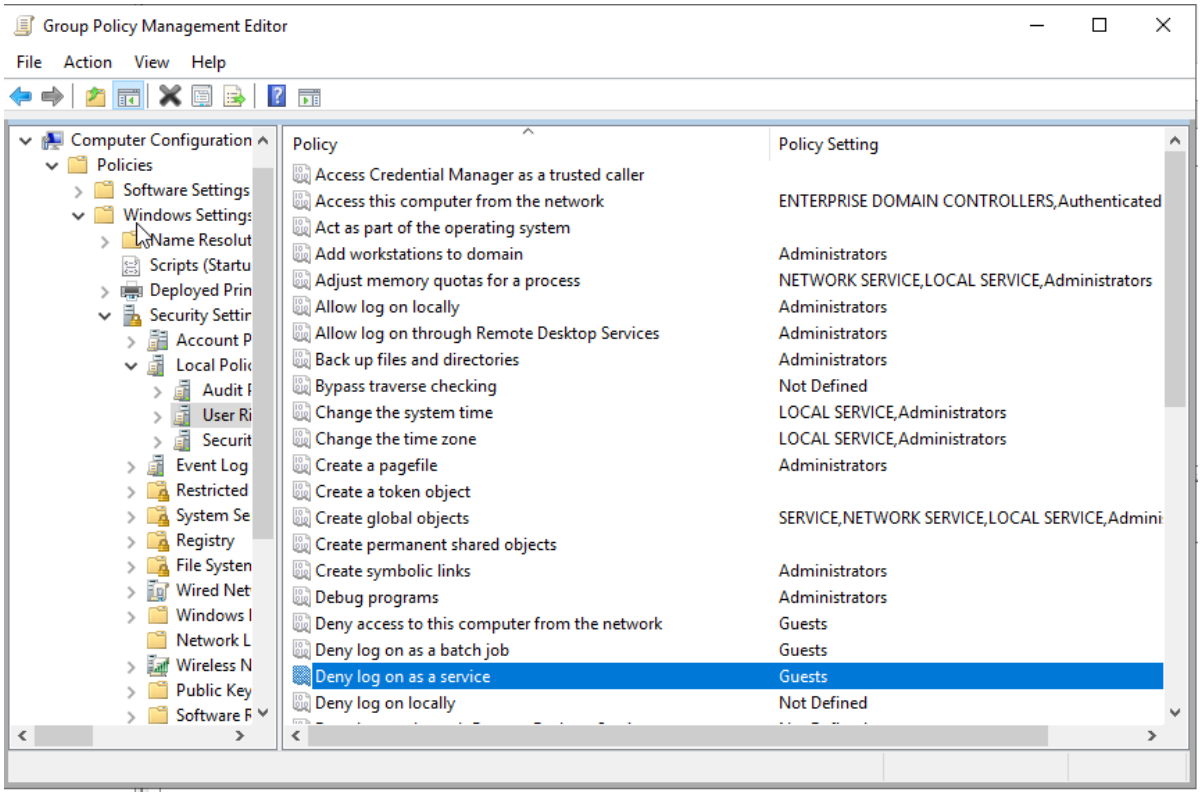


Image 29-Ensure 'Deny log on as a service' to include 'Guests'

3.1.20 Ensure 'Deny log on locally' to include 'Guests'

This security setting specifies which users are prevented from logging on to the computer locally, overriding the "Allow log on locally" policy if both apply to an account. It is recommended to include Guests in this setting. Note that applying this policy to the Everyone group will prevent all local logins. Allowing any account to log on locally can enable unauthorized access to the computer's console, where malicious software could be downloaded and executed to elevate privileges. Restricting the "Deny log on locally" user right to additional accounts might limit the capabilities of users assigned to specific roles. However, this right should be explicitly assigned to the ASPNET account on computers running IIS 6.0. Ensure that delegated activities are not negatively impacted.

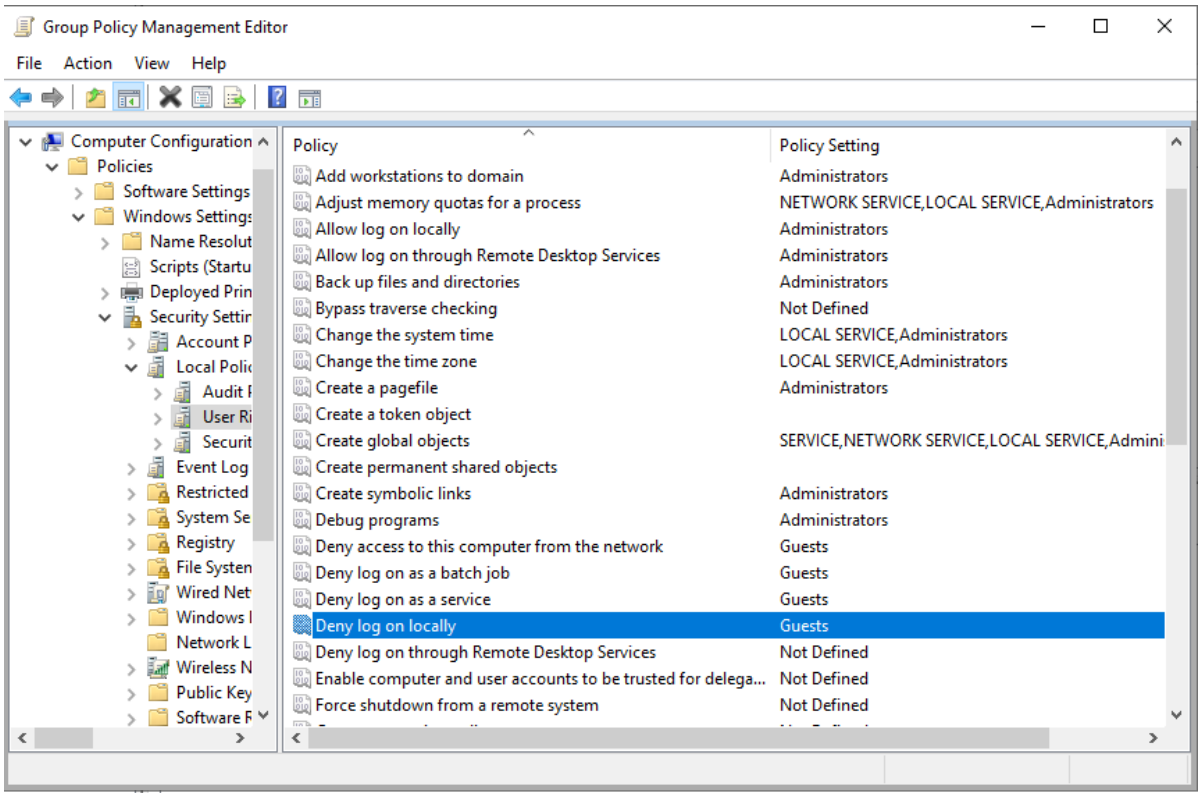


Image 30-Ensure 'Deny log on locally' to include 'Guests'

3.1.21 Ensure 'Deny log on through Remote Desktop Services' to include 'Guests'

This policy setting determines whether users can log on as Remote Desktop clients, overriding the "Allow log on through Remote Desktop Services" user right if both apply. It is recommended to include Guests in this setting. After a Member Server is joined to a domain, local accounts are unnecessary for network access; domain accounts suffice for administration and end-user processing. Allowing any account to log on through Remote Desktop Services can enable unauthorized access to the remote console, where malicious software could be downloaded and executed to elevate privileges. Restricting the "Deny log on through Remote Desktop Services" user right to additional groups might limit the capabilities of users in specific administrative roles, preventing those accounts from connecting through Remote Desktop Services or Remote Assistance. Ensure that delegated tasks are not adversely affected.

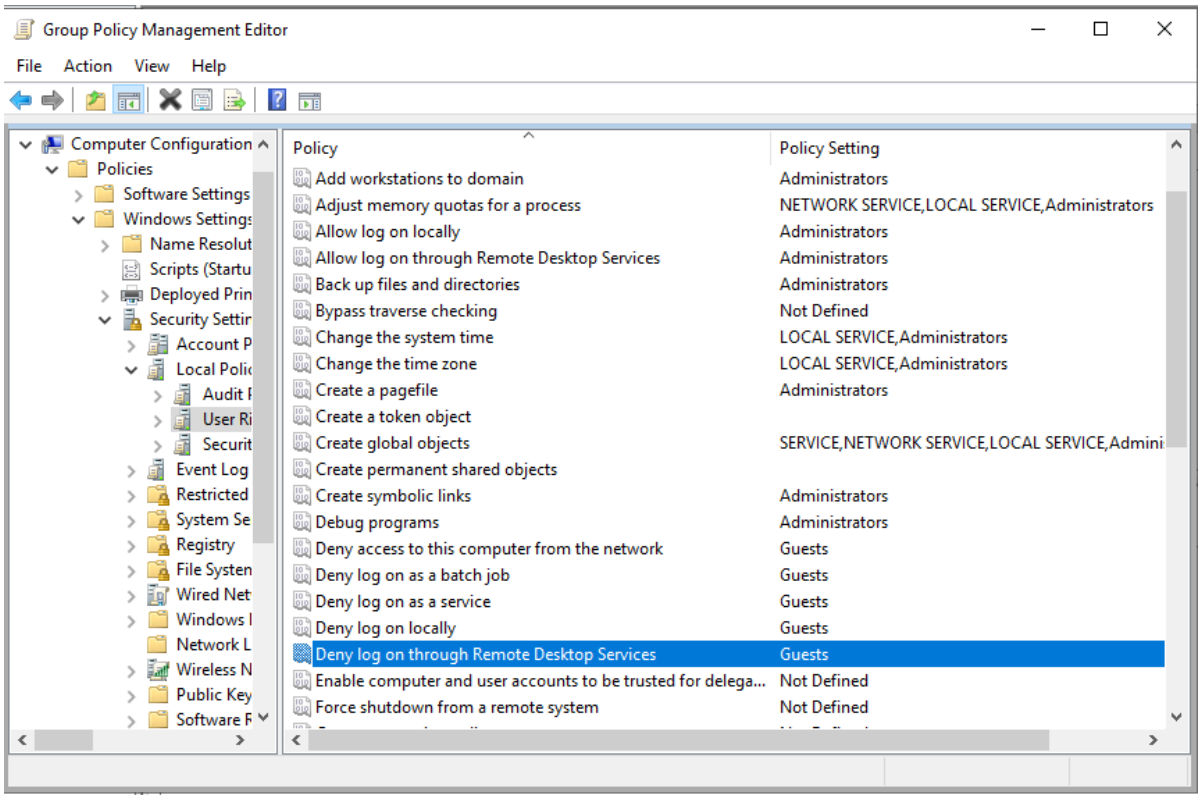


Image 31-Ensure 'Deny log on through Remote Desktop Services' to include 'Guests'

3.1.22 Ensure 'Enable computer and user accounts to be trusted for delegation' is set to 'Administrators'

This policy setting allows users to change the "Trusted for Delegation" setting on a computer object in Active Directory. Misuse of this privilege could enable unauthorized users to impersonate others on the network. The recommended setting is to grant this privilege to Administrators only. This user right is considered a "sensitive privilege" for auditing purposes. Unauthorized use of the "Enable computer and user accounts to be trusted for delegation" user right could allow attackers to access network resources and complicate post-incident investigations.

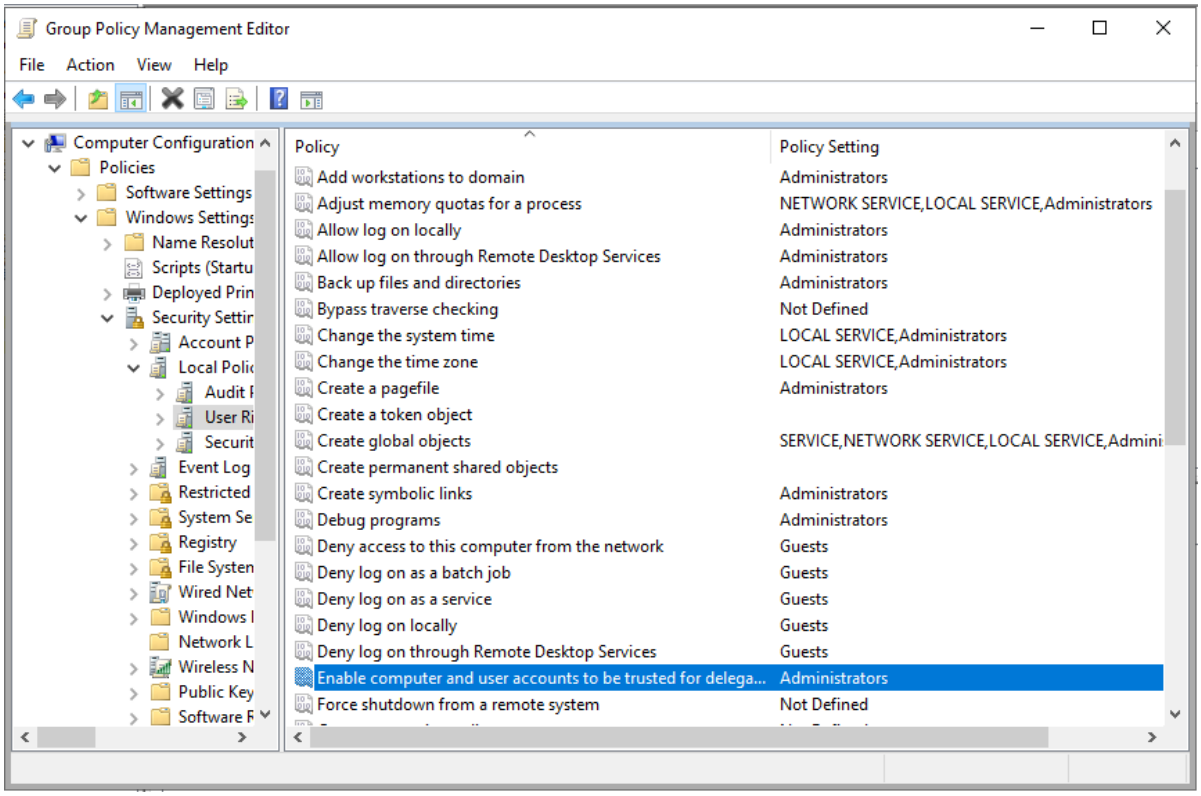


Image 32-Ensure 'Enable computer and user accounts to be trusted for delegation' is set to 'Administrators'

3.1.23 Ensure 'Force shutdown from a remote system' is set to 'Administrators'

This policy setting allows users to shut down Windows Vista-based or newer computers remotely. Granting this user right can lead to a denial of service (DoS) condition, making the computer unavailable for user requests. Therefore, it is recommended that only highly trusted administrators be assigned this user right. The recommended state for this setting is Administrators. Any user with the ability to shut down a computer could cause a DoS condition, so this user right should be tightly restricted. Removing the "Force shutdown from a remote system" user right from the Server Operators group could limit the capabilities of users in specific administrative roles. Ensure that delegated activities are not negatively impacted.

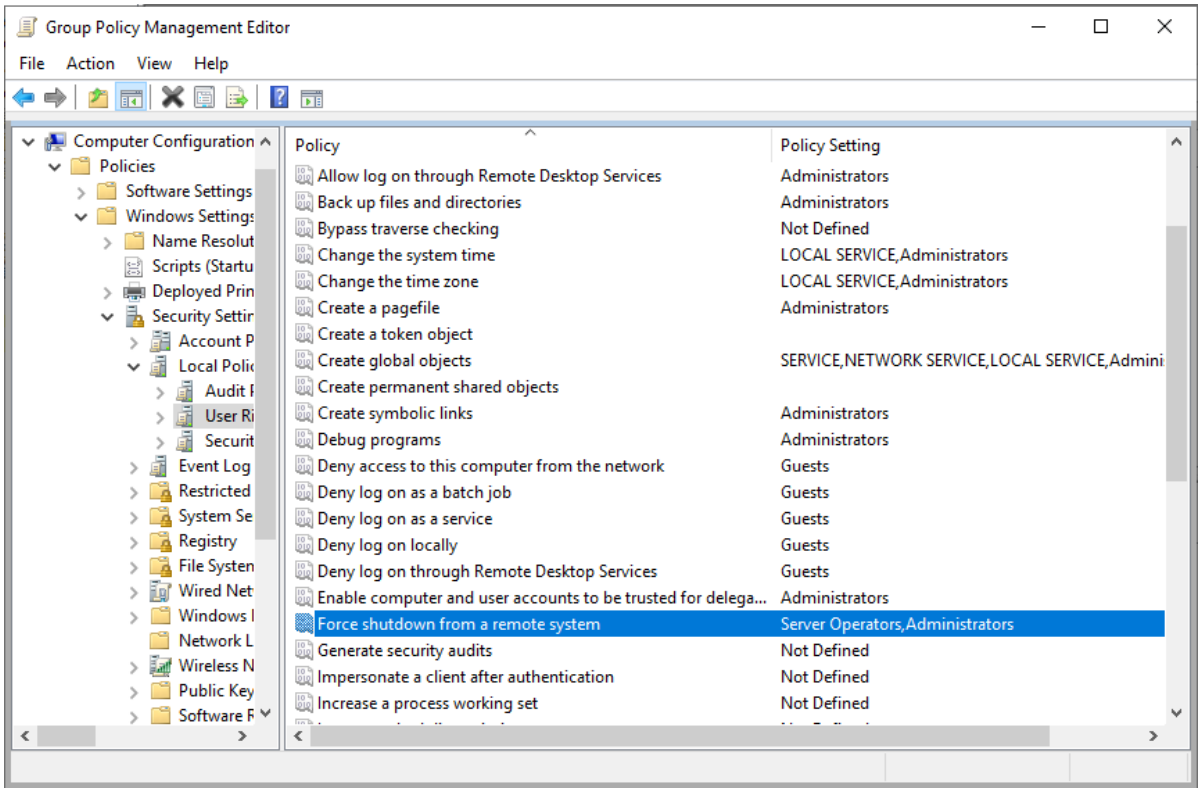


Image 33-Ensure 'Force shutdown from a remote system' is set to 'Administrators'

3.1.24 Ensure 'Generate security audits' is set to 'LOCAL SERVICE, NETWORK SERVICE'

This policy setting determines which users or processes can generate audit records in the Security log. The recommended state is to assign this right to LOCAL SERVICE and NETWORK SERVICE. This user right is considered a "sensitive privilege" for auditing purposes. Exceptions are necessary for Member Servers with the Web Server (IIS) Role to allow IIS application pools, and for those with the Active Directory Federation Services Role to allow the NT SERVICE\ADFSSrv and NT SERVICE\DRS services, as well as the Active Directory Federation Services service account, to have this right. An attacker could exploit this capability to generate numerous audit events, complicating the detection of illicit activity and potentially overwriting evidence of unauthorized actions. On most computers, this default configuration will have no negative impact, but special exceptions are required for servers with specific roles.

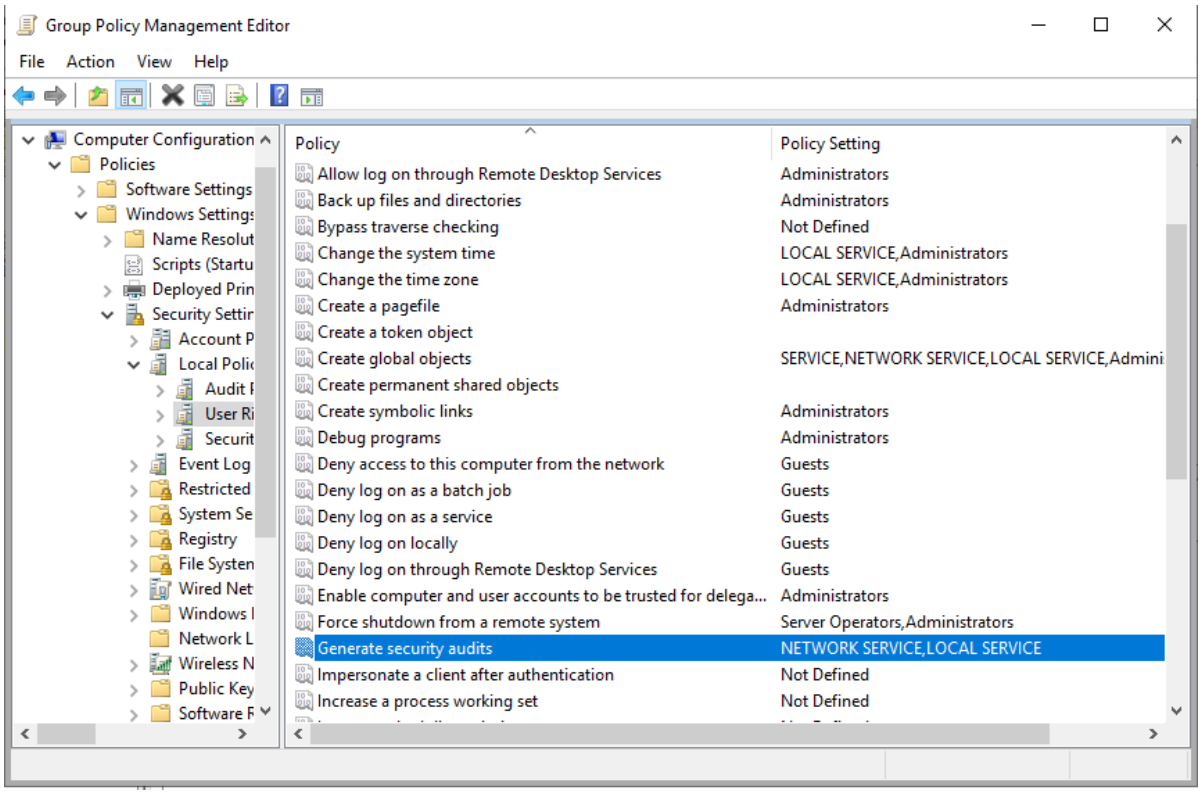


Image 34-Ensure 'Generate security audits' is set to 'LOCAL SERVICE, NETWORK SERVICE'

3.1.25 Ensure 'Impersonate a client after authentication' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE'

This policy setting allows programs running on behalf of a user to impersonate that user or another specified account. Without this right, unauthorized users cannot convince clients to connect to a service they created for impersonation, which could otherwise elevate their permissions to administrative or system levels. Services started by the Service Control Manager and COM servers configured to run under a specific account automatically have the Service group added to their access tokens, granting them this user right. Users can impersonate an access token if it belongs to them, if they logged on with explicit credentials, or if the requested level is less than Impersonate.

An attacker with the "Impersonate a client after authentication" right could create a service, trick clients into connecting, and then impersonate those clients to gain elevated access. The recommended state for this setting is to assign it to Administrators, LOCAL SERVICE, NETWORK SERVICE, and SERVICE. This user right is considered a "sensitive privilege" for auditing. Member Servers with Microsoft SQL Server and its "Integration Services" component require a special exception for additional SQL-generated entries.

This setting usually has no impact, but if the Web Server (IIS) Role with Web Services Role Service is installed, the right must also be assigned to IIS_IUSRS.

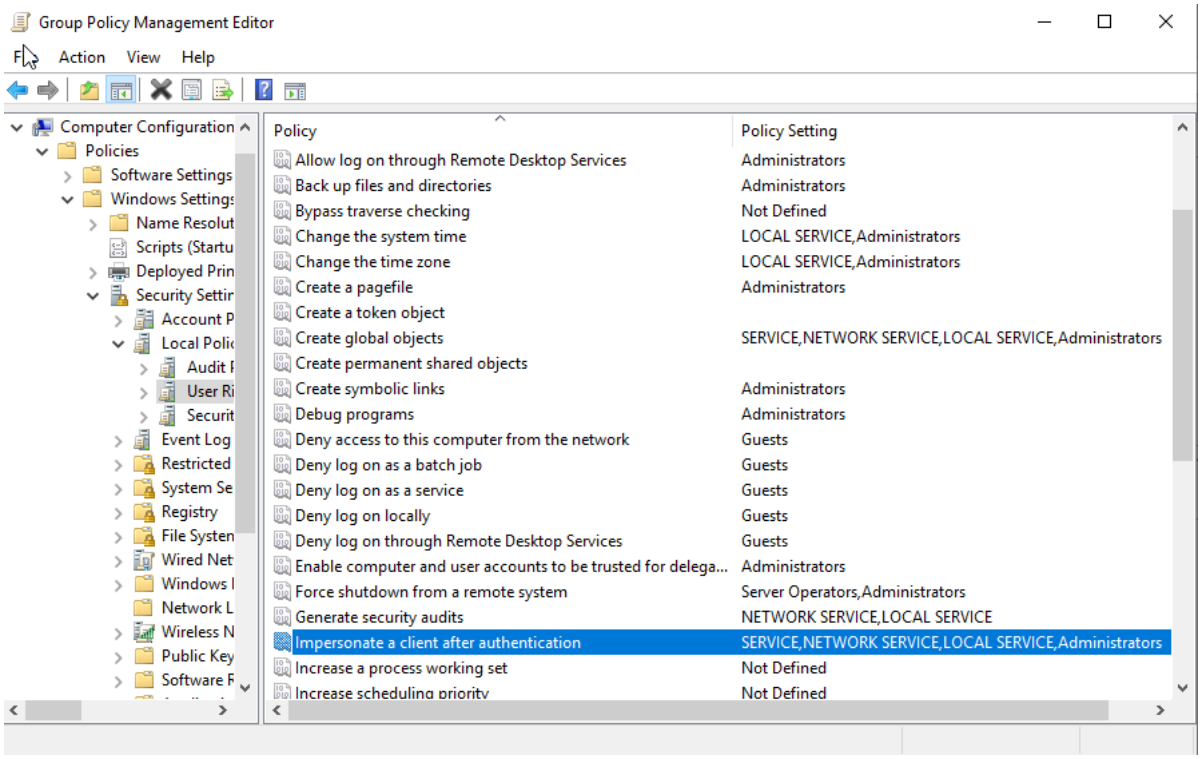


Image 35-Ensure 'Impersonate a client after authentication' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE'

3.1.26 Ensure 'Increase scheduling priority' is set to 'Administrators, Window Manager\Window Manager Group'

This policy setting controls whether users can raise the base priority class of a process. Note that it is not a privileged action to adjust relative priority within a priority class. While administrative tools supplied with the operating system do not require this user right, certain software development tools might. The recommended configuration is to assign this right to Administrators and the Window Manager\Window Manager Group. Allowing a user to increase a process's scheduling priority to Real-Time could reduce processing time available for other processes, potentially causing a Denial of Service (DoS) condition.

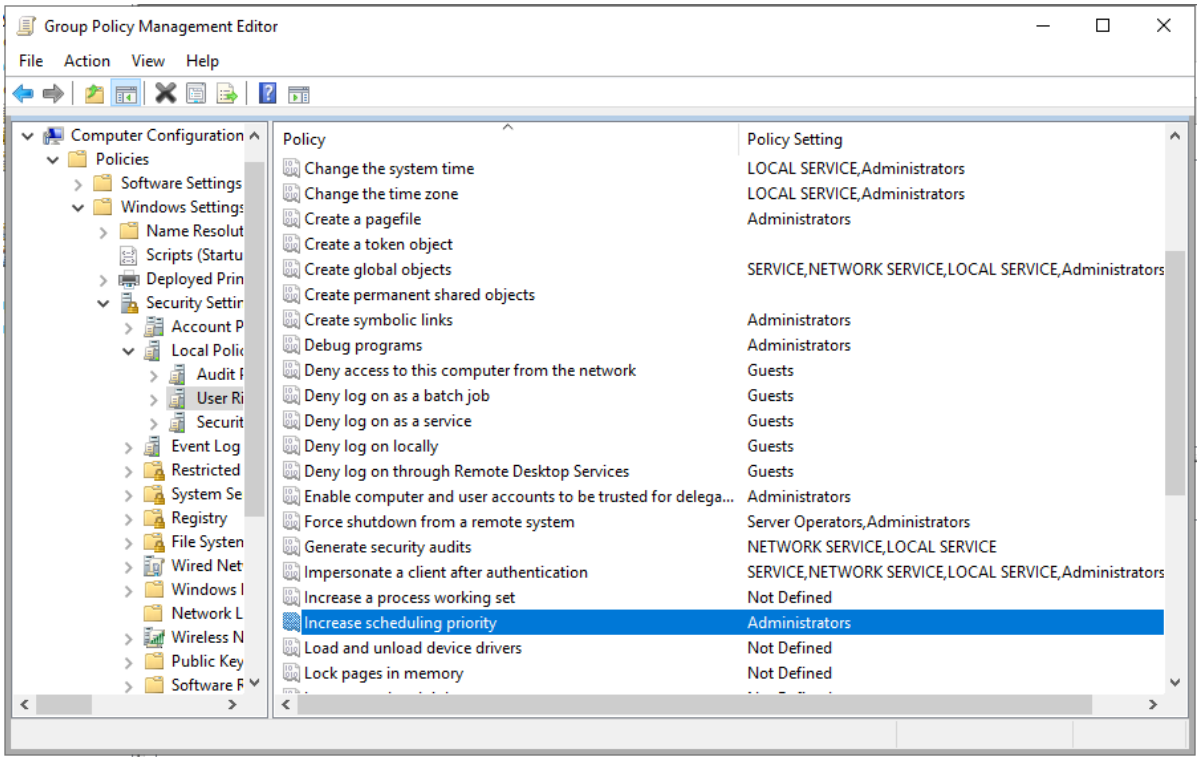


Image 36-Ensure 'Increase scheduling priority' is set to 'Administrators, Window Manager\Window Manager Group'

3.1.27 Ensure 'Load and unload device drivers' is set to 'Administrators'

This policy setting permits users to dynamically load a new device driver on a system, which could be exploited by an attacker to install malicious code disguised as a device driver. This right is needed for users to add local printers or printer drivers in Windows Vista. The recommended assignment for this setting is Administrators only. This user right is considered a "sensitive privilege" for auditing purposes.

Device drivers operate as highly privileged code, and users with the "Load and unload device drivers" right could unintentionally install malicious code. Administrators should ensure only drivers with verified digital signatures are installed. Removing this right from the Print Operators group or other accounts may limit certain administrative capabilities, so it is important to verify that delegated tasks are not adversely affected.

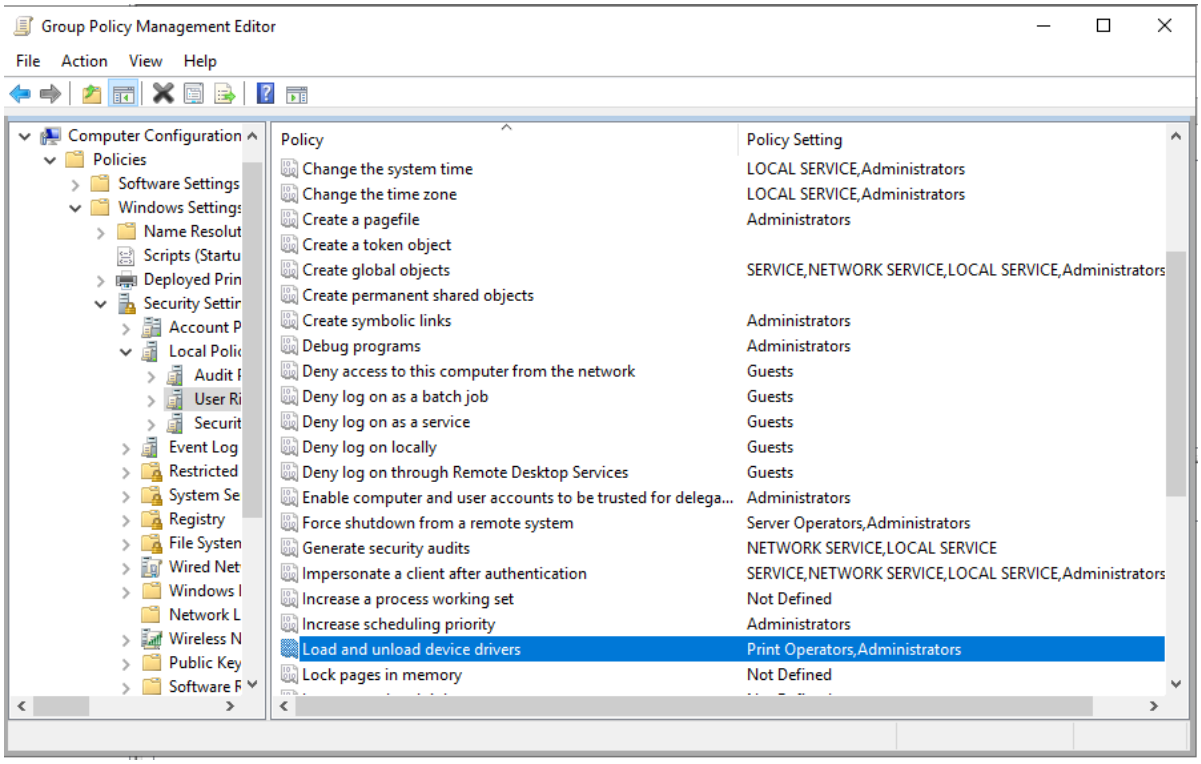


Image 37-Ensure 'Load and unload device drivers' is set to 'Administrators'

3.1.28 Ensure 'Lock pages in memory' is set to 'No One'

This policy setting allows a process to retain data in physical memory, preventing the system from paging the data to virtual memory on disk. Assigning this user right can significantly degrade system performance. The recommended configuration is to assign this right to no one. However, a Member Server with Microsoft SQL Server installed will require an exception to this recommendation for additional SQL-generated entries. Users with the "Lock pages in memory" right could allocate physical memory to several processes, potentially leaving insufficient RAM for other processes and causing a Denial of Service (DoS) condition.

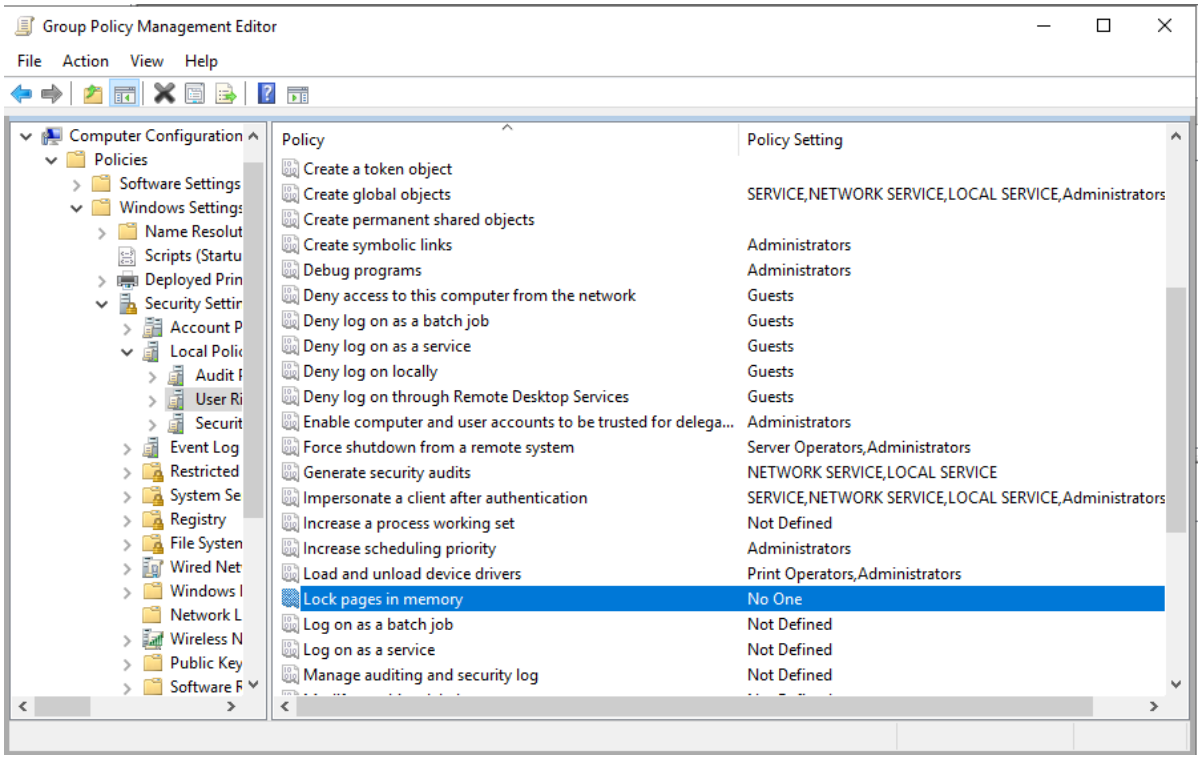


Image 38-Ensure 'Lock pages in memory' is set to 'No One'

3.1.29 Ensure 'Log on as a batch job' is set to 'Administrators'

This policy setting permits accounts to log on using the task scheduler service. While task scheduler is essential for administrative tasks in enterprise environments, its use should be limited in high-security settings to prevent misuse of system resources and to avoid attackers leveraging this right to execute malicious code after gaining user-level access. The recommended assignment for this setting is Administrators.
The "Log on as a batch job" user right is considered a low-risk vulnerability, and the default settings are usually adequate for most organizations. However, configuring this setting through domain-based Group Policies can prevent the computer from assigning this right to accounts needed for scheduled jobs in the Task Scheduler. If optional components like ASP.NET or IIS are installed, this right might need to be assigned to additional accounts such as IIS_WPG, IUSR_(ComputerName), ASPNET, and IWAM_(ComputerName). Without this right, IIS will be unable to run certain COM objects necessary for its functionality.

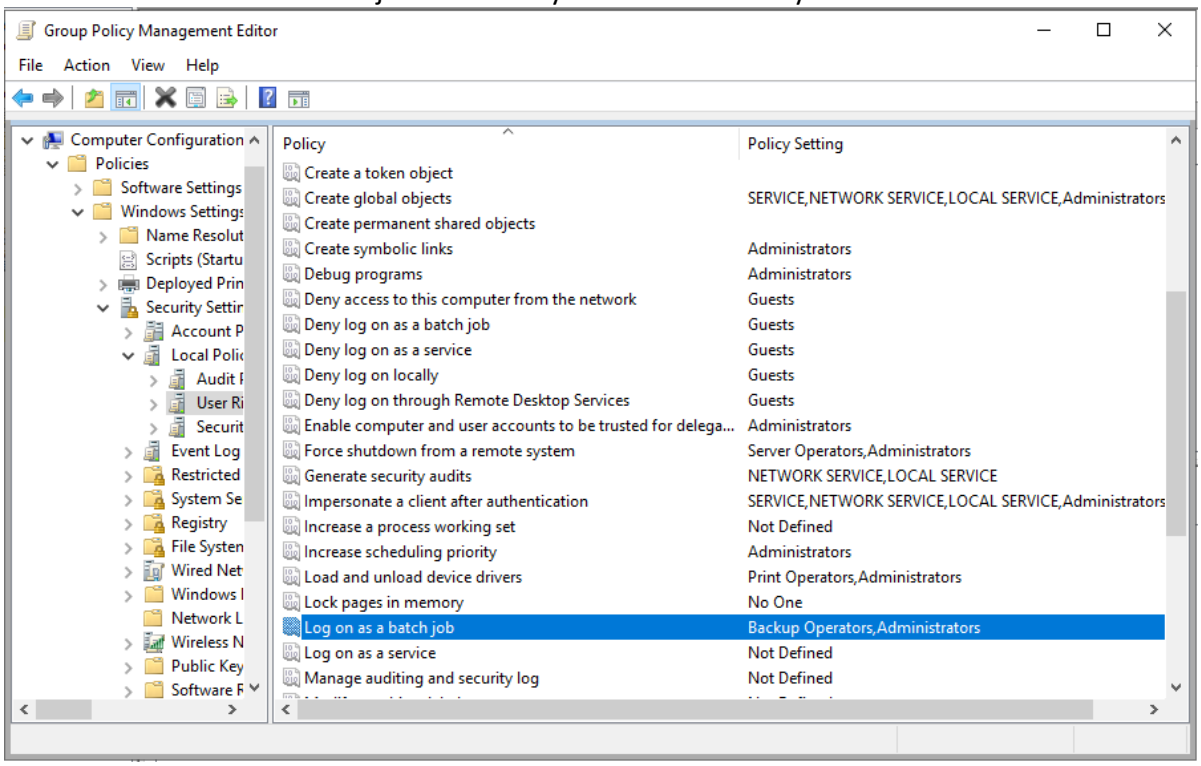


Image 39-Ensure 'Log on as a batch job' is set to 'Administrators'

3.1.30 Ensure 'Manage auditing and security log' is set to 'Administrators'

This policy setting specifies which users can modify auditing options for files and directories and clear the Security log. For environments with Microsoft Exchange Server, the Exchange Servers group must have this privilege on Domain Controllers (DCs) to function properly. In such cases, DCs granting this privilege to the Exchange Servers group meet the benchmark. In environments without Microsoft Exchange Server, this privilege should be restricted to Administrators on DCs. The recommended configuration is to assign this privilege to Administrators, and to Exchange Servers if Exchange is running in the environment. This user right is considered a "sensitive privilege" for auditing purposes. The ability to manage the Security event log is highly powerful and should be closely guarded, as it allows users to clear the Security log and potentially erase evidence of unauthorized activities.

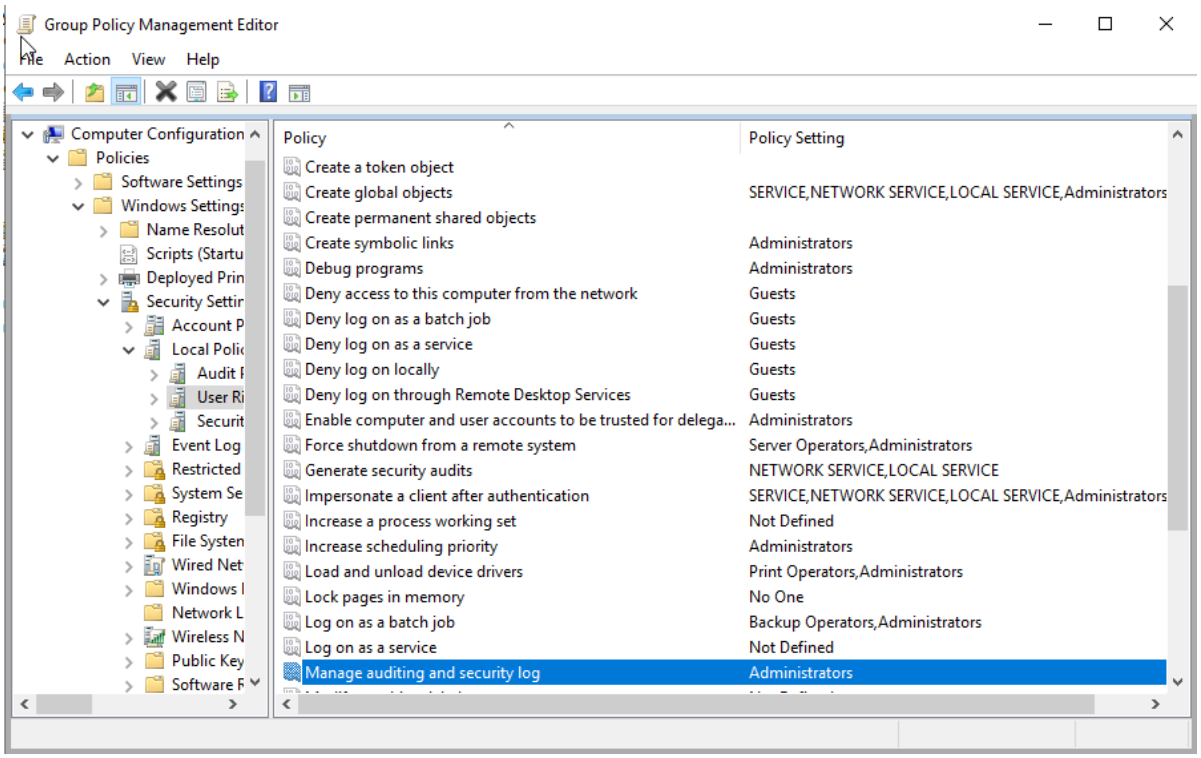


Image 40-Ensure 'Manage auditing and security log' is set to 'Administrators'

3.1.31 Ensure 'Modify an object label' is set to 'No One'

This privilege determines which user accounts can modify the integrity labels of objects, such as files, registry keys, or processes owned by others. User accounts can lower the integrity label of objects they own without this privilege. The recommended configuration for this setting is to assign it to no one. Allowing modification of the integrity labels of objects owned by others could enable malicious users to elevate privileges and execute code at a higher level than intended.

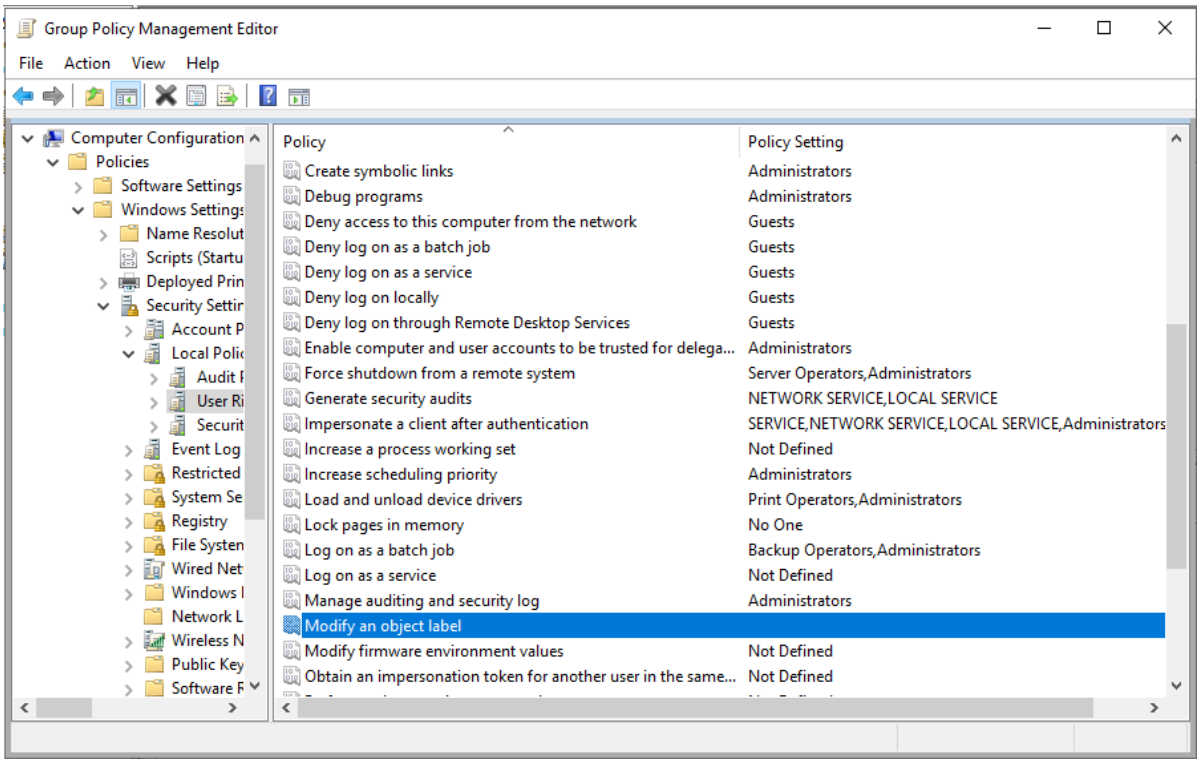


Image 41-Ensure 'Modify an object label' is set to 'No One'

3.1.32 Ensure 'Modify firmware environment values' is set to 'Administrators'

This policy setting allows users to configure system-wide environment variables that affect hardware configuration, typically stored in the Last Known Good Configuration. Modifying these values could lead to hardware failure and result in a denial of service (DoS) condition. The recommended assignment for this setting is Administrators. This user right is considered a "sensitive privilege" for auditing purposes. Granting the "Modify firmware environment values" user right could enable someone to misconfigure hardware settings, causing failure, data corruption, or a DoS condition.

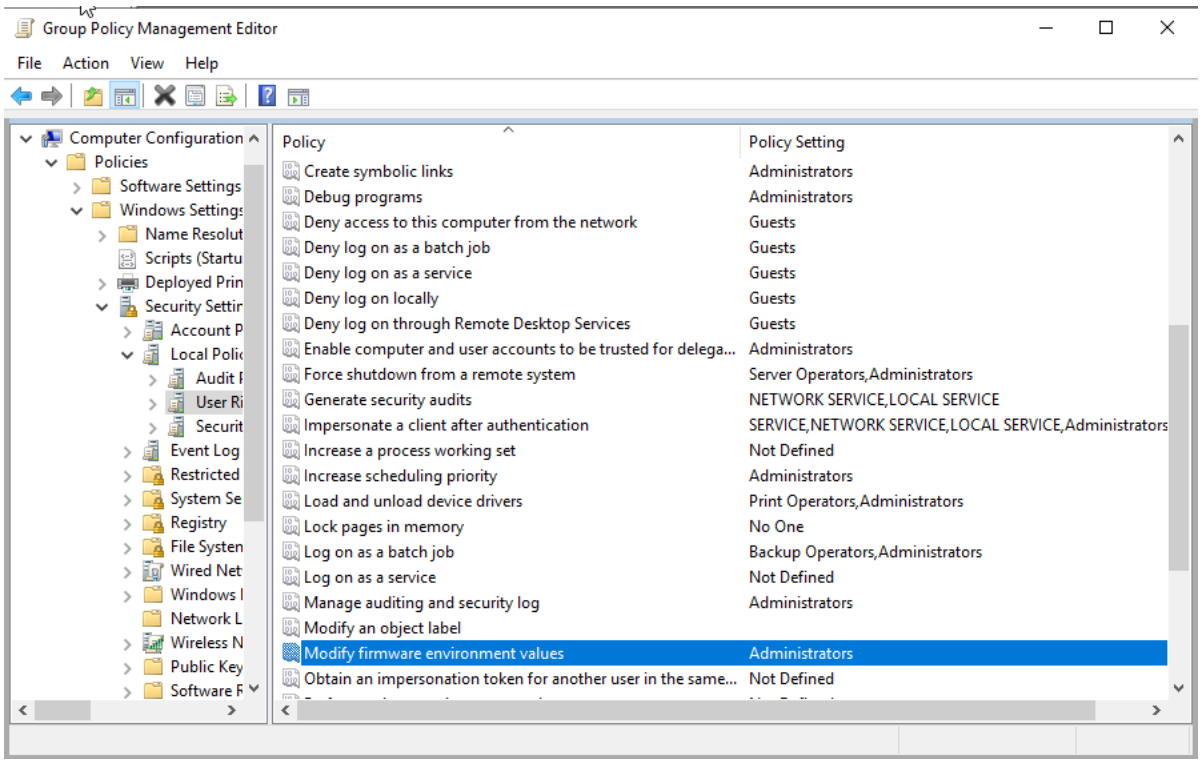


Image 42-Ensure 'Modify firmware environment values' is set to 'Administrators'

3.1.33 Ensure 'Perform volume maintenance tasks' is set to 'Administrators'

This policy setting enables users to manage the system's volume or disk configuration, potentially allowing a user to delete a volume, which could lead to data loss and a denial-of-service condition. The recommended setting for this policy is: Administrators. However, a Member Server with Microsoft SQL Server installed requires a special exception for the account running the SQL Server service to be granted this user right. Assigning the Perform volume maintenance tasks user right to a user could result in the deletion of a volume, causing data loss or a denial-of-service condition.

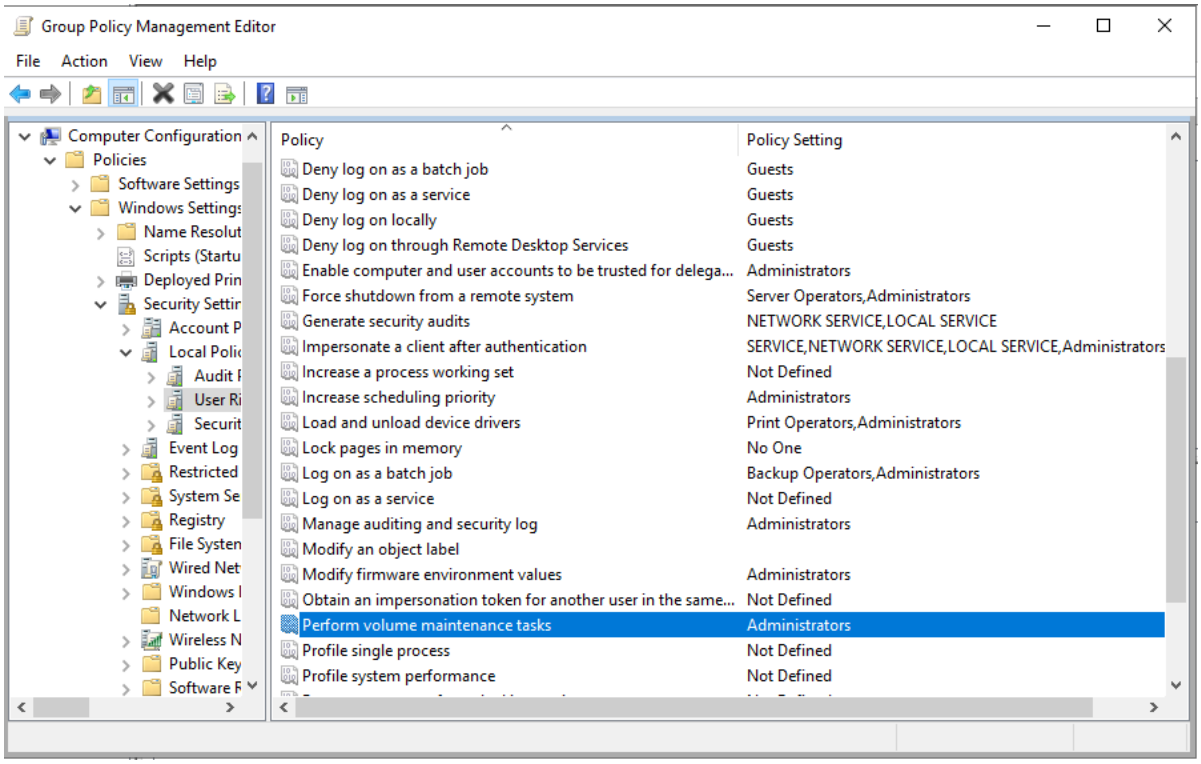


Image 43-Ensure 'Perform volume maintenance tasks' is set to 'Administrators'

3.1.34 Ensure 'Profile single process' is set to 'Administrators'

This policy setting determines which users can use tools to monitor the performance of non-system processes. Generally, you do not need to configure this user right for the Microsoft Management Console (MMC) Performance snap-in, but it is required if System Monitor is set to collect data using Windows Management Instrumentation (WMI). Restricting the Profile single process user right helps prevent intruders from gaining information that could be used to attack the system. The recommended setting for this policy is: Administrators. This user right poses a moderate vulnerability, as an attacker with this right could monitor a computer's performance to identify critical processes to attack or determine running processes to avoid countermeasures like antivirus software, an intrusion detection system, or identify other logged-on users.

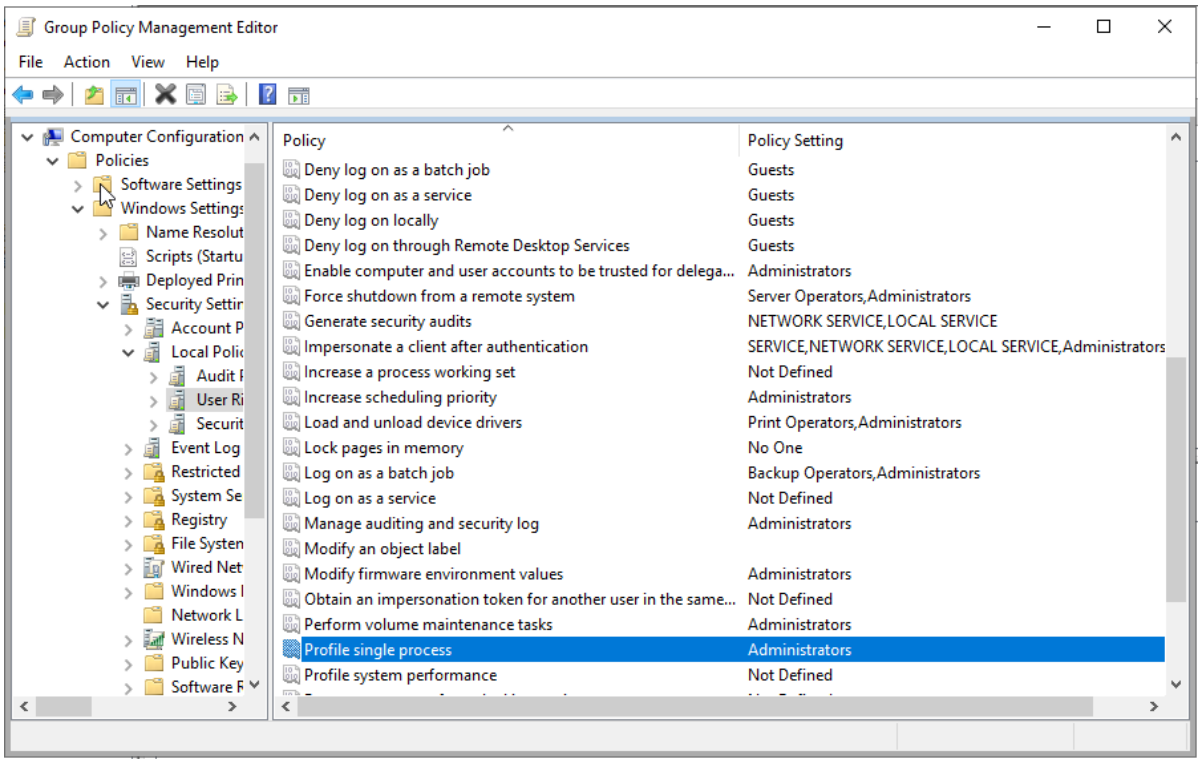


Image 44-Ensure 'Profile single process' is set to 'Administrators'

3.1.35 Ensure 'Profile system performance' is set to 'Administrators, NT SERVICE\WdiServiceHost'

This policy setting allows users to use tools to view the performance of different system processes, which could be exploited by attackers to determine a system's active processes and assess the potential attack surface. The recommended state for this setting is: Administrators, NT SERVICE\WdiServiceHost. This user right poses a moderate vulnerability, as attackers with this access could monitor a computer's performance to identify critical processes to attack or determine active processes to evade countermeasures like antivirus software or an intrusion detection system.

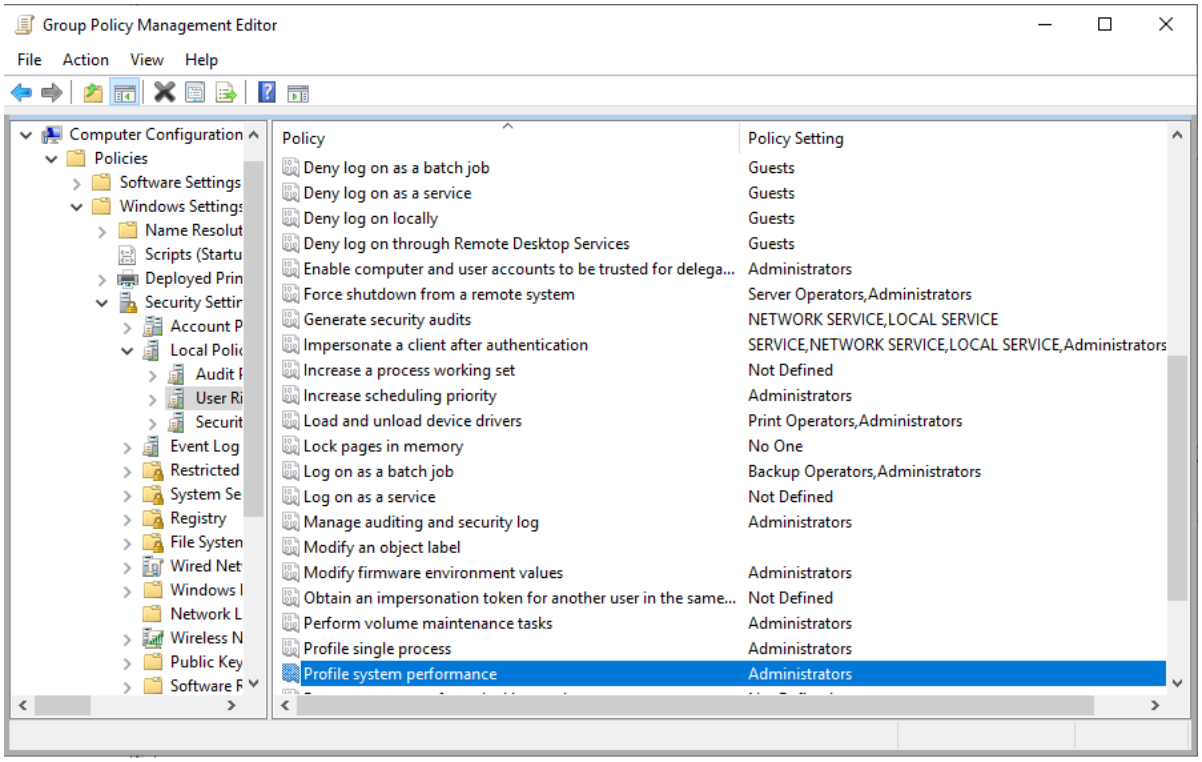


Image 45-Ensure 'Profile system performance' is set to 'Administrators, NT SERVICE\WdiServiceHost'

3.1.36 Ensure 'Replace a process level token' is set to 'LOCAL SERVICE, NETWORK SERVICE'

This policy setting allows a process or service to start another service or process with a different security access token, potentially leading to privilege escalation by modifying the security access token of the sub-process. The recommended state for this setting is: LOCAL SERVICE, NETWORK SERVICE. This user right is considered a "sensitive privilege" for auditing purposes. Member Servers with the Web Server (IIS) Role or Microsoft SQL Server installed require special exceptions to this recommendation to allow IIS application pools and additional SQL-generated entries to be granted this user right. Users with the Replace a process level token privilege can start processes as other users, potentially hiding unauthorized actions. Additionally, on Windows 2000-based computers, using this right also requires the Adjust memory quotas for a process user right.

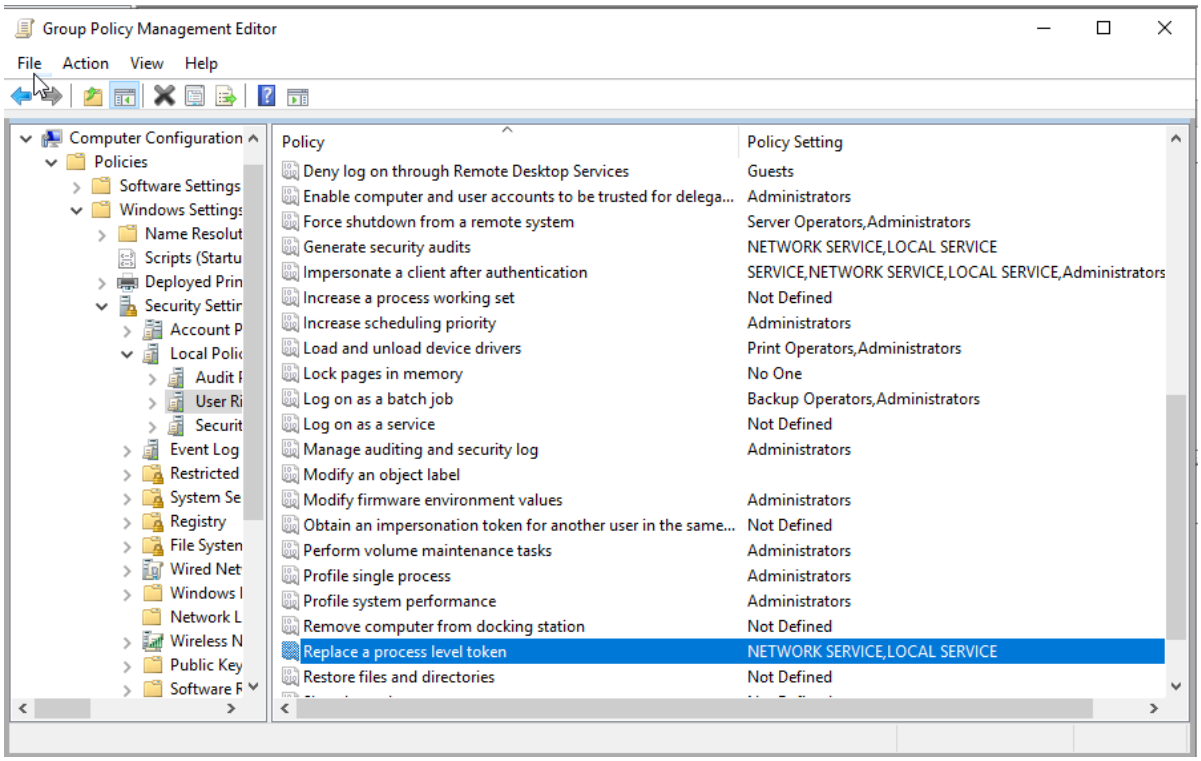


Image 46-Ensure 'Replace a process level token' is set to 'LOCAL SERVICE, NETWORK SERVICE'

3.1.37 Ensure 'Restore files and directories' is set to 'Administrators'

This policy setting determines which users can bypass file, directory, registry, and other persistent object permissions when restoring backed-up files and directories on computers running Windows Vista or newer. It also determines which users can set valid security principals as object owners, similar to the Back up files and directories user right. The recommended state for this setting is: Administrators. This user right is considered a "sensitive privilege" for auditing purposes.

An attacker with the Restore files and directories user right could restore sensitive data to a computer, potentially overwriting more recent data, leading to data loss, corruption, or a denial of service. Attackers could also replace executable files used by legitimate administrators or system services with malicious versions to gain elevated privileges, compromise data, or install backdoors for continued access. Therefore, it is crucial to protect backup media, as attackers could restore data to a computer within a domain they control.

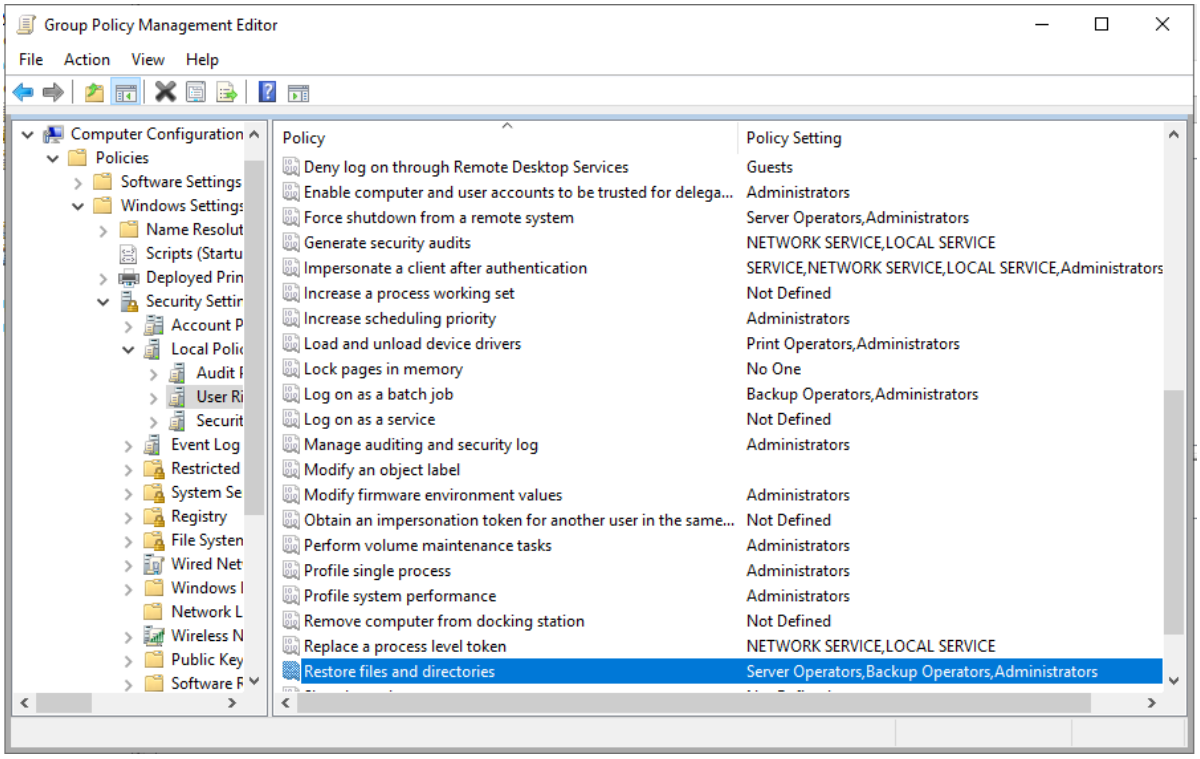


Image 47-Ensure 'Restore files and directories' is set to 'Administrators'

3.1.38 Ensure 'Shut down the system' is set to 'Administrators'

This policy setting determines which users logged on locally to the computers in your environment can shut down the operating system using the Shut Down command. Misuse of this user right can lead to a denial of service condition. The recommended state for this setting is: Administrators.

Limiting the ability to shut down Domain Controllers and Member Servers to a small number of trusted Administrators is essential. Although this right requires the ability to log on to the server, it is crucial to carefully control which accounts and groups are permitted to shut down these critical systems. Shutting down a Domain Controller makes it unavailable for processing logons, serving Group Policy, and handling LDAP queries. Additionally, shutting down Domain Controllers with Flexible Single Master Operations (FSMO) roles can disable essential domain functionalities, such as processing logons for new passwords, a key function of the Primary Domain Controller (PDC) Emulator role.

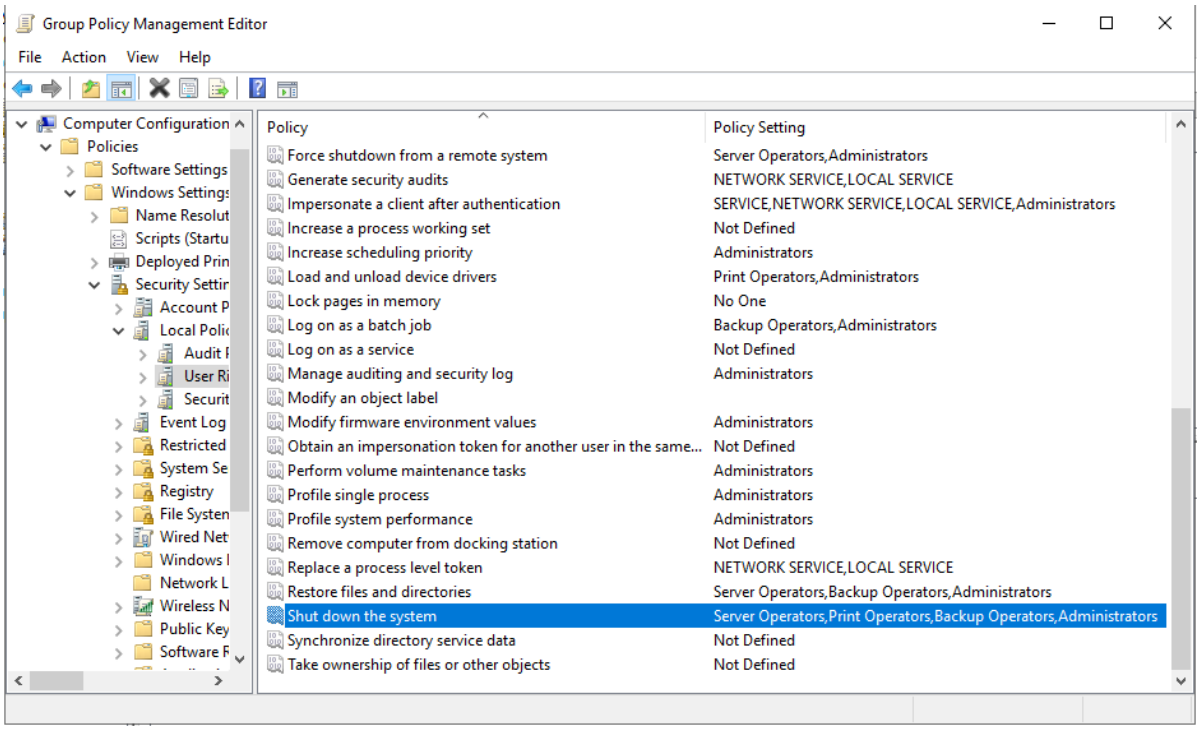


Image 48-Ensure 'Shut down the system' is set to 'Administrators'

3.1.39 Ensure 'Synchronize directory service data' is set to 'No One'

This security setting determines which users and groups can synchronize all directory service data, known as Active Directory synchronization. The recommended state for this setting is: No One.

Only Domain Controllers should have the ability to synchronize directory service data, as they inherently possess this user right since the synchronization process runs in the context of the System account on Domain Controllers. Granting this right to attackers would allow them to view all information stored in the directory, potentially facilitating further attacks or exposing sensitive data, such as direct telephone numbers or physical addresses.

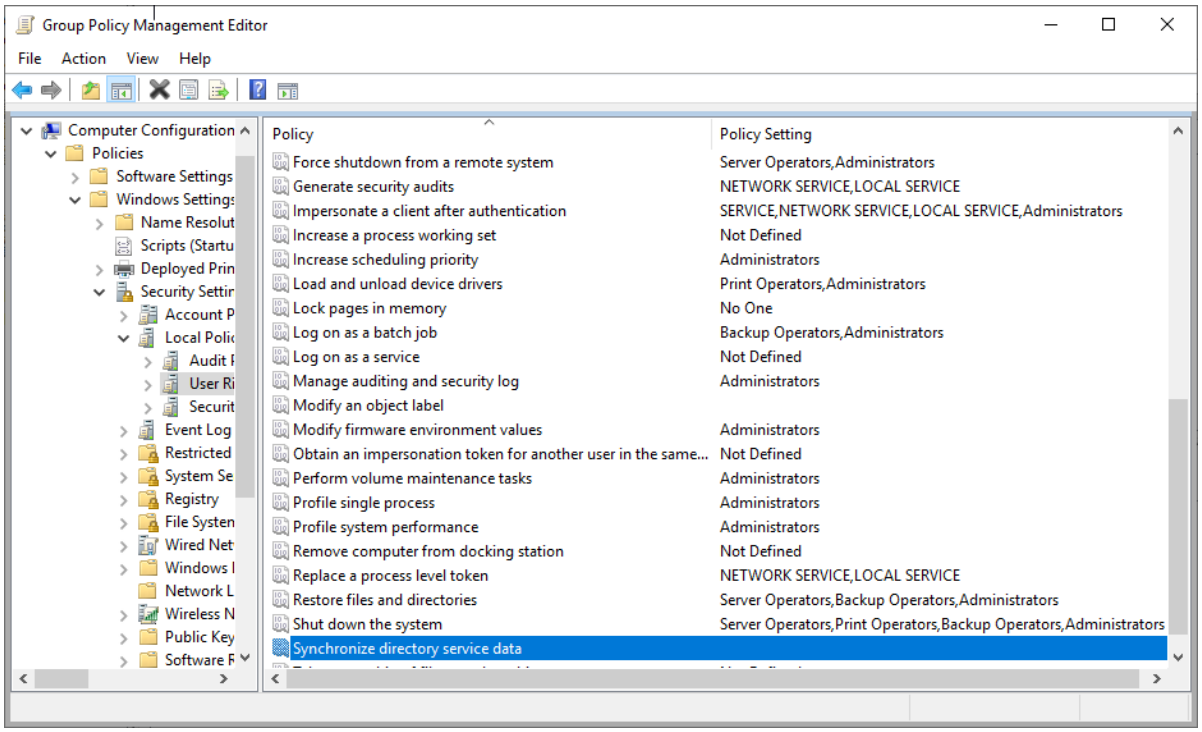


Image 49-Ensure 'Synchronize directory service data' is set to 'No One'

3.1.40 Ensure 'Take ownership of files or other objects' is set to 'Administrators'

This policy setting allows users to take ownership of files, folders, registry keys, processes, or threads, bypassing existing permissions to grant ownership to the specified user. The recommended state for this setting is: Administrators. This user right is considered a "sensitive privilege" for auditing purposes.

Users with the Take ownership of files or other objects user right can control any object, regardless of its permissions, and make any changes they wish. This capability could lead to data exposure, data corruption, or a denial of service condition.

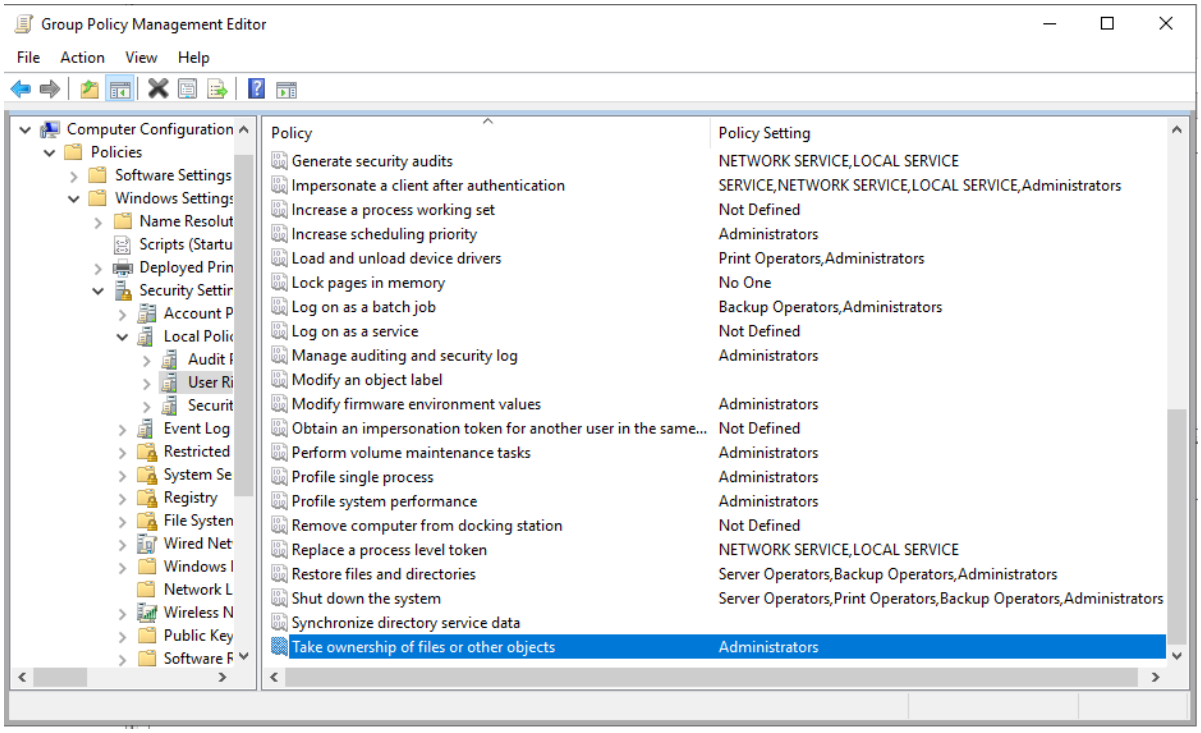


Image 50-Ensure 'Take ownership of files or other objects' is set to 'Administrators'

3.2 Security Options

Security Options encompass a range of settings that enhance the protection of a computer or network by controlling security-related behaviors and features. These options include settings for user authentication, access controls, and system auditing, ensuring a secure and compliant operating environment. By carefully configuring Security Options, organizations can mitigate risks, prevent unauthorized access, and maintain the integrity and confidentiality of sensitive information.

3.2.1 Accounts

3.2.1.1 Ensure 'Accounts: Block Microsoft accounts' is set to 'Users can't add or log on with Microsoft accounts'

This policy setting restricts users from adding new Microsoft accounts on the computer. It is recommended that users be prevented from adding or logging in with Microsoft accounts. Organizations aiming to enforce strict identity management policies and control which accounts are used for logging onto their computers should consider blocking Microsoft accounts. Additionally, blocking these accounts may be necessary to meet compliance requirements for their information systems.

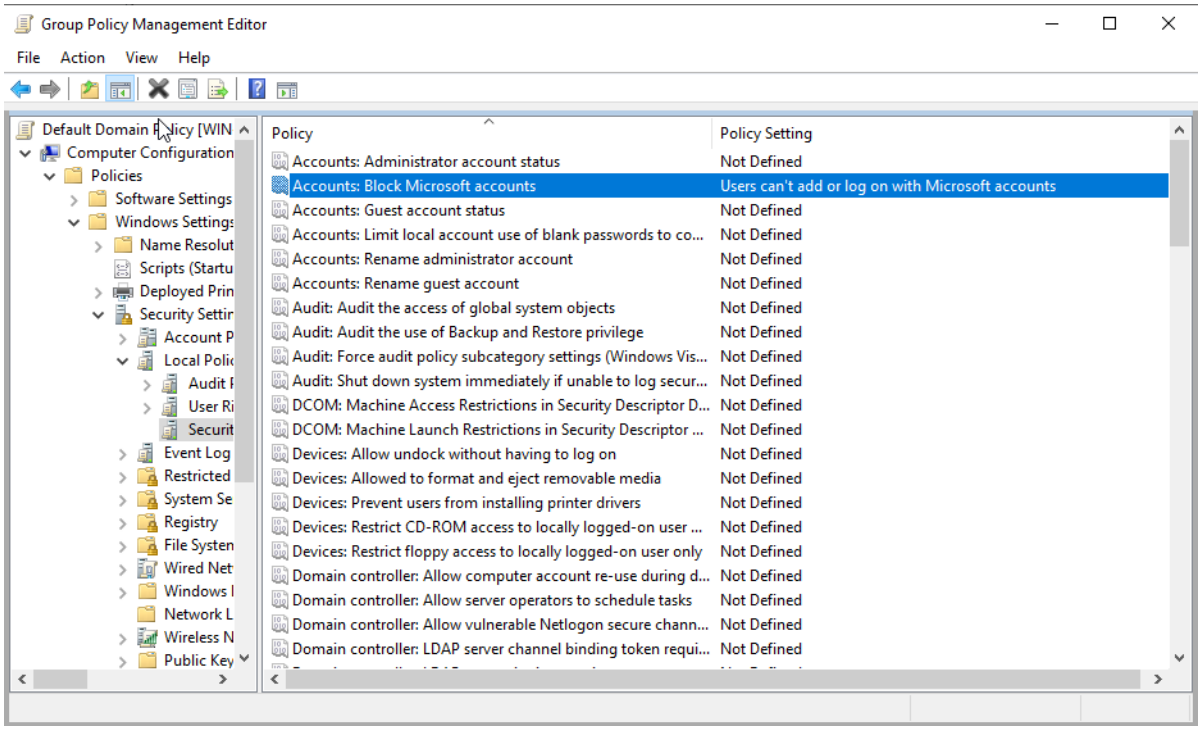


Image 51-Ensure 'Accounts: Block Microsoft accounts' is set to 'Users can't add or log on with Microsoft accounts'

3.2.1.2 Ensure 'Accounts: Guest account status' is set to 'Disabled'

This policy setting controls whether the Guest account is enabled or disabled, with the Guest account allowing unauthenticated network users to access the system. It is recommended to disable this account to prevent unauthorized access. Note that applying this setting to the Domain Controllers organizational unit via group policy will have no effect, as Domain Controllers lack a local account database. Instead, it should be configured at the domain level, similar to other policies like account lockout and password settings. The rationale for disabling the Guest account is to prevent unauthenticated users from accessing network resources, which could lead to data exposure or corruption if network shares are accessible to the Guest account, the Guests group, or the Everyone group.

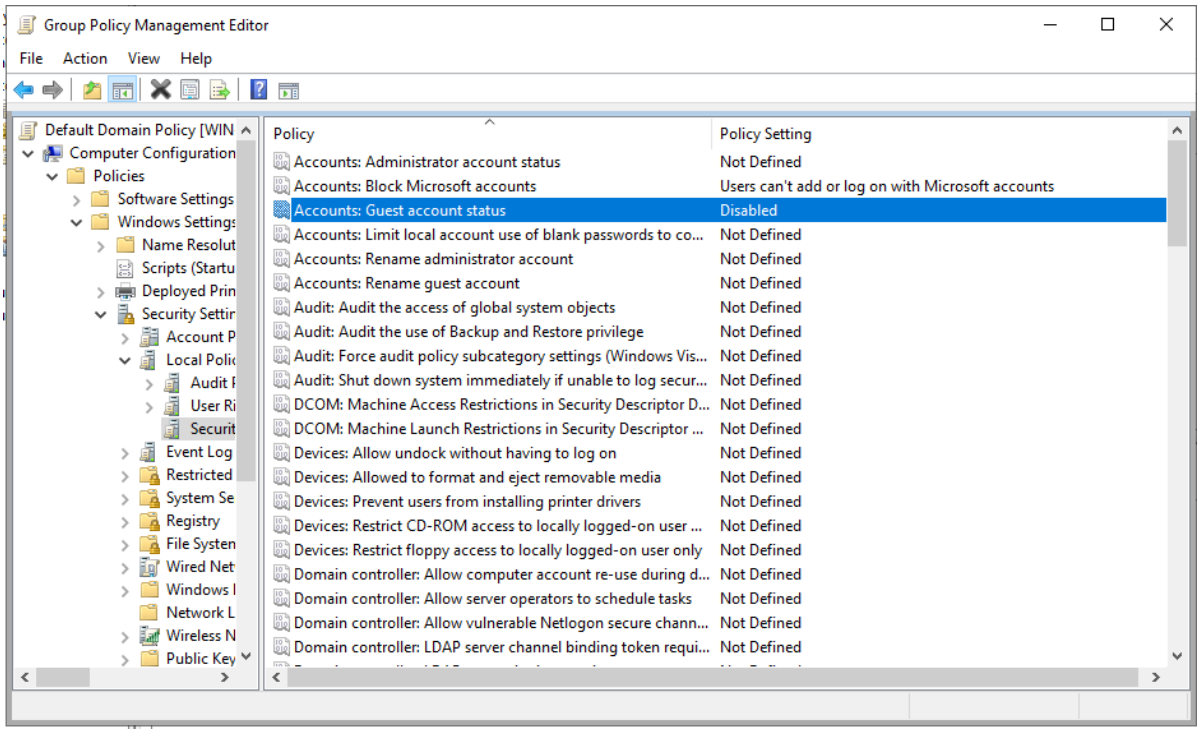


Image 52-Ensure 'Accounts: Guest account status' is set to 'Disabled'

3.2.1.3 Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled'

This policy setting determines whether local accounts with blank passwords can be used to log on from locations other than the physical computer console. When enabled, this policy ensures that such accounts can only log in directly at the computer and not from remote client computers. The recommended configuration for this setting is to enable it.

Blank passwords present a serious security threat and should be strictly prohibited through both organizational policies and technical controls. Although Active Directory domains typically enforce complex passwords of at least seven characters, users with the ability to create new accounts might bypass these domain policies by establishing accounts with blank passwords. For instance, a user could set up a standalone computer, create accounts with blank passwords, and then join the computer to the domain, allowing these unprotected accounts to function and potentially be accessed by anyone who knows their names.

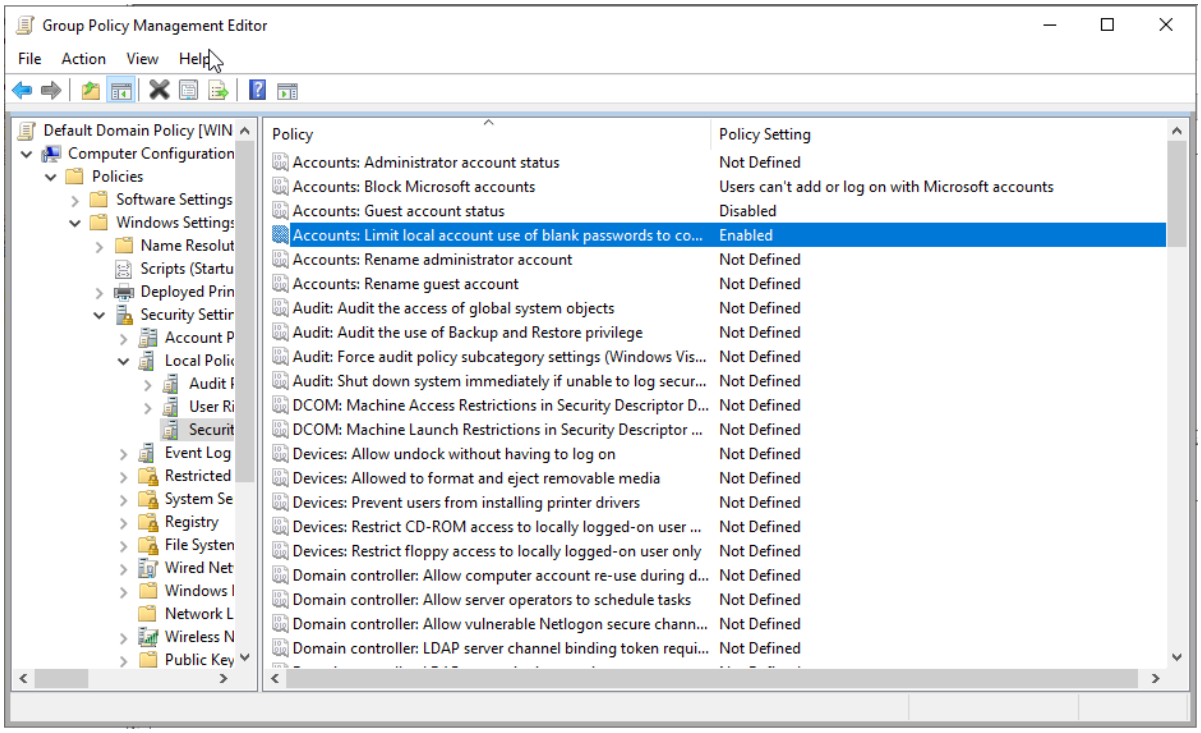


Image 53-Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled'

3.2.1.4 Configure 'Accounts: Rename administrator account'

The built-in local administrator account is a commonly targeted account due to its well-known name. It is recommended to rename this account to a less obvious name and avoid using names that suggest administrative or elevated access. Additionally, update the default description for the local administrator account via the Computer Management console. For Domain Controllers, which do not have local accounts, this guidance applies to the built-in Administrator account created during domain setup.

Renaming the Administrator account makes it somewhat more difficult for unauthorized users to guess the privileged username and password. Since the built-in Administrator account cannot be locked out regardless of failed password attempts, it is a frequent target for brute force attacks. While renaming the account offers some security benefits, its effectiveness is reduced because the account has a well-known SID, and third-party tools can authenticate using the SID rather than the account name. As a result, even if the account is renamed, attackers could potentially exploit the SID to conduct brute force attacks.

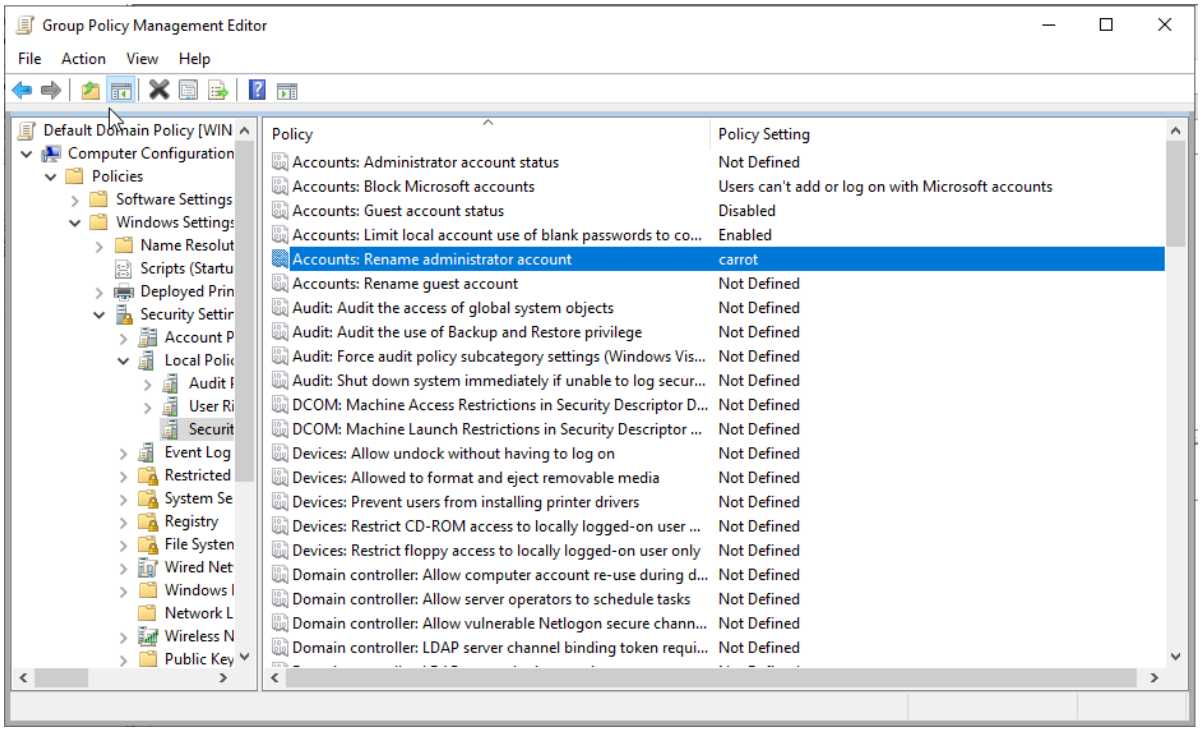


Image 54-Configure 'Accounts: Rename administrator account'

3.2.1.5 Configure 'Accounts: Rename guest account'

The built-in local guest account is a commonly known target for attackers. It is advisable to rename this account to a name that does not reveal its purpose, even if you disable it, which is the recommended action. On Domain Controllers, which lack local accounts, this guidance applies to the built-in Guest account created during domain setup.
Renaming the Guest account adds an extra layer of security by making it harder for unauthorized individuals to guess the account name and password. This practice helps to obscure the account's function and reduces its attractiveness as a target for attacks.

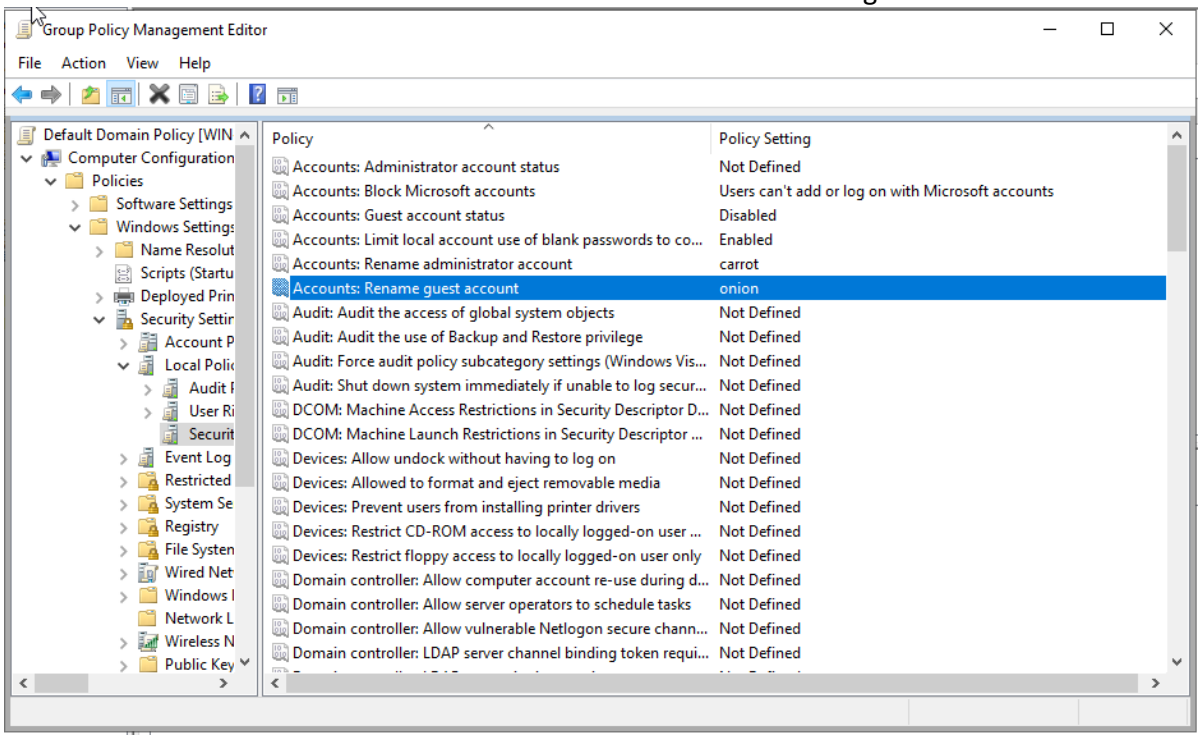


Image 55-Configure 'Accounts: Rename guest account'

3.2.2 Audit

3.2.2.1 Ensure 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' is set to 'Enabled'

This policy setting enables administrators to utilize the advanced auditing features introduced in Windows Vista. Unlike the Audit Policy settings available in Windows Server 2003 Active Directory, which do not support the new auditing subcategories, configuring the setting "Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings" to Enabled is essential for applying the required auditing policies.

The recommended configuration for this setting is Enabled. However, caution is advised with audit settings that may generate excessive traffic. For instance, enabling success or failure auditing for all Privilege Use subcategories could produce a high volume of audit events, complicating the identification of other entries in the Security log and potentially affecting system performance.

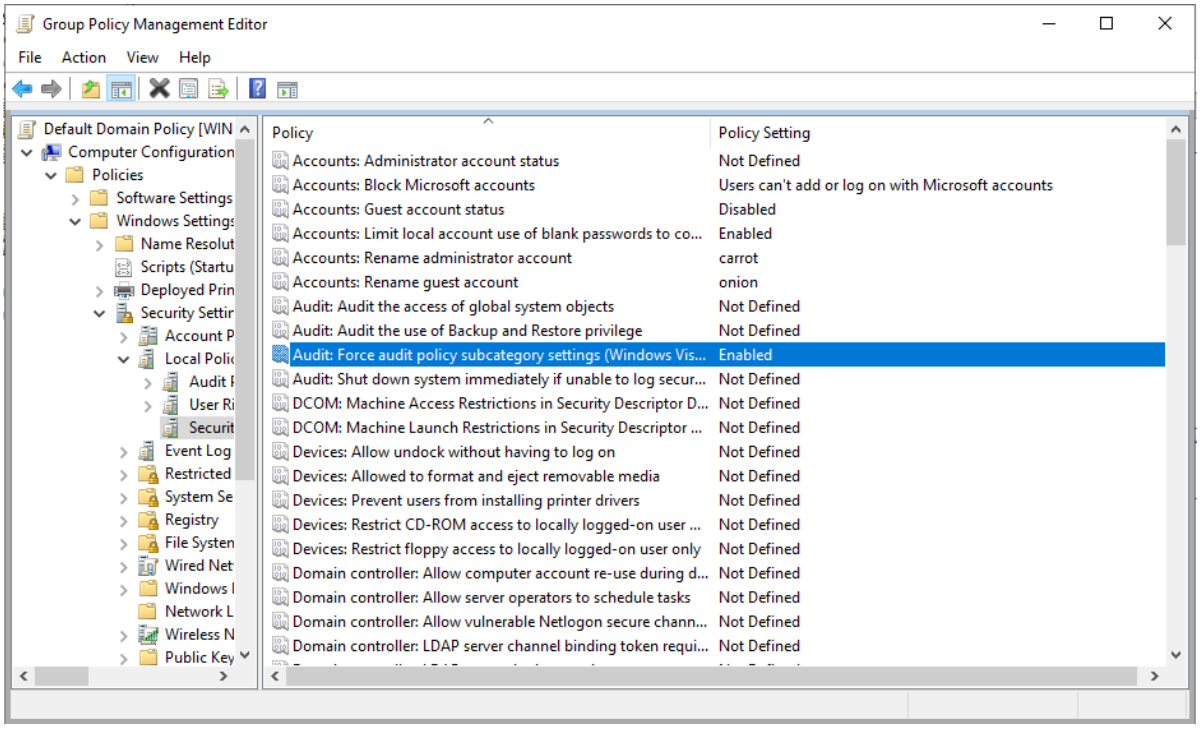


Image 56-Ensure 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' is set to 'Enabled'

3.2.2.2 Ensure 'Audit: Shut down system immediately if unable to log security audits' is set to 'Disabled'

This policy setting determines whether the system will shut down if it cannot log Security events. To meet Trusted Computer System Evaluation Criteria (TCSEC)-C2 and Common Criteria certification, which aim to ensure that auditable events are not lost if the audit system fails, Microsoft has chosen to implement this requirement by shutting down the system and displaying a stop message in case of an auditing failure. When enabled, this setting will cause the system to shut down if security audits cannot be logged for any reason.

Enabling the "Audit: Shut down system immediately if unable to log security audits" setting can lead to unplanned system failures and significant administrative challenges, especially if the Security log retention is set to "Do not overwrite events (clear log manually)." This configuration could transform a potential repudiation threat into a denial of service (DoS) vulnerability, as an overwhelmed server with excessive logon and security events could be forced to shut down. Moreover, the abrupt shutdown might cause irreparable damage to the operating system, applications, or data. Although the NTFS file system maintains integrity during an ungraceful shutdown, it cannot guarantee the usability of all data files or applications upon restart.

The recommended state for this setting is Disabled. This configuration helps ensure that critical evidence and troubleshooting information remain available after a security incident and prevents attackers from deliberately generating excessive Security log events to trigger a shutdown.

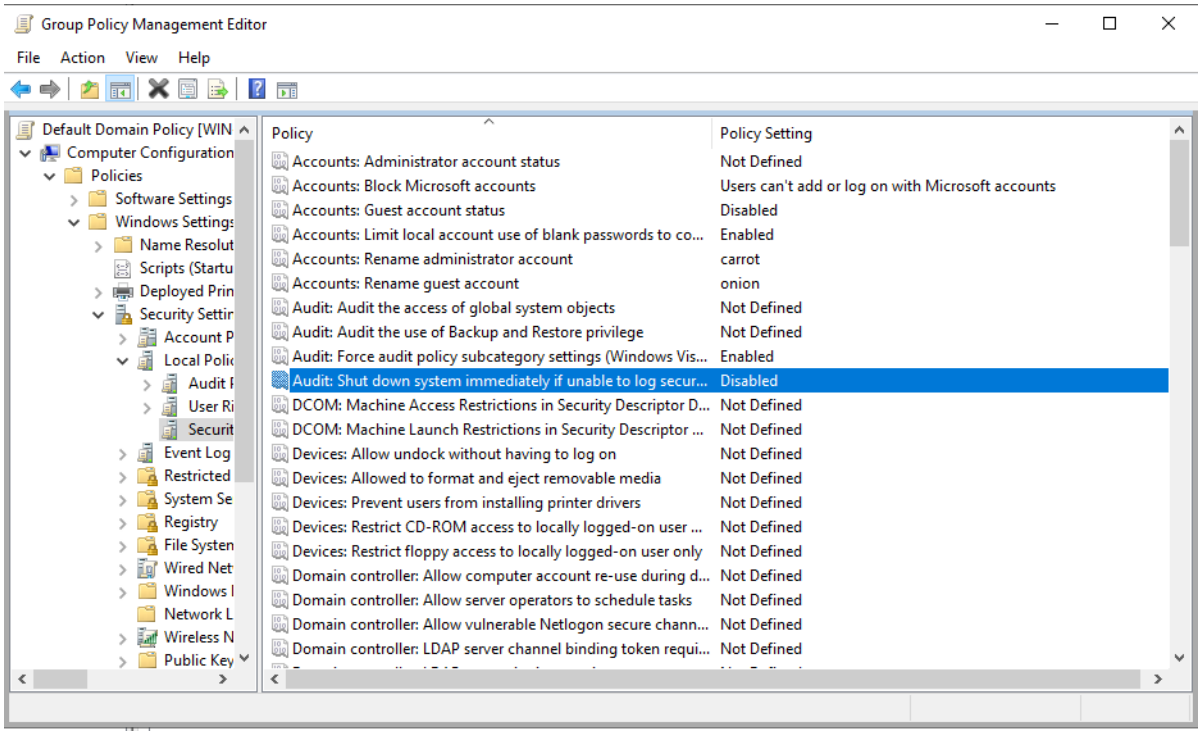


Image 57-Ensure 'Audit: Shut down system immediately if unable to log security audits' is set to 'Disabled'

3.2.3 Devices

3.2.3.1 Ensure 'Devices: Prevent users from installing printer drivers' is set to 'Enabled'

This policy setting governs who can install printer drivers when connecting to a shared printer. For a computer to print to a shared printer, the corresponding driver must be installed locally. The recommended configuration for this setting is Enabled. It is important to note that this setting does not influence the ability to add local printers and does not apply to Administrators.

Allowing users to install printer drivers on their workstations may be suitable in some organizations. However, it is advisable to restrict this capability to Administrators on servers to avoid potential instability. Printer driver installations on servers can unintentionally compromise system stability. Malicious users might install harmful drivers intentionally or accidentally introduce malware disguised as printer drivers. An attacker could exploit this by masking a Trojan horse as a printer driver, which might appear necessary for printing but could instead deploy malicious code across the network.

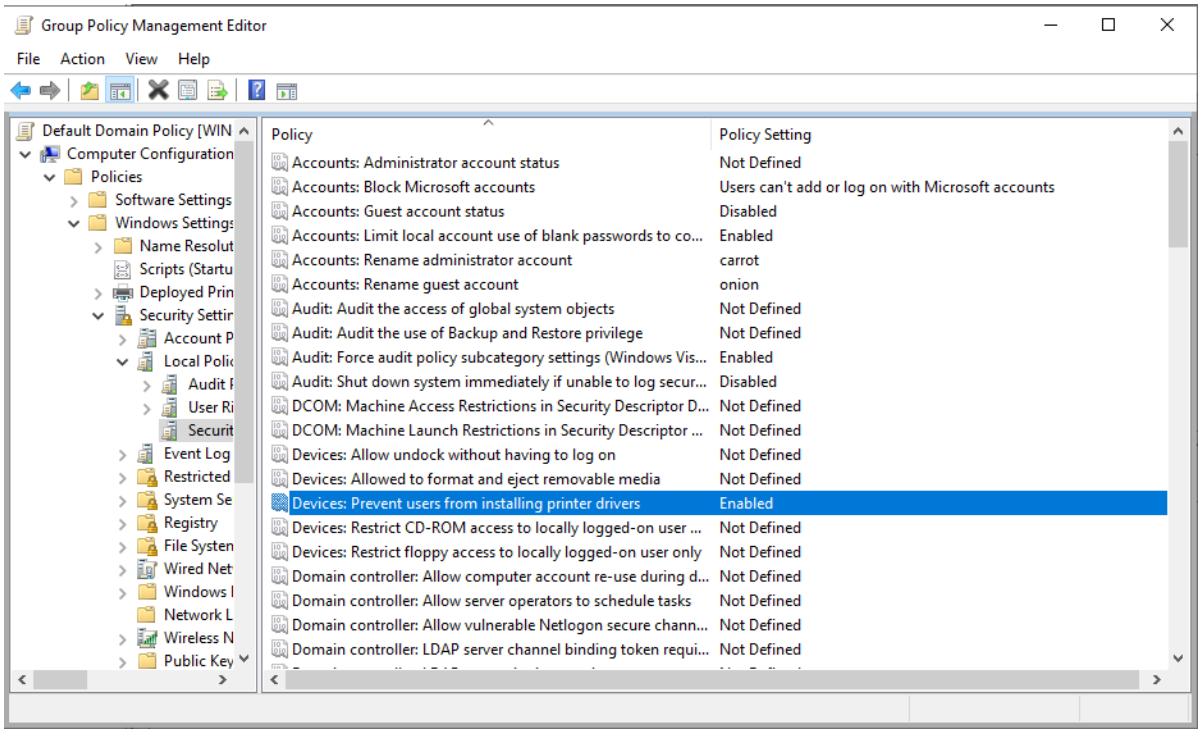


Image 58-Ensure 'Devices: Prevent users from installing printer drivers' is set to 'Enabled'

3.2.4 Interactive logon

3.2.4.1 Ensure 'Interactive logon: Do not require CTRL+ALT+DEL' is set to 'Disabled'

This policy setting controls whether users must press CTRL+ALT+DEL before logging on to their computers. The recommended configuration for this setting is Disabled.

Microsoft introduced this feature to assist users with specific physical impairments by simplifying the logon process. However, omitting the CTRL+ALT+DEL requirement can expose users to attacks aimed at intercepting their passwords. Requiring this key combination ensures that passwords are transmitted through a secure and trusted path.

Without the CTRL+ALT+DEL prompt, attackers could deploy a Trojan horse that mimics the standard Windows logon screen to capture users' passwords. This would enable attackers to gain access to the compromised accounts with the same level of privilege as the legitimate users.

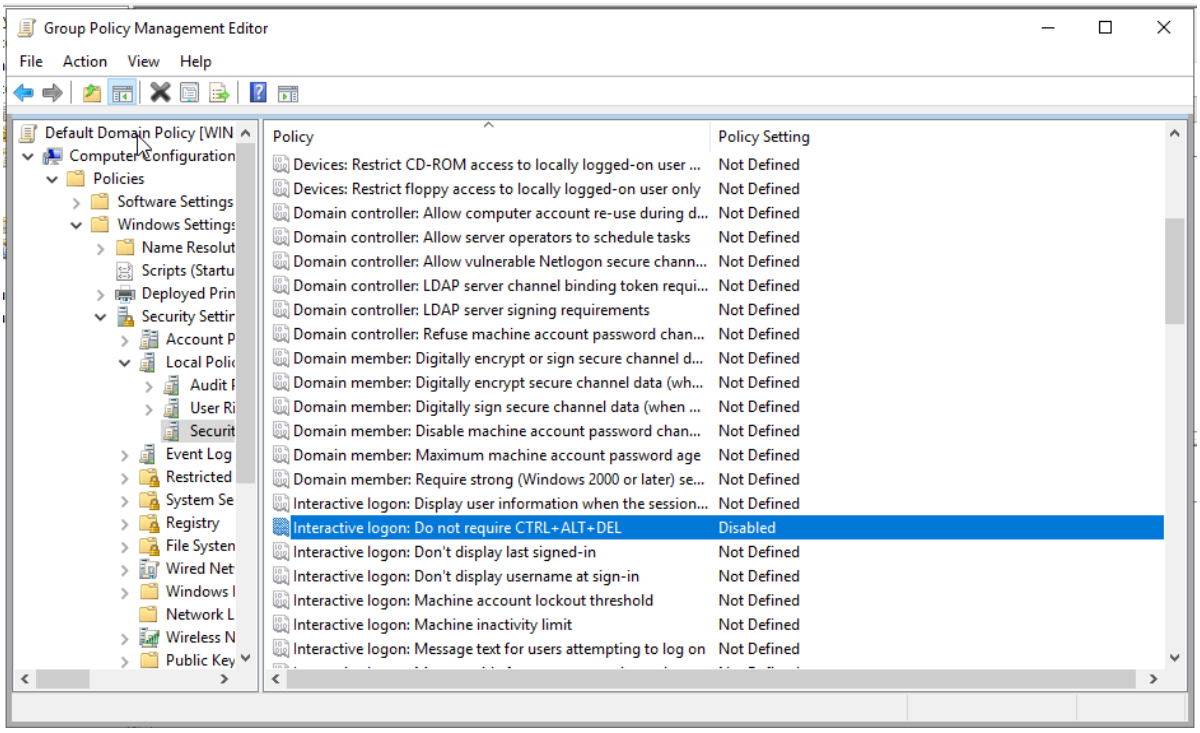


Image 59-Ensure 'Interactive logon: Do not require CTRL+ALT+DEL' is set to 'Disabled'

3.2.4.2 Ensure 'Interactive logon: Don't display last signed-in' is set to 'Enabled'

This policy setting controls whether the account name of the last user who logged on appears on the Windows logon screen of client computers within your organization. Enabling this setting helps to prevent unauthorized individuals from visually obtaining account names from desktop or laptop screens.

The recommended configuration for this setting is Enabled.

The rationale behind this recommendation is that an attacker with physical access to a computer or who can connect via Remote Desktop Services could see the name of the last user who logged on. This information could be used to attempt password guessing, dictionary attacks, or brute-force attacks to gain unauthorized access.

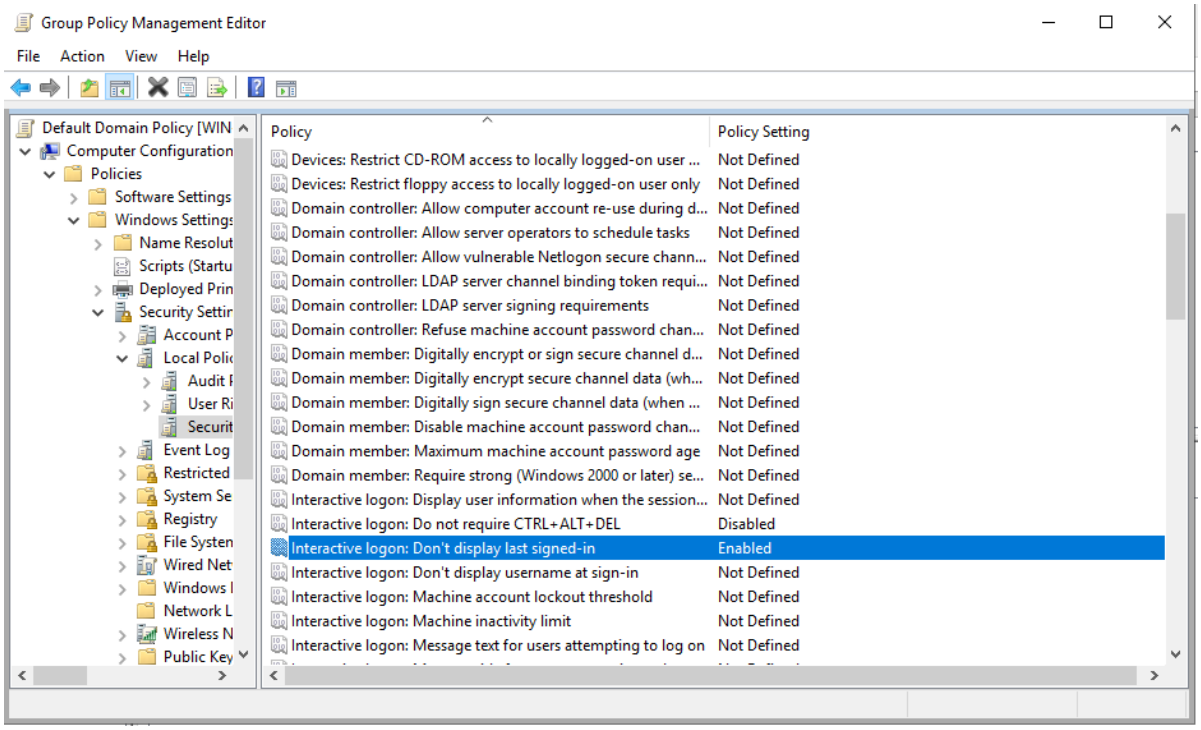


Image 60-Ensure 'Interactive logon: Don't display last signed-in' is set to 'Enabled'

3.2.4.3 Ensure 'Interactive logon: Machine inactivity limit' is set to '900 or fewer second(s), but not 0'

Windows detects inactivity in a logon session, and if the period of inactivity surpasses the set limit, the screen saver activates, locking the session. The recommended configuration for this setting is 900 seconds or less, but not 0, as a value of 0 disables the inactivity limit entirely.

The rationale for this recommendation is that if users fail to manually lock their computers when they step away, there is a risk that someone could access the machine without authorization.

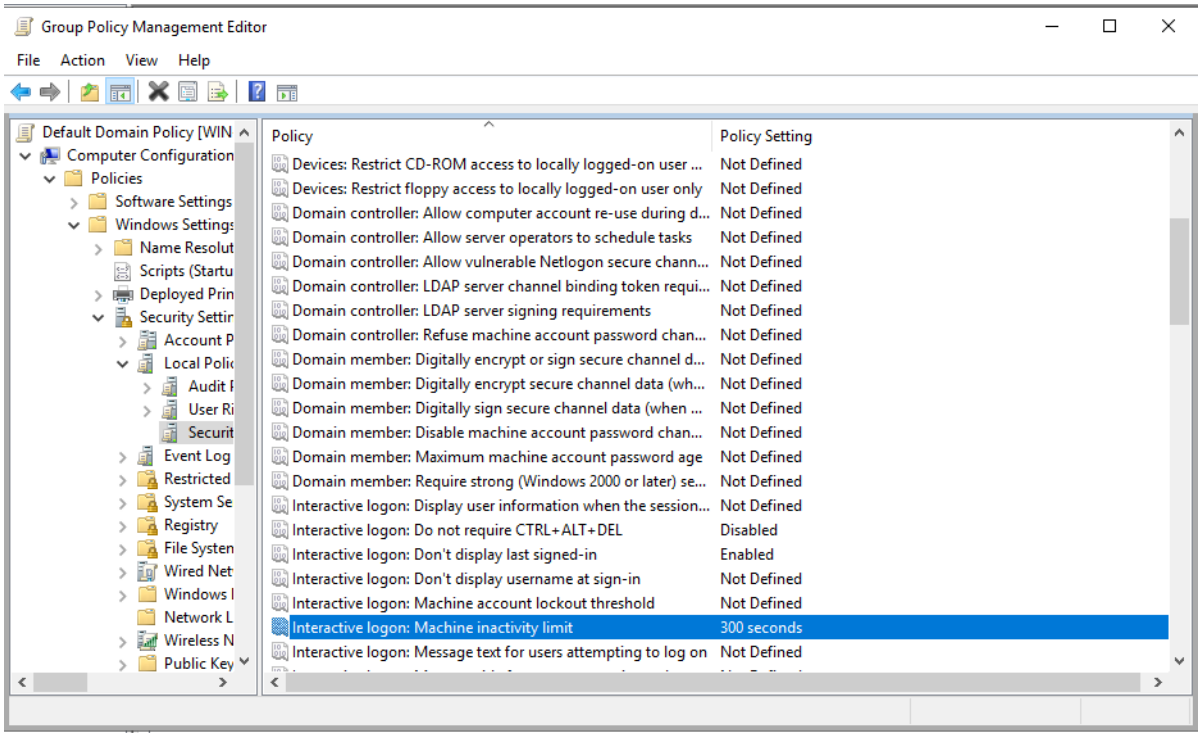


Image 61-Ensure 'Interactive logon: Machine inactivity limit' is set to '900 or fewer second(s), but not 0'

3.2.4.4 Configure 'Interactive logon: Message text for users attempting to log on'

This policy setting allows for the display of a text message to users upon logon. It should be configured to align with your organization's security and operational needs. Displaying a logon message can serve multiple purposes: it can deter potential attackers by informing them of the consequences of their actions and reinforce corporate policies by reminding employees of the rules and their potential audits. Such messages are often used for legal reasons, such as warning users about the misuse of company information or indicating that their activities may be monitored. Ensure that any warning message is reviewed and approved by your organization's legal and human resources departments.

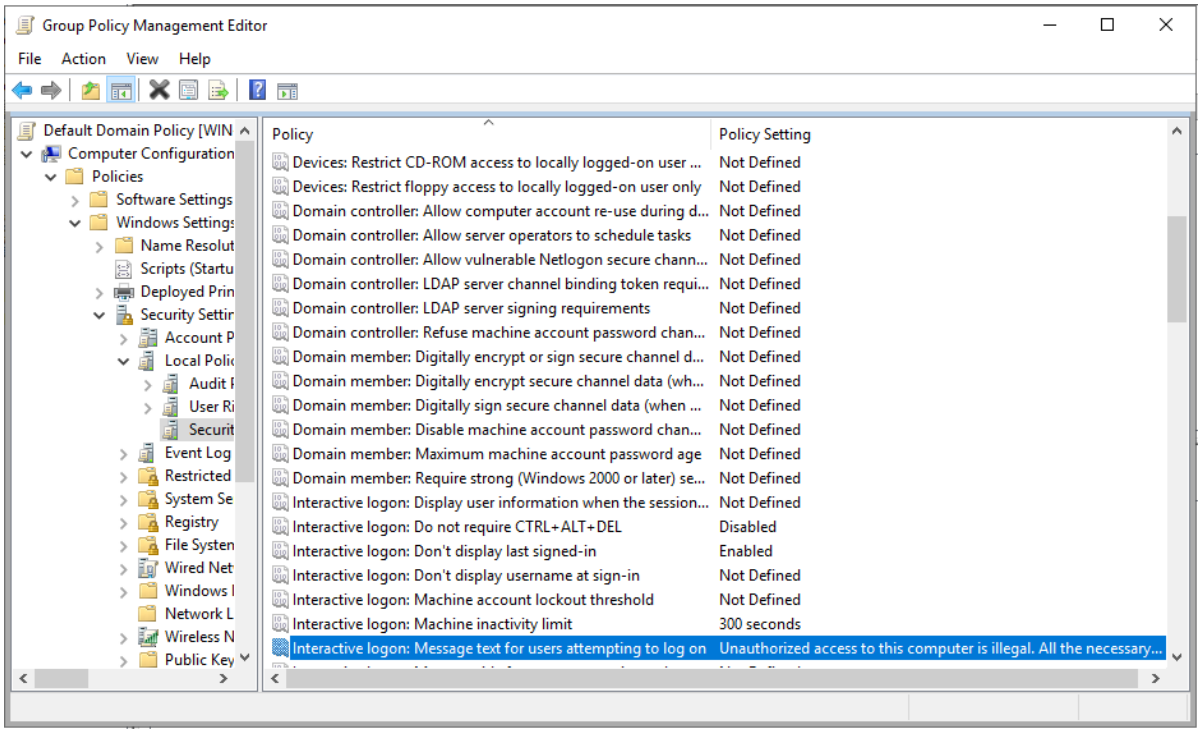


Image 62-Configure 'Interactive logon: Message text for users attempting to log on'

3.2.4.5 Configure 'Interactive logon: Message title for users attempting to log on'

This policy setting defines the text that appears in the title bar of the logon window. It should be configured to meet the security and operational needs of your organization. By displaying a warning message in this manner, you can deter potential attackers by informing them of the consequences of unauthorized actions and reinforce corporate policies by reminding employees of the rules during the logon process.

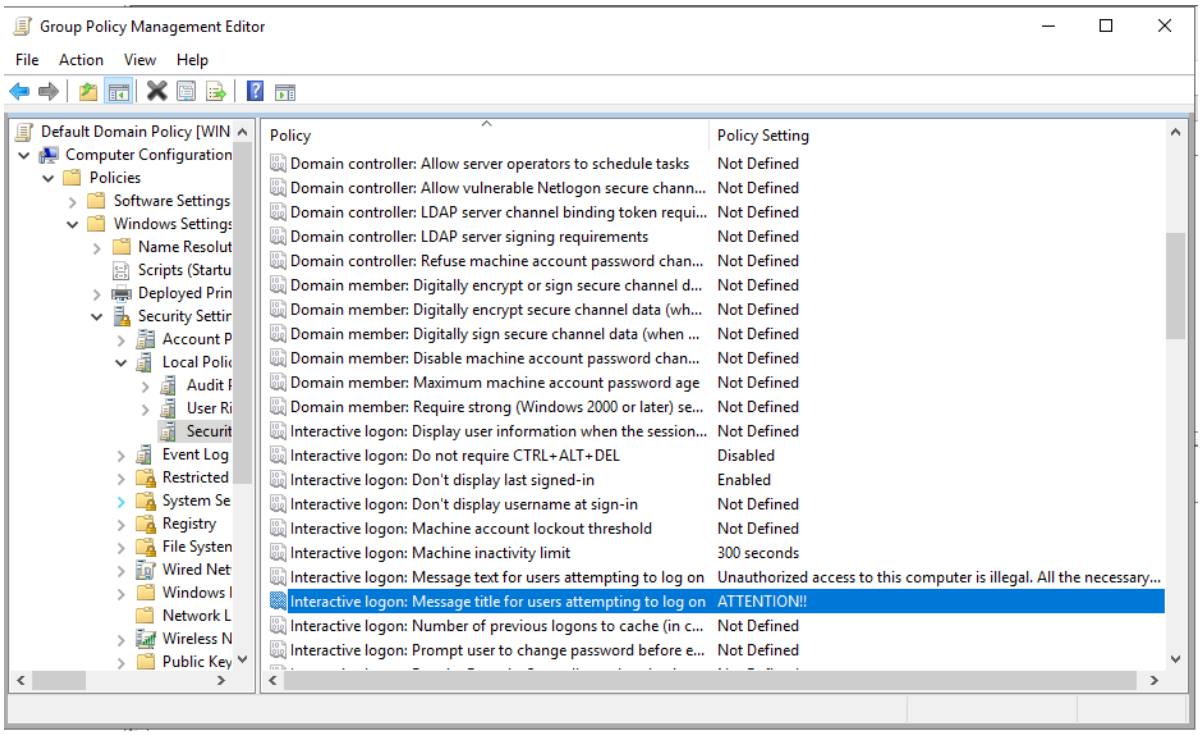


Image 63-Configure 'Interactive logon: Message title for users attempting to log on'

3.2.4.6 Ensure 'Interactive logon: Prompt user to change password before expiration' is set to 'between 5 and 14 days'

This policy setting specifies how many days in advance users are notified before their passwords expire. It is recommended to set this policy between 5 and 14 days to give users ample warning. Configuring password expiration is important to ensure that users are aware of upcoming expirations, preventing issues like accidental lockouts, which could lead to confusion or access problems, especially for those using dial-up or VPN connections. When set within the recommended range, users will receive a prompt to change their password each time they log on to the domain as the expiration date approaches.

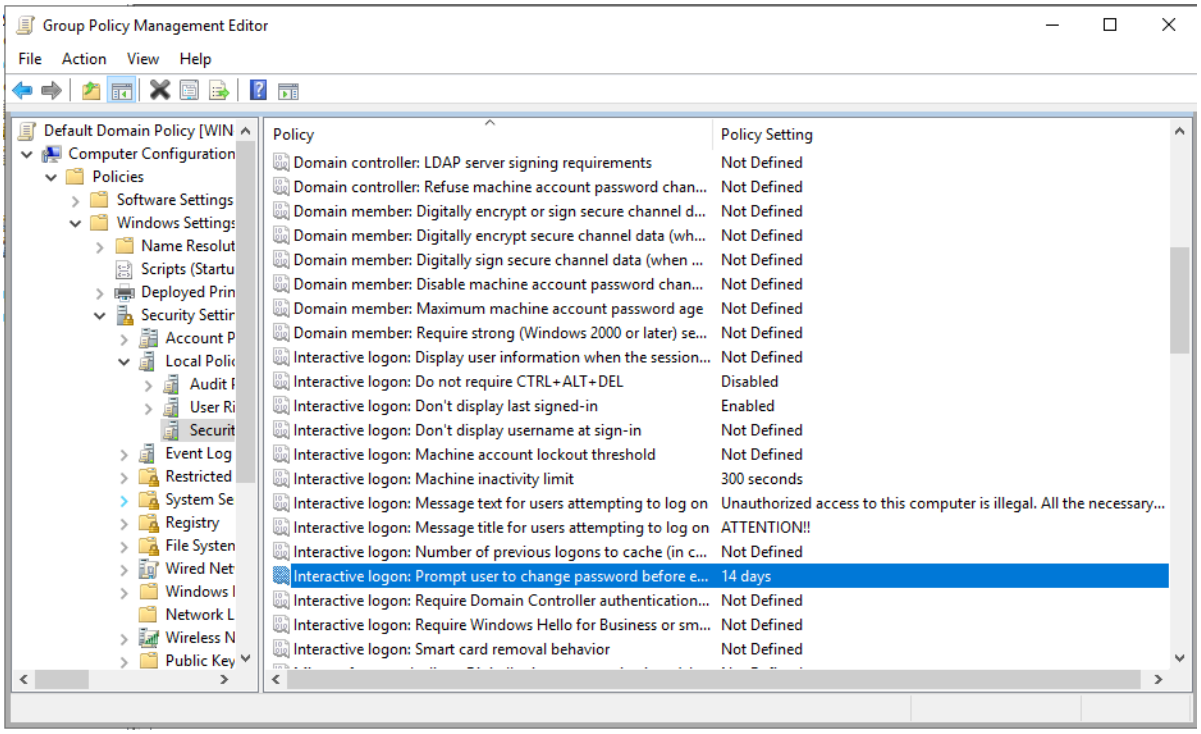


Image 64-Ensure 'Interactive logon: Prompt user to change password before expiration' is set to 'between 5 and 14 days'

3.2.4.7 Ensure 'Interactive logon: Require Domain Controller Authentication to unlock workstation' is set to 'Enabled'

This policy setting determines whether unlocking a computer requires contacting a Domain Controller for domain accounts. When enabled, users must authenticate with the Domain Controller to unlock their computer. By default, computers cache user credentials locally, allowing them to unlock the console with these cached credentials, which might not reflect recent changes to the account such as updated user rights, lockout status, or account disabling. Enabling this setting ensures that these changes are considered, preventing issues such as disabled accounts from unlocking the computer.

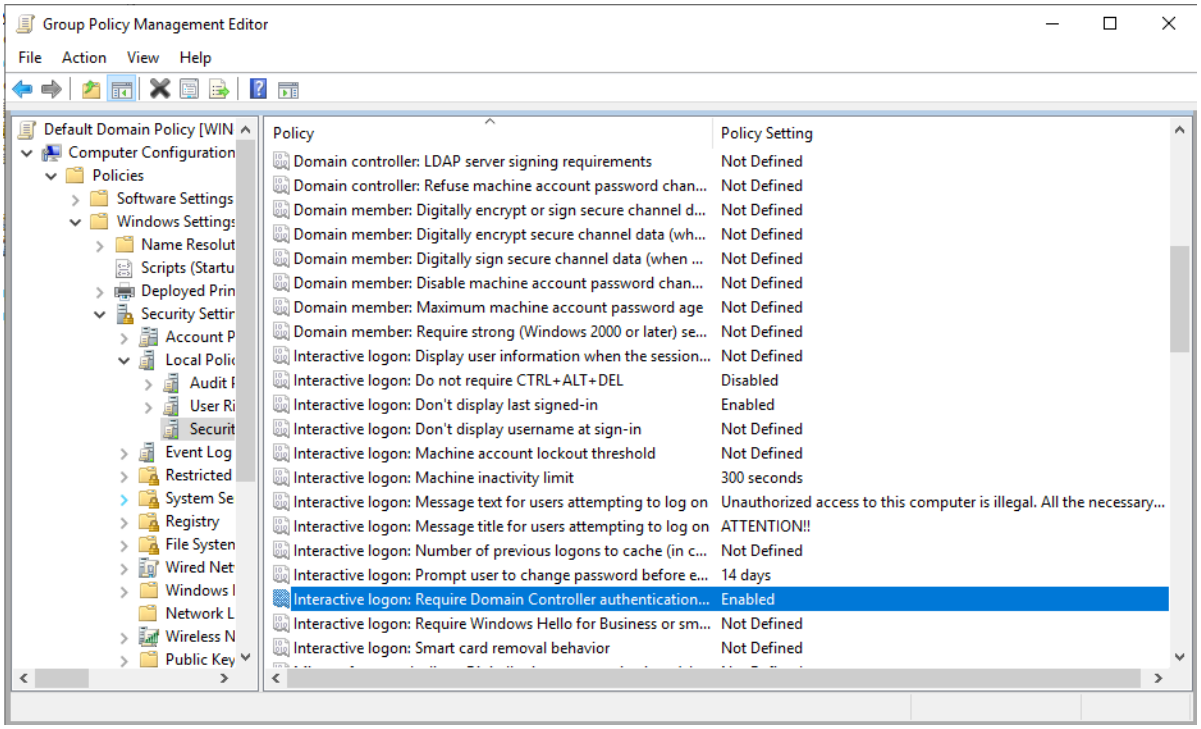


Image 65-Ensure 'Interactive logon: Require Domain Controller Authentication to unlock workstation' is set to 'Enabled'

3.2.4.8 Ensure 'Interactive logon: Require Domain Controller Authentication to unlock workstation' is set to 'Enabled'

This policy setting defines the action taken when a logged-in user's smart card is removed from the reader. The recommended configuration is to set it to "Lock Workstation," ensuring that the computer automatically locks when the smart card is removed. Alternatively, configuring it to "Force Logoff" or "Disconnect" for Remote Desktop Services sessions is also acceptable. This approach mitigates the risk of unauthorized access, as it prevents anyone from using the computer if the smart card is no longer present, thereby enhancing security by ensuring that only the cardholder can access resources.

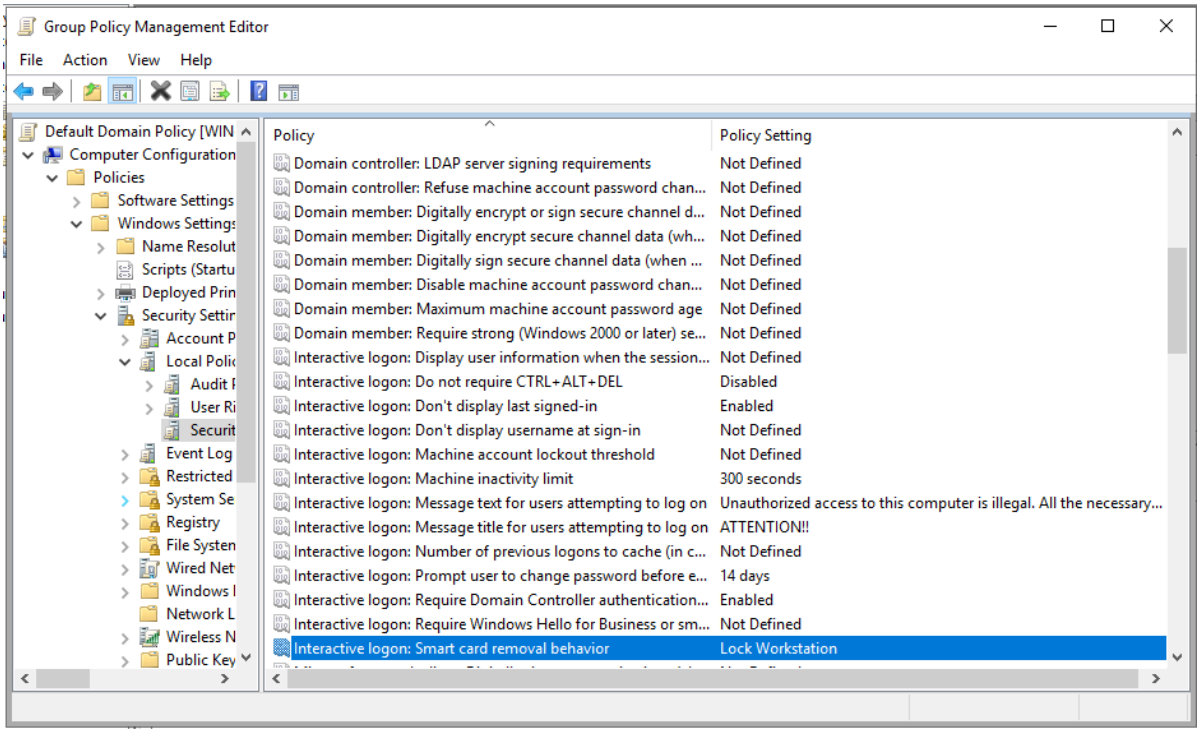


Image 66-Ensure 'Interactive logon: Require Domain Controller Authentication to unlock workstation' is set to 'Enabled'

3.2.5 Microsoft network client

3.2.5.1 Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled'

This policy setting controls whether the SMB client must use packet signing. It is essential to match this setting with the "Microsoft network server: Digitally sign communications (always)" setting on remote servers, particularly when Windows Vista-based computers connect to file or print shares.

The recommended configuration is: Enabled.

Enabling packet signing helps defend against session hijacking attacks, where attackers intercept and modify SMB packets to disrupt or steal sessions. Unsigned SMB packets are vulnerable to such attacks, which can lead to unauthorized data access and modifications. By requiring packet signing, both the client and server are authenticated, ensuring secure and reliable communication.

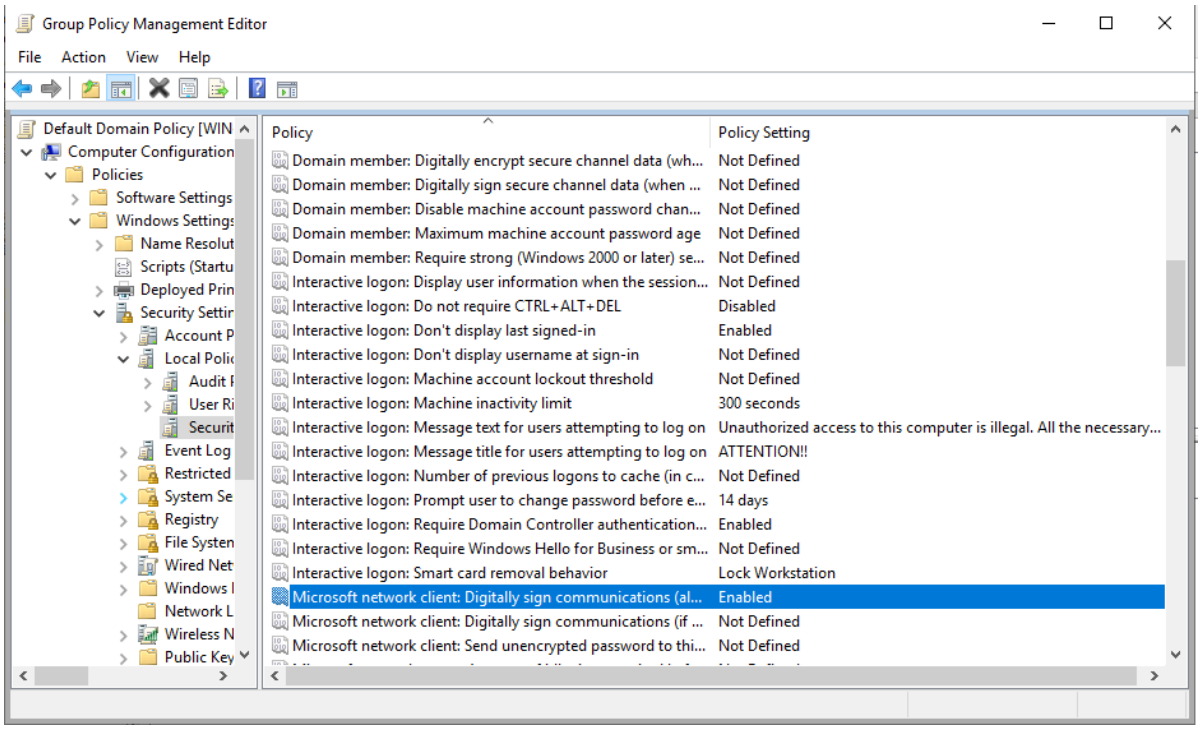


Image 67-Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled'

3.2.5.2 Ensure 'Microsoft network client: Digitally sign communications (if server agrees)' is set to 'Enabled'

This policy setting specifies whether the SMB client will attempt to negotiate SMB packet signing. Enabling this setting ensures that the client is fully capable of using packet signing with all servers and clients within the network.

The recommended configuration is: Enabled.

Session hijacking involves attackers intercepting and manipulating SMB packets to disrupt or steal sessions. By not using packet signing, these unsigned packets are vulnerable to interception and modification, which could result in unauthorized access or undesirable actions on the server. SMB, a resource-sharing protocol supported by many Windows operating systems and the basis for NetBIOS and other protocols, uses signatures to authenticate users and servers. Proper authentication ensures secure data transmission by preventing unauthorized access if either party fails the authentication process.

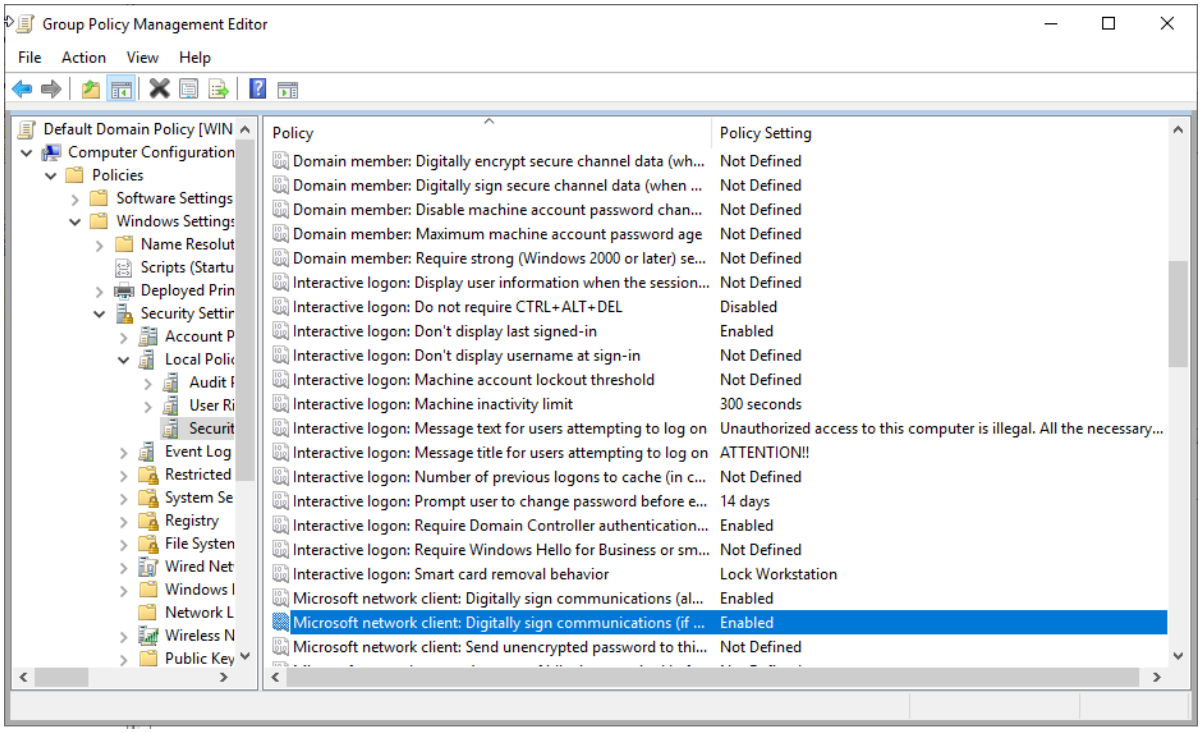


Image 68-Ensure 'Microsoft network client: Digitally sign communications (if server agrees)' is set to 'Enabled'

3.2.5.3 Ensure 'Microsoft network client: Send unencrypted password to third-party SMB servers' is set to 'Disabled'

This policy setting determines whether the SMB redirector will transmit plaintext passwords during authentication with third-party SMB servers that do not support password encryption. It is advised to disable this setting unless there is a compelling business reason to enable it, as enabling it would permit the transmission of unencrypted passwords across the network.

The recommended state for this setting is: Disabled.

Enabling this policy allows passwords to be sent in plaintext, which poses a serious security risk. These third-party servers might not implement the SMB security features available in Windows Server 2003, increasing the vulnerability of password data during transmission.

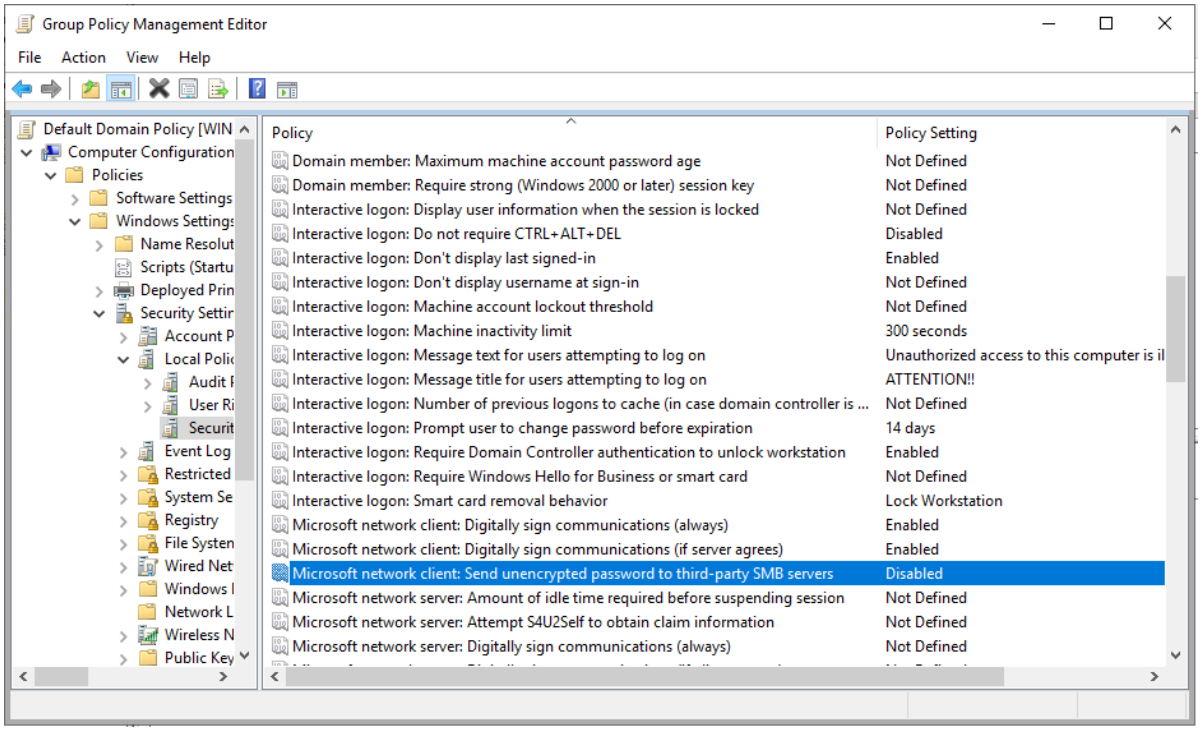


Image 69-Ensure 'Microsoft network client: Send unencrypted password to third-party SMB servers' is set to 'Disabled'

3.2.6 Microsoft network server

3.2.6.1 Ensure 'Microsoft network server: Amount of idle time required before suspending session' is set to '15 or fewer minute(s)'

This policy setting allows you to define the duration of idle time that must elapse before an SMB session is suspended due to inactivity. Administrators can use this setting to manage when inactive SMB sessions are automatically suspended, with the session being reestablished if client activity resumes.

The maximum allowable value is 99999 minutes, which equates to over 69 days and effectively disables the setting.

The recommended state for this setting is: 15 minutes or less.

Each SMB session uses server resources, and an excessive number of idle sessions can degrade server performance or cause it to become unresponsive. An attacker might exploit this by repeatedly initiating SMB sessions, potentially leading to server slowdowns or failures.

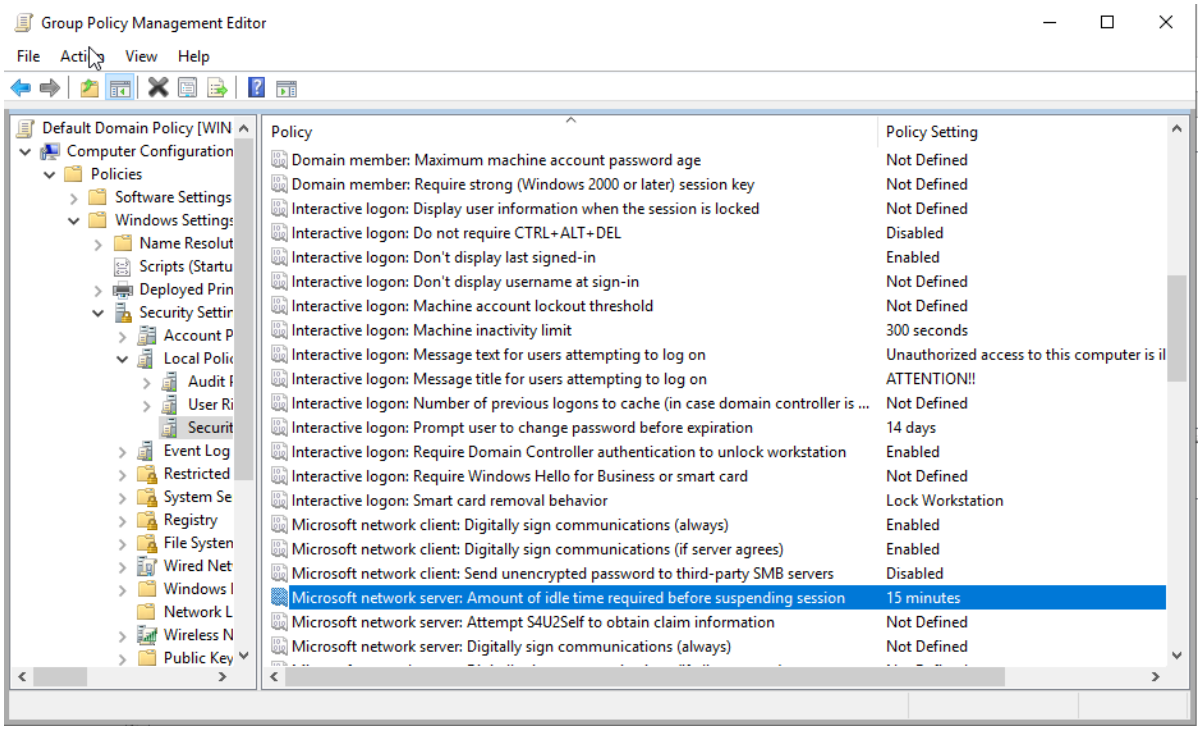


Image 70-Ensure 'Microsoft network server: Amount of idle time required before suspending session' is set to '15 or fewer minute(s)'

3.2.6.2 Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled'

This policy setting determines whether packet signing is mandatory for the SMB server component. Enabling this setting is advisable in mixed environments to ensure that downstream clients cannot use the workstation as a network server.

The recommended state for this setting is: Enabled.

Session hijacking tools can allow attackers with network access to disrupt or steal ongoing sessions. Unsigned SMB packets can be intercepted and altered, potentially leading to unauthorized actions by the server. Attackers might also impersonate legitimate servers or clients after authentication to gain unauthorized data access. SMB, a resource-sharing protocol used by many Windows operating systems, relies on signatures to authenticate both users and servers. Without proper authentication, data transmission cannot occur.

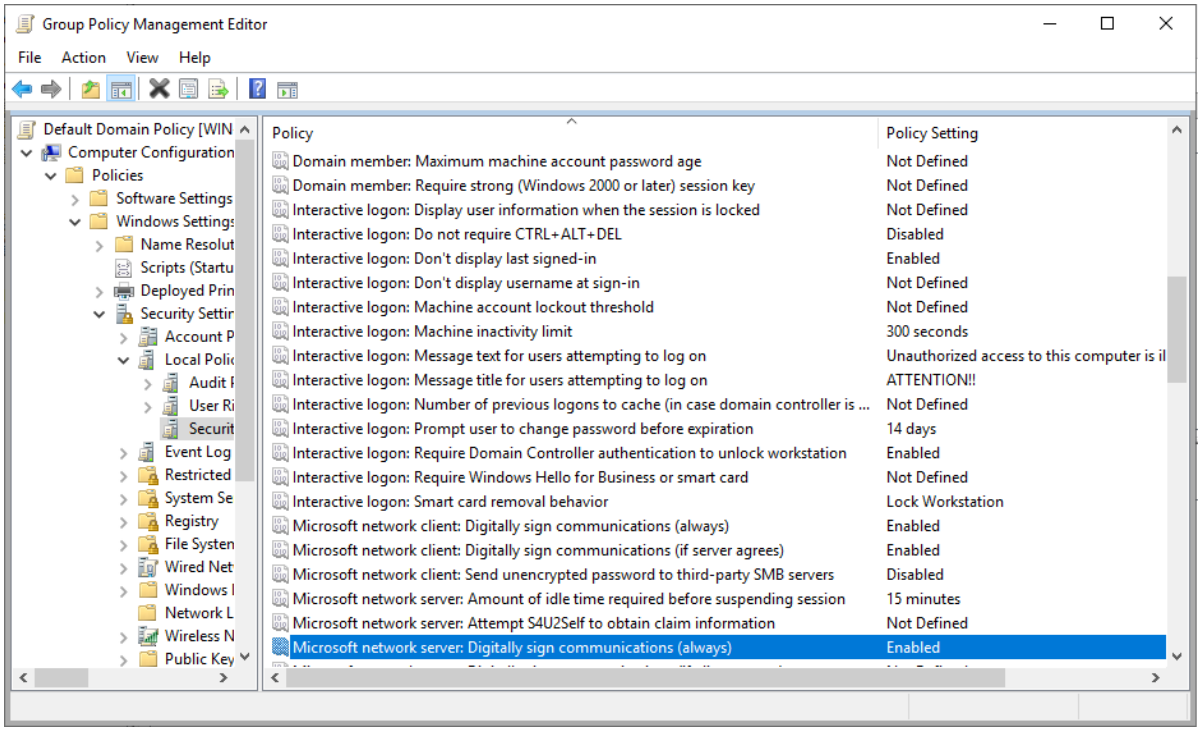


Image 71-Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled'

3.2.6.3 Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled'

This policy setting governs whether the SMB server will negotiate SMB packet signing with clients that request it. If a client does not request signing, and if the setting for "Microsoft network server: Digitally sign communications (always)" is not enabled, the connection will proceed without a signature.

For optimal security, it is recommended to enable this policy setting, ensuring that SMB clients on your network are fully effective for packet signing with all clients and servers in your environment.

Session hijacking can occur when attackers with network access interrupt or steal active sessions. Unsigned SMB packets can be intercepted and modified, potentially leading to unauthorized server actions or data access. SMB, a protocol supported by many Windows operating systems and the basis for NetBIOS and other protocols, uses signatures to authenticate both users and servers. If either party fails authentication, data transmission is blocked.

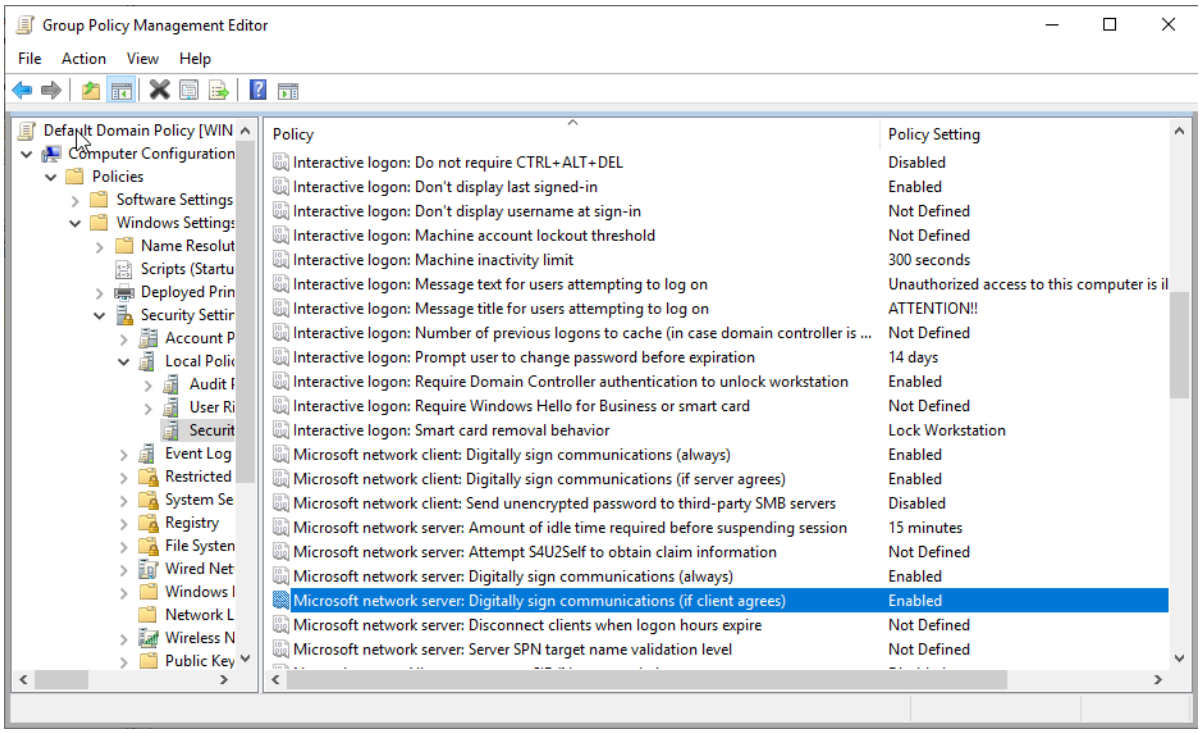


Image 72-Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled'

3.2.6.4 Ensure 'Microsoft network server: Disconnect clients when logon hours expire' is set to 'Enabled'

This security setting controls whether users are disconnected from the local computer if they access it outside their designated logon hours. This setting impacts the Server Message Block (SMB) component. Enabling this policy should be accompanied by enabling "Network security: Force logoff when logon hours expire (Rule 2.3.11.6)" to ensure comprehensive enforcement.

The recommended configuration for this setting is: Enabled.

If your organization has specific logon hours for users, enabling this policy is crucial. Without it, users might continue to access network resources beyond their allowed hours using sessions established during permitted times.

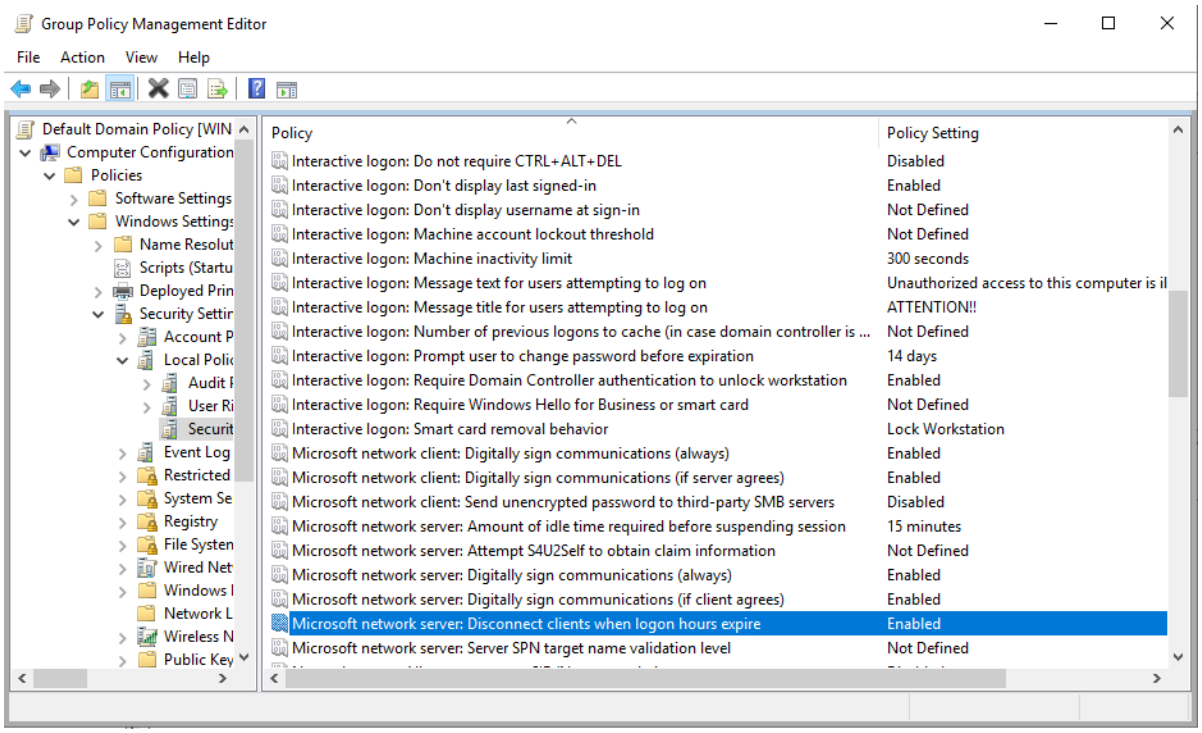


Image 73-Ensure 'Microsoft network server: Disconnect clients when logon hours expire' is set to 'Enabled'

3.2.6.5 Ensure 'Microsoft network server: Server SPN target name validation level' is set to 'Accept if provided by client' or higher

This policy setting determines the level of validation a server performs on the service principal name (SPN) provided by a client when establishing a session using the Server Message Block (SMB) protocol. SMB is fundamental for file and print sharing, as well as other networking functions, including remote Windows administration. The SMB protocol supports SPN validation to protect against SMB relay attacks, which can compromise SMB servers. This setting impacts both SMB1 and SMB2.

The recommended configuration for this setting is: Accept if provided by client. Setting it to Required from client is also compliant with the benchmark.

Since the release of MS KB3161561, this setting may cause significant issues, such as replication problems, group policy editing issues, and blue screen crashes on Domain Controllers when used alongside UNC path hardening (Rule 18.5.14.1). Therefore, CIS advises against deploying this setting on Domain Controllers.

The rationale behind this setting is to prevent unauthorized access to network resources by spoofing the identity of a computer.

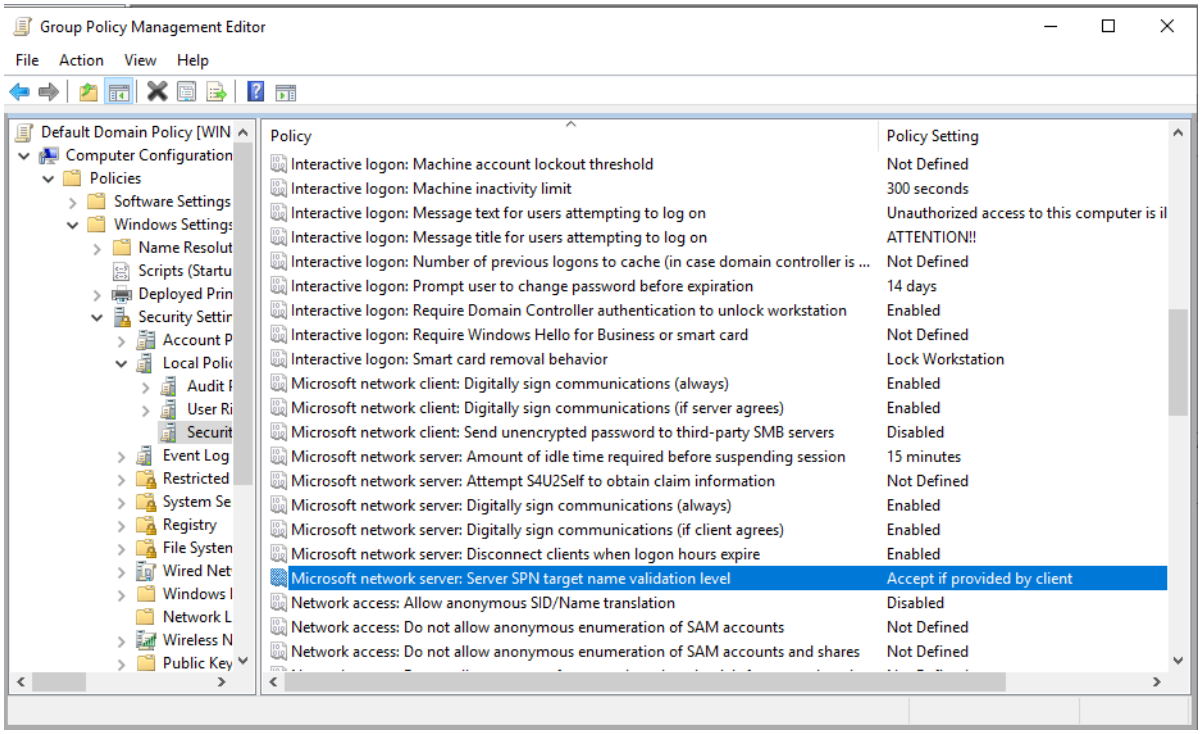


Image 74-Ensure 'Microsoft network server: Server SPN target name validation level' is set to 'Accept if provided by client' or higher

3.2.7 Network access

3.2.7.1 Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled'

This policy setting controls whether an anonymous user can request security identifier (SID) attributes for another user or use a SID to retrieve its associated user name. The recommended state for this setting is: Disabled.

If enabled, a local user could exploit this setting to discover the real name of the built-in Administrator account by querying the well-known Administrator SID, even if the account has been renamed. This information could then be used to attempt a password guessing attack.

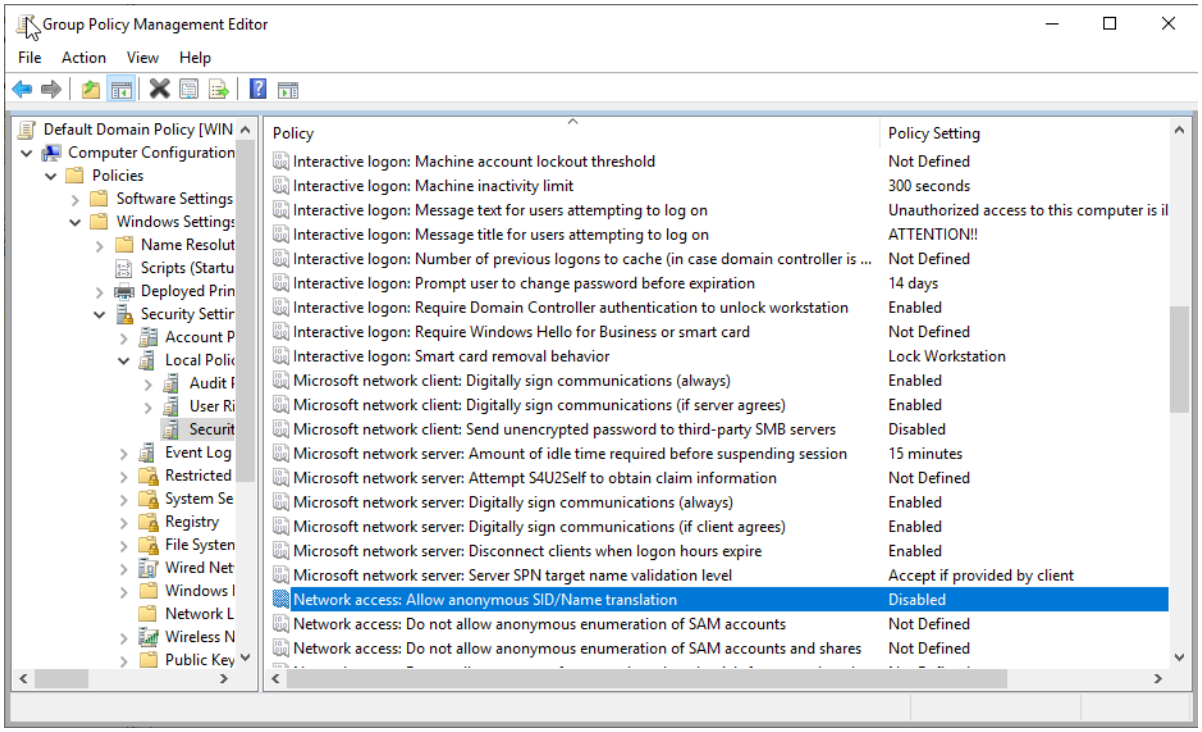


Image 75-Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled'

3.2.7.2 Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts' is set to 'Enabled'

This policy setting controls the ability of anonymous users to enumerate accounts in the Security Accounts Manager (SAM). If you enable this policy setting, users with anonymous connections will not be able to enumerate domain account user names on the systems in your environment. This policy setting also allows additional restrictions on anonymous connections.

The recommended state for this setting is: Enabled.

An unauthorized user could anonymously list account names and use the information to attempt to guess passwords or perform social engineering attacks.

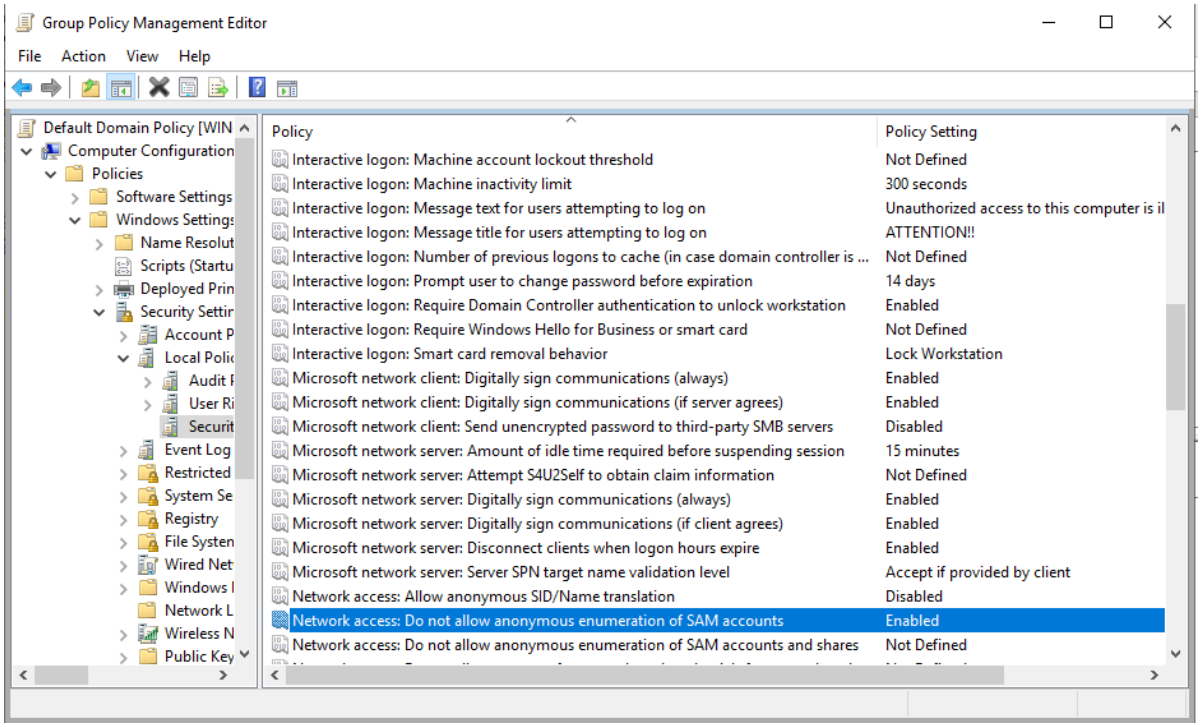


Image 76-Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts' is set to 'Enabled'

3.2.7.3 Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled'

This policy setting regulates whether anonymous users can enumerate Security Accounts Manager (SAM) accounts and network shares. When enabled, it prevents anonymous users from listing domain account user names and network share names on your systems.
The recommended state for this setting is: Enabled.
Unauthorized users could exploit this setting to gather information about account names and shared resources, which might then be used to guess passwords or carry out social engineering attacks to obtain sensitive security information.

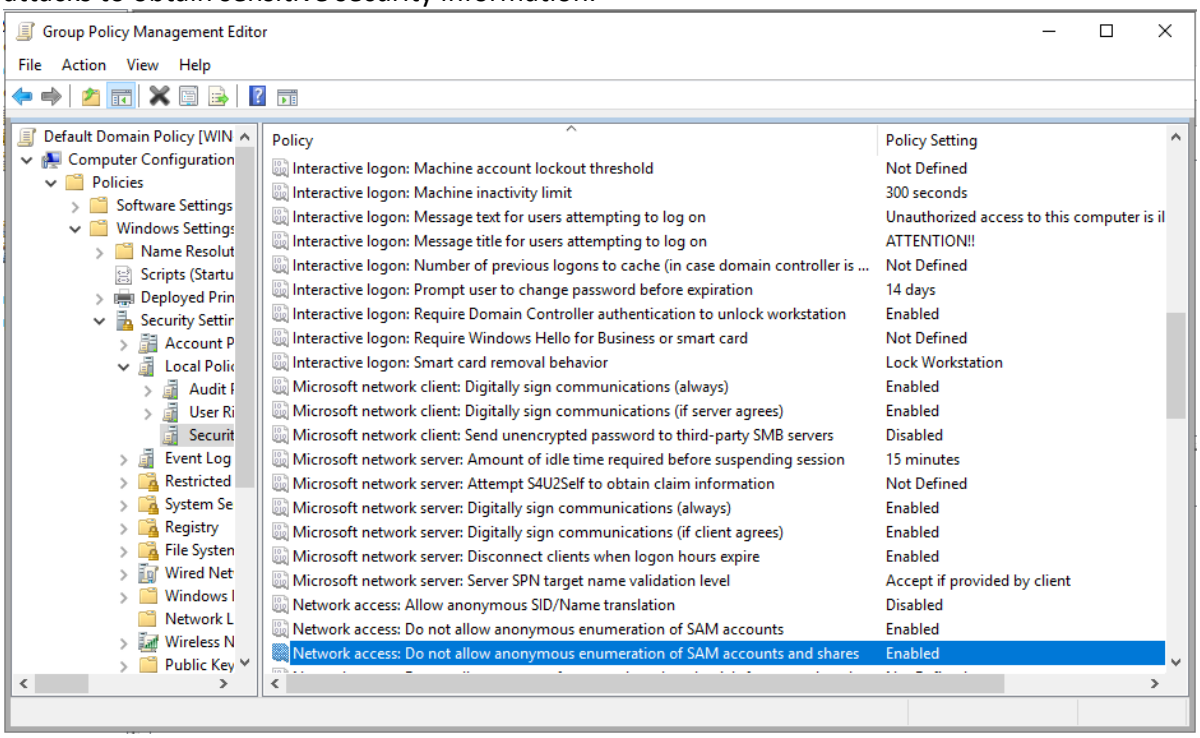


Image 77-Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled'

3.2.7.4 Ensure 'Network access: Do not allow storage of passwords and credentials for network authentication' is set to 'Enabled'

This policy setting determines whether Credential Manager, previously known as Stored User Names and Passwords, should save passwords or credentials for future use after domain authentication.

The recommended state for this setting is: Enabled.

Changes to this setting will only take effect after a restart of Windows. Cached passwords can be accessed by the user while logged into the computer, but this can become a security issue if the user inadvertently runs malicious code that extracts and sends these passwords to unauthorized individuals.

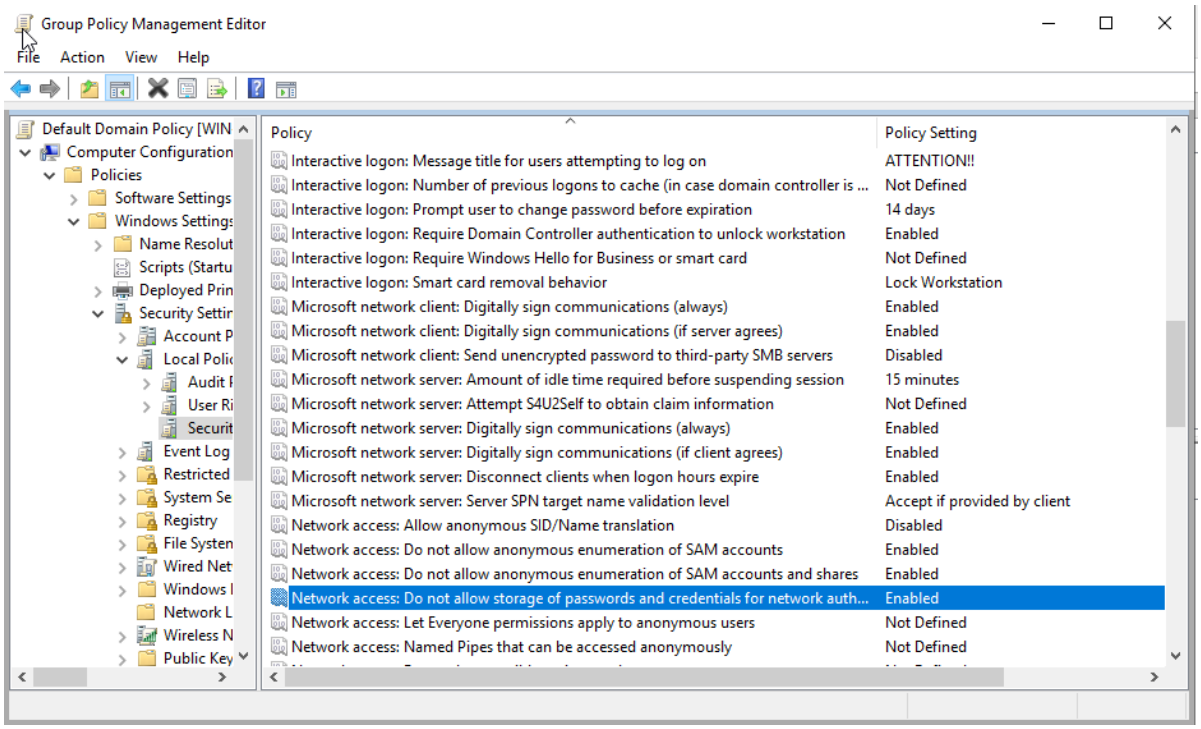


Image 78-Ensure 'Network access: Do not allow storage of passwords and credentials for network authentication' is set to 'Enabled'

3.2.7.5 Ensure 'Network access: Let Everyone permissions apply to anonymous users' is set to 'Disabled'

This policy setting specifies the additional permissions granted to anonymous connections on the computer.

The recommended state for this setting is: Disabled.

Allowing additional permissions for anonymous connections can enable unauthorized users to list account names and shared resources, potentially leading to password guessing, social engineering attacks, or denial-of-service (DoS) attacks.

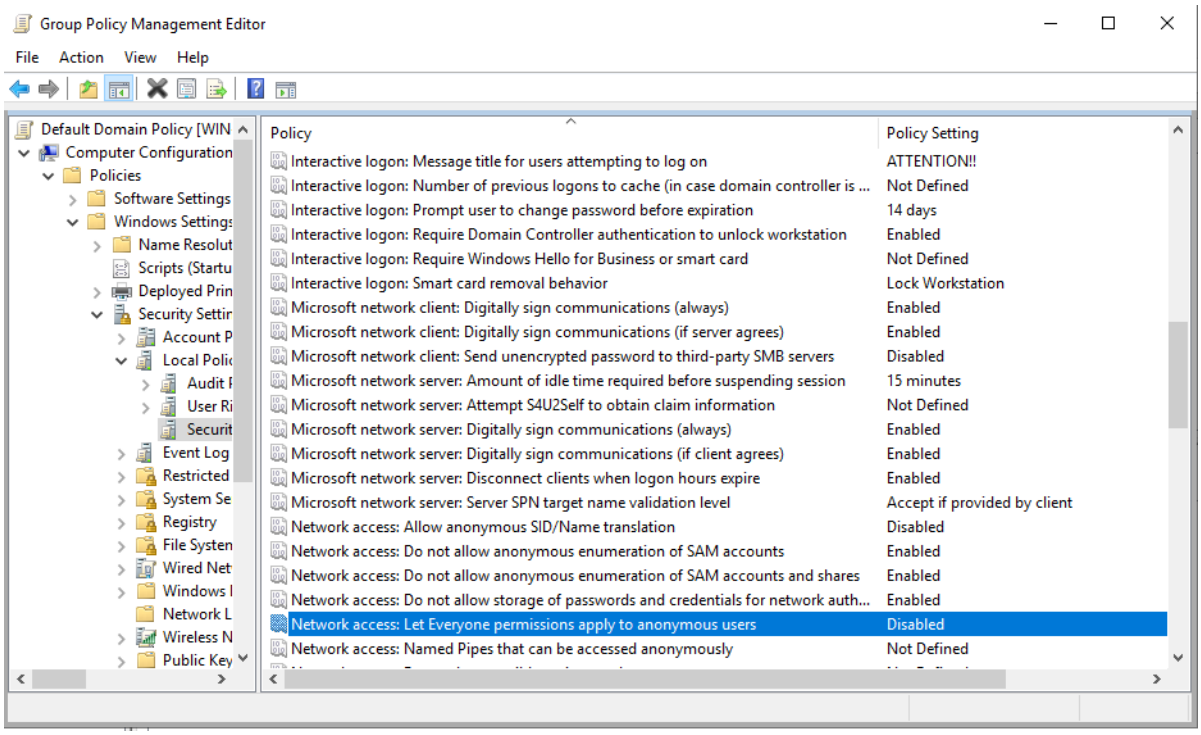


Image 79-Ensure 'Network access: Let Everyone permissions apply to anonymous users' is set to 'Disabled'

3.2.7.6 Configure 'Network access: Named Pipes that can be accessed anonymously'

This policy setting specifies which communication sessions, or pipes, are accessible anonymously, detailing their attributes and permissions.

The recommended state for this setting is: LSARPC, NETLOGON, SAMR, and (if the legacy Computer Browser service is active) BROWSER.

A Member Server with the Remote Desktop Services Role and Remote Desktop Licensing Role Service requires an exception to this policy, allowing anonymous access to HydraLSPipe and TermServLicensing Named Pipes.

Restricting anonymous access to named pipes helps minimize the system's attack surface.

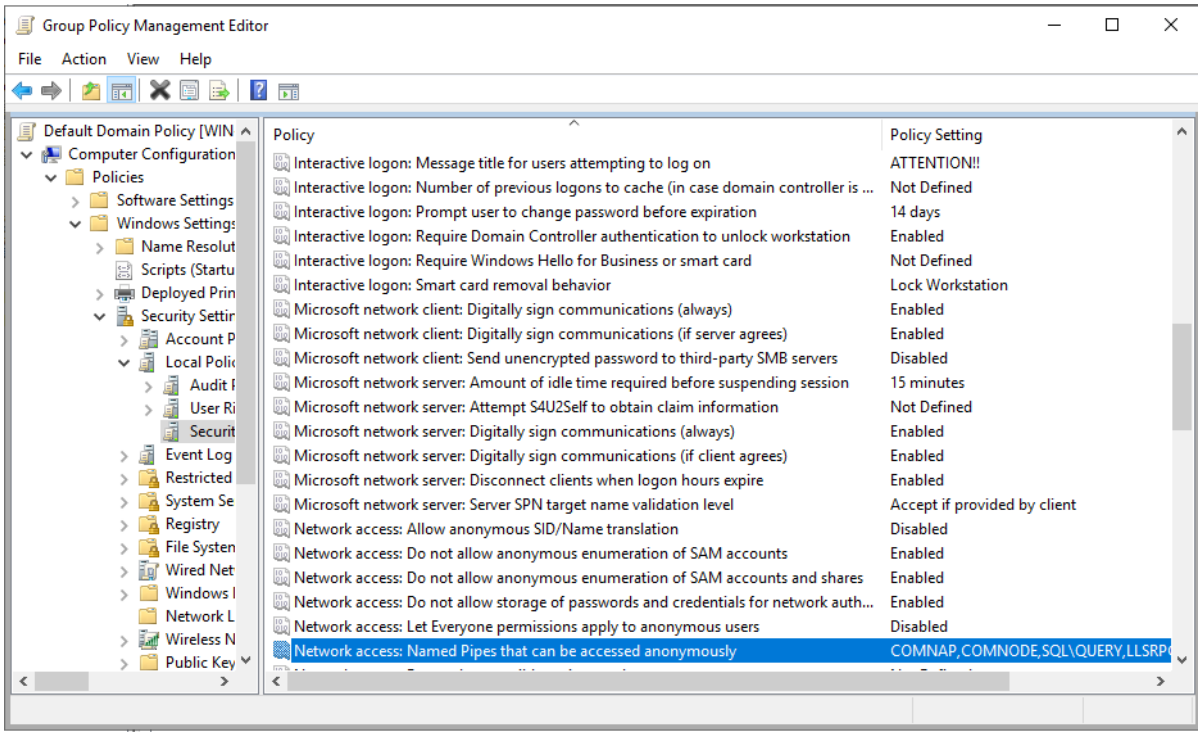


Image 80-Configure 'Network access: Named Pipes that can be accessed anonymously'

3.2.7.7 Configure 'Network access: Remotely accessible registry paths' is configured

This policy setting specifies which registry paths can be accessed over the network, overriding the permissions listed in the access control list (ACL) of the winreg registry key.

Note that this setting does not apply to Windows XP; it is known as "Network access: Remotely accessible registry paths and sub-paths" in Windows Server 2003, Windows Vista, and Windows Server 2008 (non-R2). When configuring this setting, you enter a list of objects separated by line feeds or carriage returns. Although the list appears comma-delimited in Group Policy Editor and the Resultant Set of Policy console, it is stored as a line-feed delimited list in the registry as a REG_MULTI_SZ value.

The recommended state for this setting includes:

- System\CurrentControlSet\Control\ProductOptions
- System\CurrentControlSet\Control\Server Applications
- Software\Microsoft\Windows NT\CurrentVersion

The registry contains sensitive configuration information that could be exploited by attackers. To mitigate the risk of unauthorized access, appropriate ACLs should be set to protect registry data.

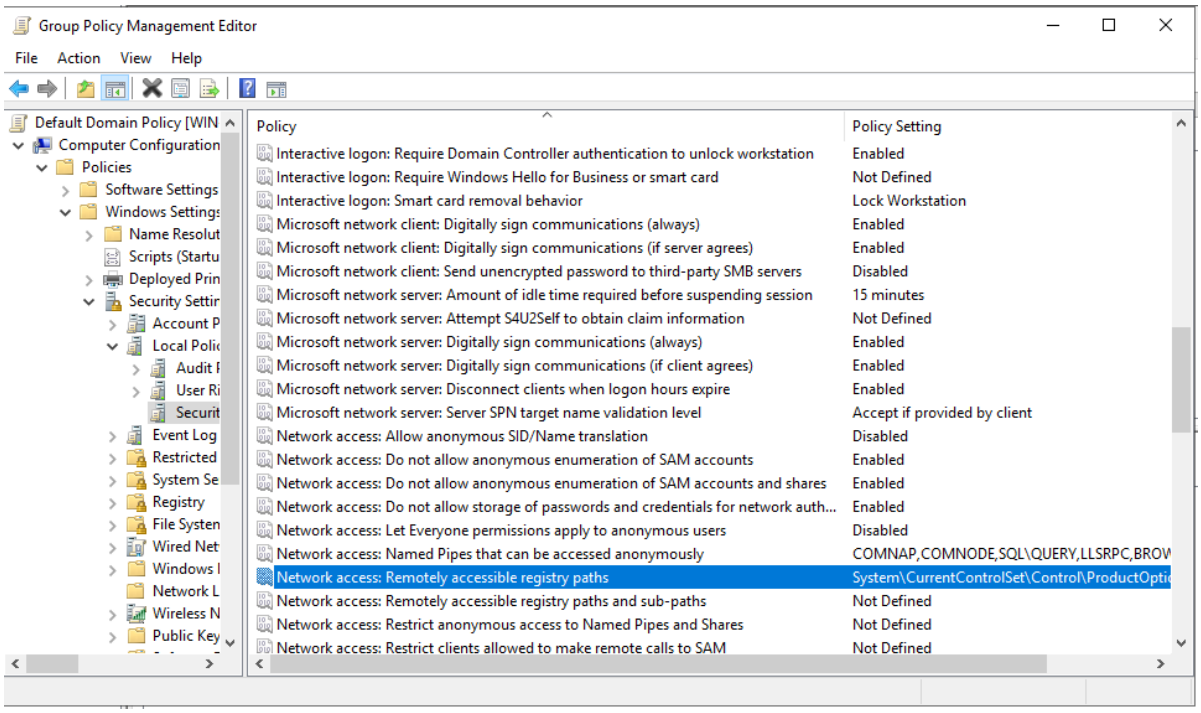


Image 81-Configure 'Network access: Remotely accessible registry paths' is configured

3.2.7.8 Configure 'Network access: Remotely accessible registry paths and sub-paths' is configured

This policy setting defines which registry paths and sub-paths are accessible over the network, overriding the default permissions set in the ACL of the winreg registry key.

In Windows XP, this setting is labeled as "Network access: Remotely accessible registry paths." In Windows Vista, Windows Server 2003, and Windows Server 2008 (non-R2), it uses a similar concept but with different naming conventions. To configure this, list the paths separated by line feeds or carriage returns; this list is stored as a line-feed delimited list in the registry.

Setting appropriate ACLs on these registry paths helps protect sensitive information and reduces the risk of unauthorized access.

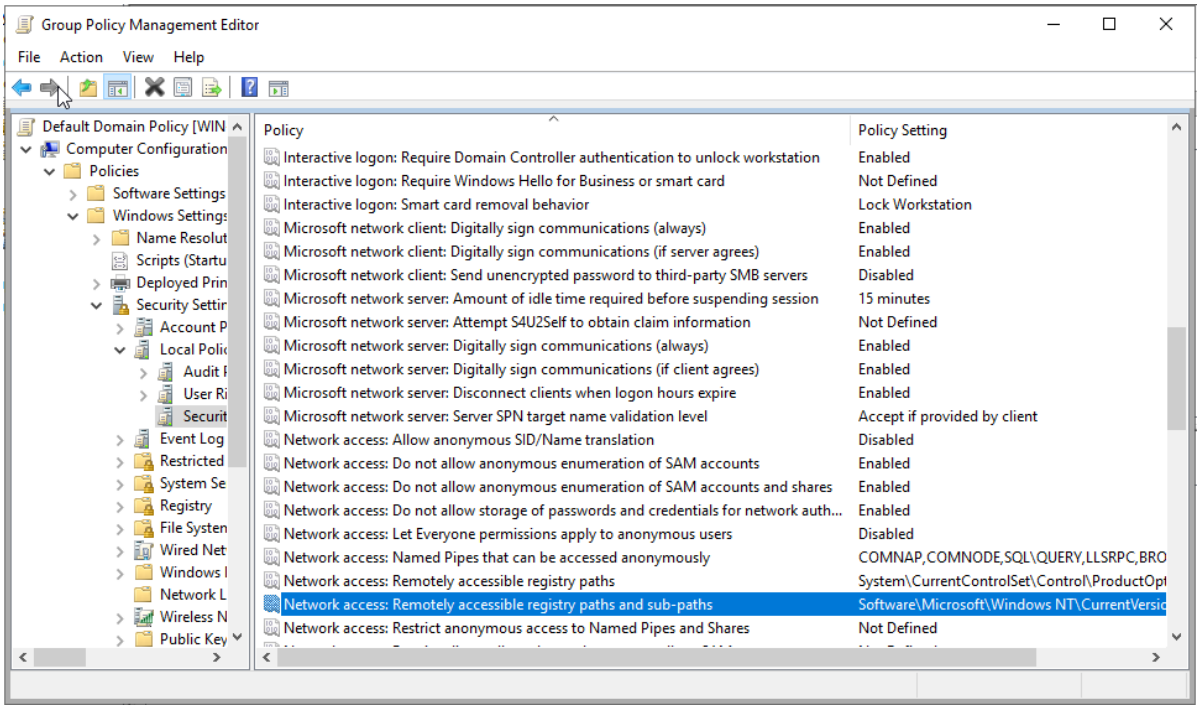


Image 82-Configure 'Network access: Remotely accessible registry paths and sub-paths' is configured

3.2.7.9 Ensure 'Network access: Restrict anonymous access to Named Pipes and Shares' is set to 'Enabled'

When enabled, this policy setting limits anonymous access to only those shares and pipes specified in the "Network access: Named pipes that can be accessed anonymously" and "Network access: Shares that can be accessed anonymously" settings. It manages null session access by setting the RestrictNullSessAccess registry value to 1 in the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters registry key. This configuration controls whether the server service allows unauthenticated clients to access named resources.

The recommended state for this setting is: Enabled.

Null sessions pose a security risk as they can be exploited through shares, including default ones, on your computers.

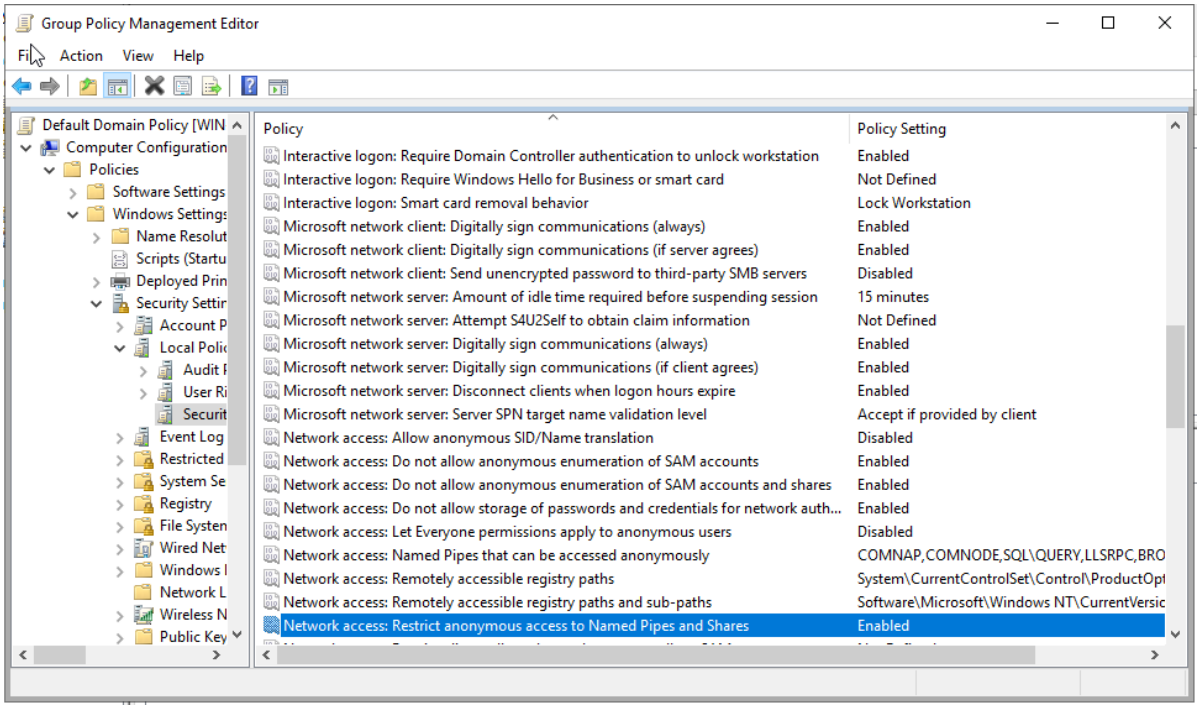


Image 83-Ensure 'Network access: Restrict anonymous access to Named Pipes and Shares' is set to 'Enabled'

3.2.7.10 Ensure 'Network access: Restrict clients allowed to make remote calls to SAM' is set to 'Administrators: Remote Access: Allow'

This policy setting restricts remote RPC connections to SAM, with the recommended state being "Administrators: Remote Access: Allow." It requires Windows 10 R1607, Server 2016, or newer to access and set this value in Group Policy. Originally supported only on Windows Server 2016 or newer, it was extended to Windows Server 2008 R2 or newer via March 2017 security patches. For organizations using Azure Advanced Threat Protection (APT), the "AATP Service" account needs to be added to the recommended configuration to enable lateral movement path detection in Microsoft Defender for Identity. This setting helps prevent unauthorized users from anonymously listing local account names or groups, which could be used to guess passwords or conduct social engineering attacks.

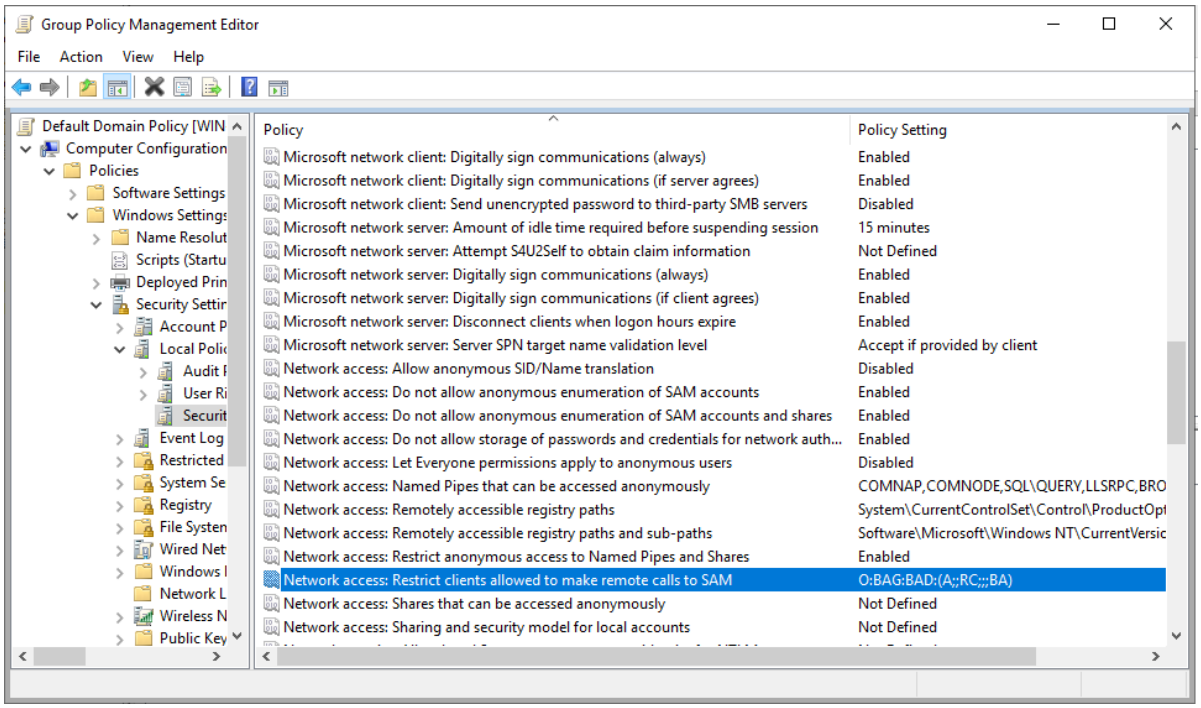


Image 84-Ensure 'Network access: Restrict clients allowed to make remote calls to SAM' is set to 'Administrators: Remote Access: Allow'

3.2.7.11 Ensure 'Network access: Shares that can be accessed anonymously' is set to 'None'

This policy setting controls which network shares can be accessed by anonymous users. By default, this setting has minimal effect since all users must be authenticated to access shared resources on the server. The recommended state is to leave this setting blank (i.e., none). Allowing any values in this setting is highly risky, as listed shares would be accessible by any network user, potentially leading to the exposure or corruption of sensitive data.

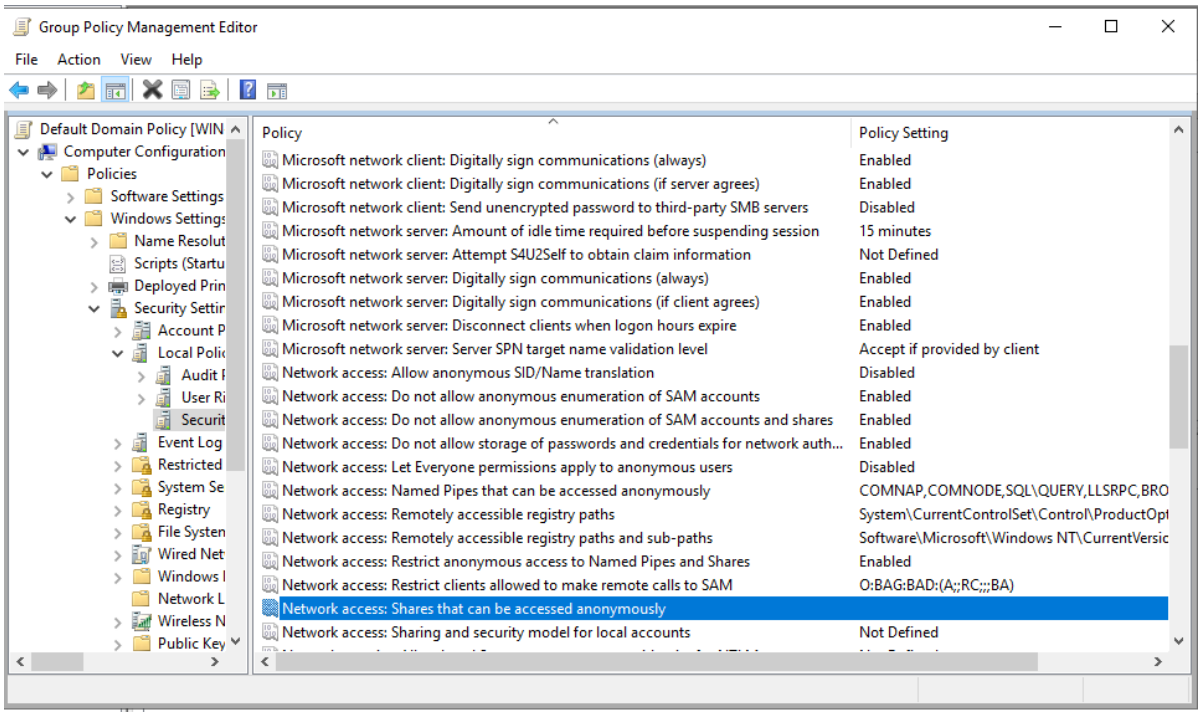


Image 85-Ensure 'Network access: Shares that can be accessed anonymously' is set to 'None'

3.2.7.12 Ensure 'Network access: Sharing and security model for local accounts' is set to 'Classic - local users authenticate as themselves'

This policy setting determines how network logons using local accounts are authenticated. The Classic option allows for detailed control over resource access, enabling different access levels for various users on the same resource. The Guest only option treats all users equally, authenticating them as Guest with the same access level to a resource. The recommended state is Classic, where local users authenticate as themselves. This setting does not affect remote interactive logons via services like Telnet or Remote Desktop Services. The Guest only model increases security by restricting network users to guest privileges, typically preventing write access to shared resources. However, it complicates authorized user access, requiring ACEs for the Guest account in ACLs. In the Classic model, local accounts must be password-protected to prevent unauthorized access to shared resources.

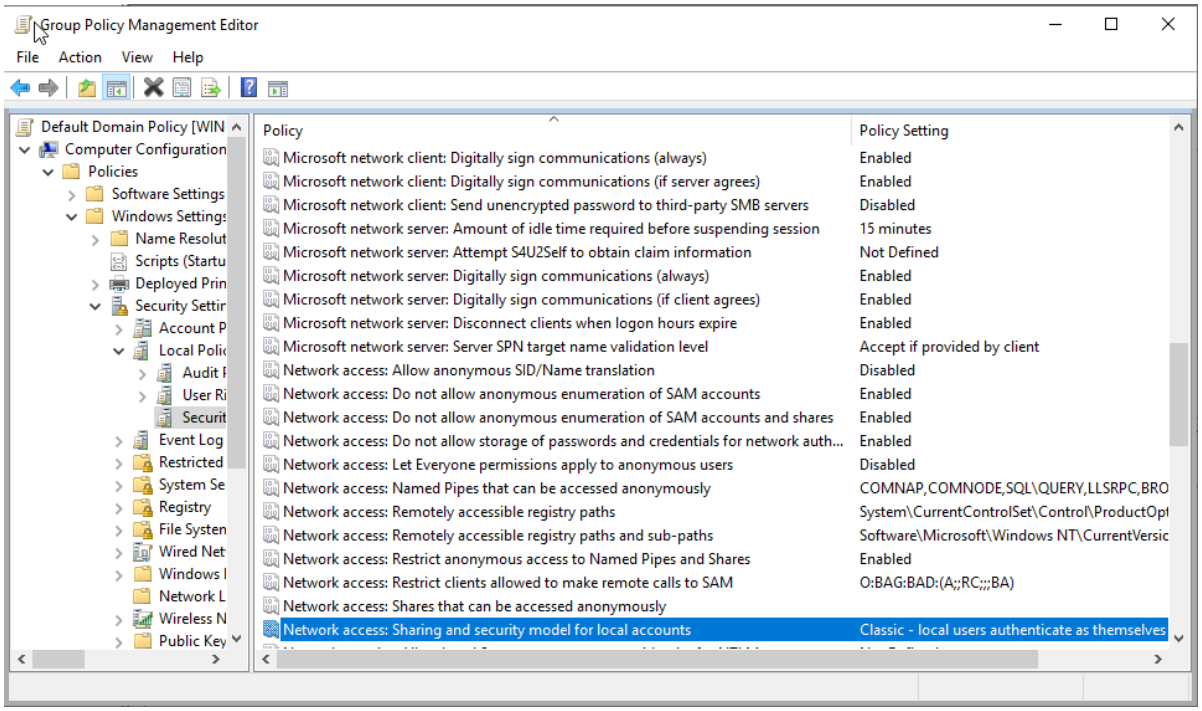


Image 86-Ensure 'Network access: Sharing and security model for local accounts' is set to 'Classic - local users authenticate as themselves'

3.2.8 Network security

3.2.8.1 Ensure 'Network security: Allow Local System to use computer identity for NTLM' is set to 'Enabled'

This policy setting determines if Local System services using Negotiate and reverting to NTLM authentication can utilize the computer identity. It is supported on Windows 7 or Windows Server 2008 R2 and later. The recommended state for this setting is Enabled. When connecting to computers running Windows versions earlier than Vista or Server 2008, services using SPNEGO (Negotiate) that revert to NTLM use the computer identity. In Windows 7, if connecting to a computer running Windows Vista or Server 2008, the system service may use either the computer identity or a NULL session. Using a NULL session generates a system session key that allows signing and encrypting data without errors but offers no protection. Using the computer identity supports both signing and encryption, ensuring data protection.

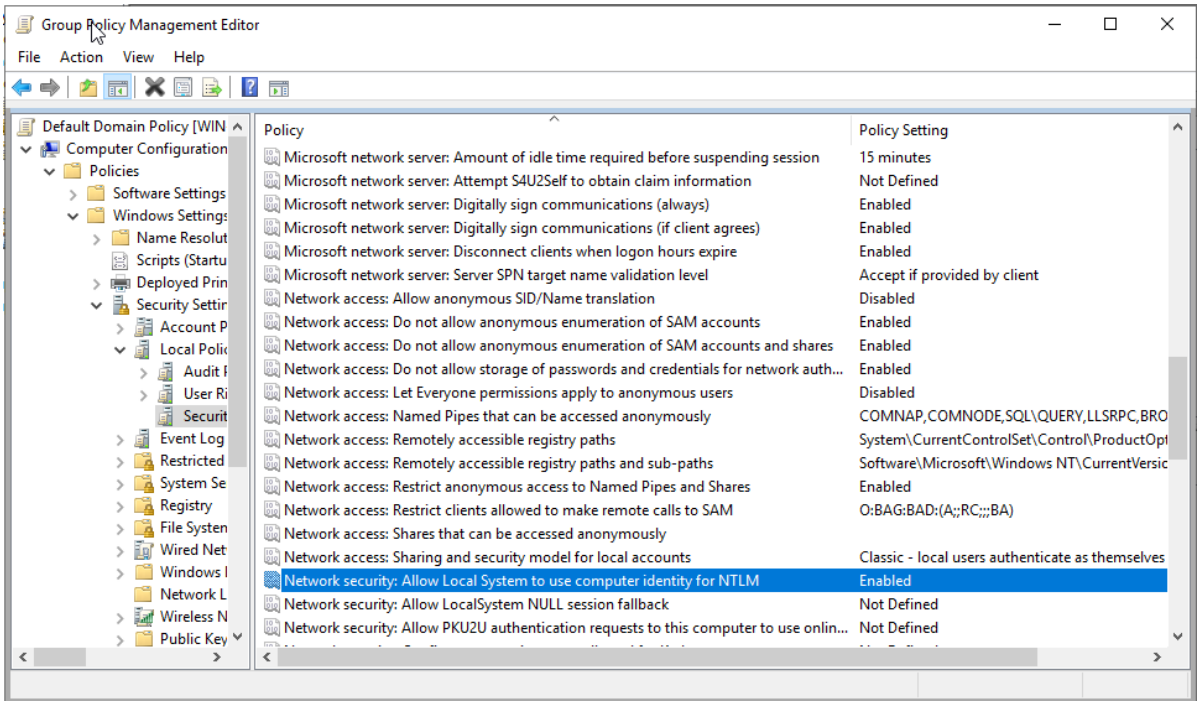


Image 87-Ensure 'Network security: Allow Local System to use computer identity for NTLM' is set to 'Enabled'

3.2.8.2 Ensure 'Network security: Allow LocalSystem NULL session fallback' is set to 'Disabled'

This policy setting controls whether NTLM can revert to a NULL session when used with LocalSystem. The recommended state for this setting is Disabled. NULL sessions are inherently less secure as they are unauthenticated.

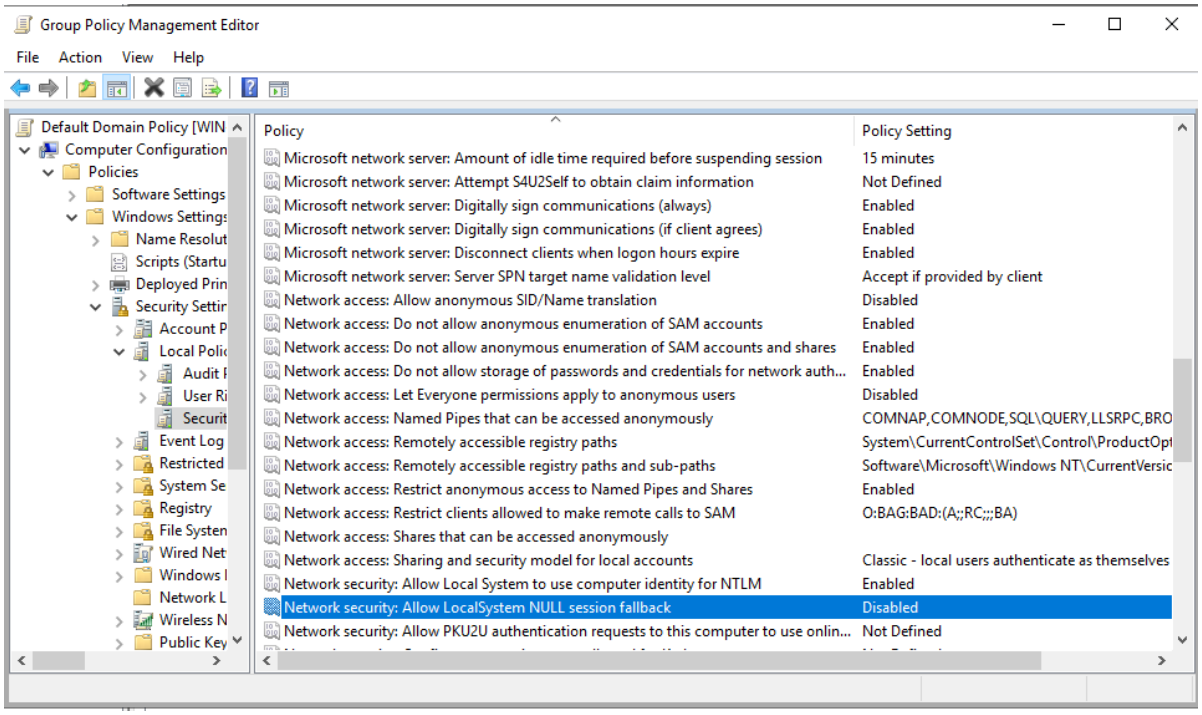


Image 88-Ensure 'Network security: Allow LocalSystem NULL session fallback' is set to 'Disabled'

3.2.8.3 Ensure 'Network Security: Allow PKU2U authentication requests to this computer to use online identities' is set to 'Disabled'

This policy setting determines whether online identities can authenticate to this computer using the Public Key Cryptography Based User-to-User (PKU2U) protocol, which is a peer-to-peer authentication protocol introduced in Windows 7 and Windows Server 2008 R2. This protocol supports peer-to-peer authentication through features like HomeGroup for sharing between non-domain computers. PKU2U extends the Negotiate authentication package with Negoexts.dll, which supports various Microsoft SSPs, including PKU2U. When configured to accept online ID authentication, Negoexts.dll calls PKU2U SSP to exchange certificates and validate logon requests between peer computers. The recommended state for this setting is Disabled, as authentication should typically be managed centrally in most managed networks.

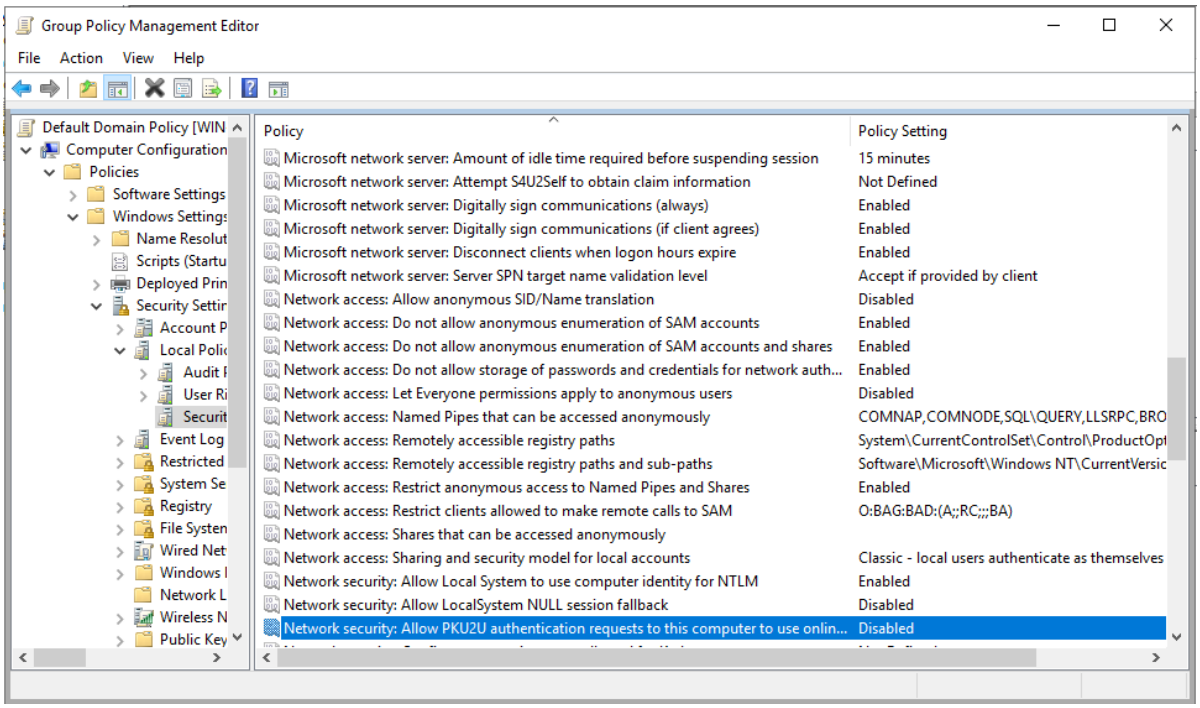


Image 89-Ensure 'Network Security: Allow PKU2U authentication requests to this computer to use online identities' is set to 'Disabled'

3.2.8.4 Ensure 'Network security: Configure encryption types allowed for Kerberos' is set to 'AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types'

This policy setting allows you to specify the encryption types that Kerberos can use. The recommended state is to use AES128_HMAC_SHA1, AES256_HMAC_SHA1, and Future encryption types. Some legacy applications and operating systems may still require RC4_HMAC_MD5, so it's advisable to test your environment to verify if it can be safely removed. Stronger encryption algorithms reduce the risk of compromise, but may cause compatibility issues with systems that do not support them.

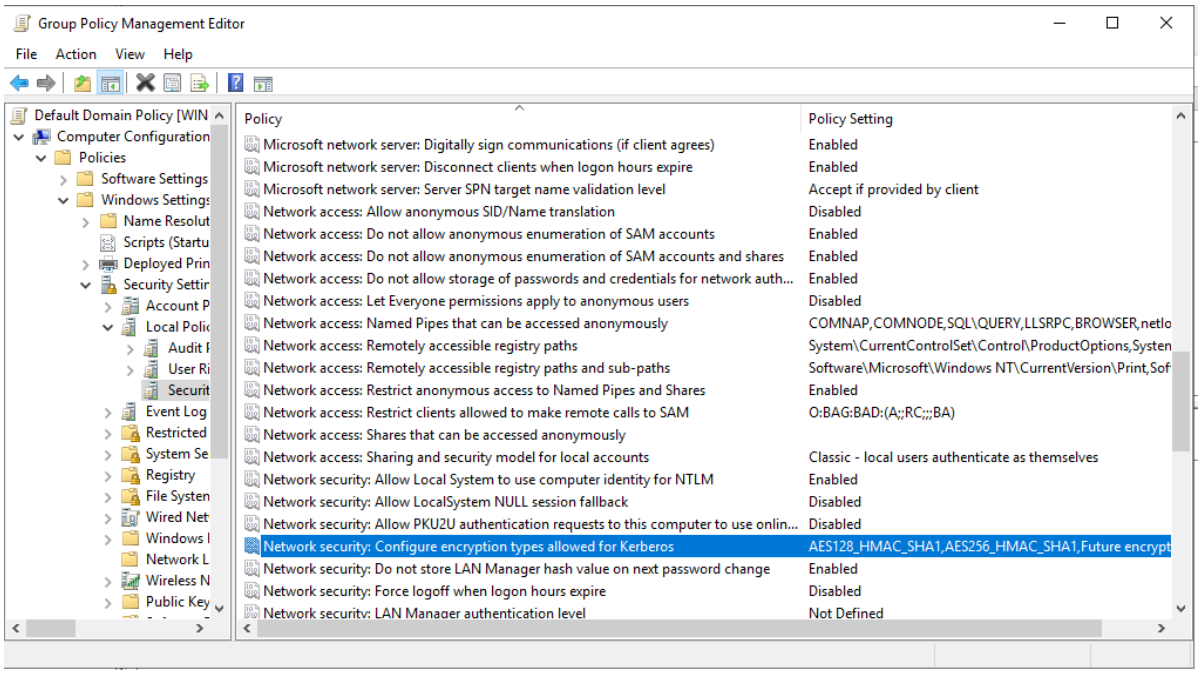


Image 90-Ensure 'Network security: Configure encryption types allowed for Kerberos' is set to 'AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types'

3.2.8.5 Ensure 'Network security: Do not store LAN Manager hash value on next password change' is set to 'Enabled'

This policy setting determines whether the LAN Manager (LM) hash value for a new password is stored when the password is changed. The LM hash is weaker and more vulnerable to attacks compared to the stronger Microsoft Windows NT hash. Storing LM hashes locally in the security database can lead to password compromises if the database is attacked. Note that enabling this setting may cause issues with older operating systems and some third-party applications, and passwords must be changed on all accounts after enabling to take effect. The recommended state for this setting is Enabled. This measure won't prevent attacks on the SAM file, but it will make successful attacks much more difficult.

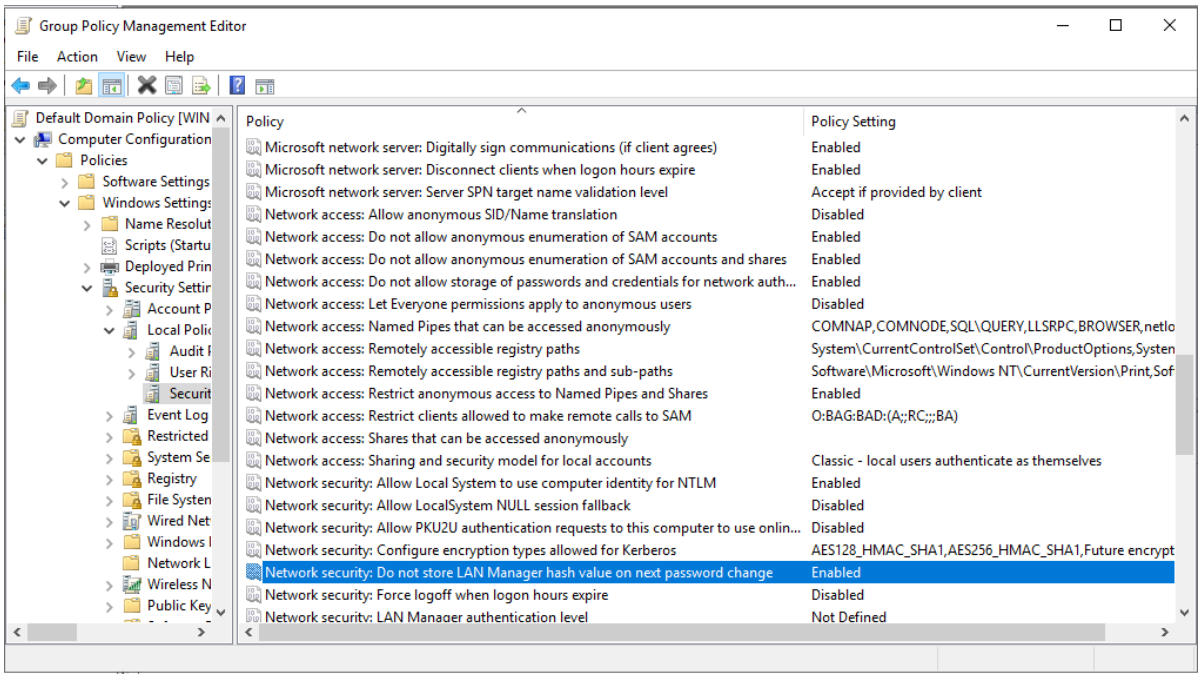


Image 91-Ensure 'Network security: Do not store LAN Manager hash value on next password change' is set to 'Enabled'

3.2.8.6 Ensure 'Network security: Force logoff when logon hours expire' is set to 'Enabled'

This policy setting specifies whether to disconnect users connected to the local computer outside their valid logon hours, affecting the Server Message Block (SMB) component. It is recommended to also enable the "Microsoft network server: Disconnect clients when logon hours expire" setting. The recommended state for this setting is Enabled. Without this setting, users could stay connected beyond their permitted logon hours.

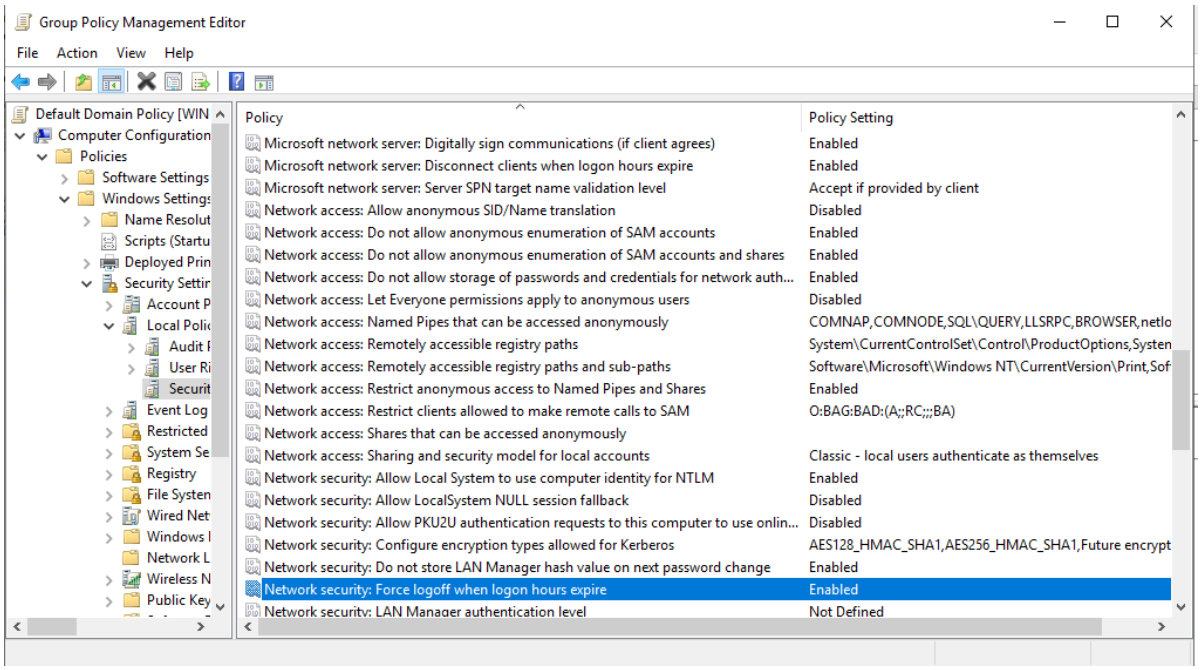


Image 92-Ensure 'Network security: Force logoff when logon hours expire' is set to 'Enabled'

3.2.8.7 Ensure 'Network security: LAN Manager authentication level' is set to 'Send NTLMv2 response only. Refuse LM & NTLM'

LAN Manager (LM) was an early Microsoft client/server software for networking personal computers, offering file and print sharing, security features, and administrative tools. In Active Directory domains, Kerberos is the default authentication protocol, but if it fails, LM, NTLM, or NTLMv2 is used. LM authentication includes LM, NTLM, and NTLMv2 and is used for domain joining, authentication between forests, down-level domains, non-Windows 2000/2003/XP computers, and non-domain computers. The "Network security: LAN Manager authentication level" setting controls the authentication protocol for network logons, affecting client authentication, session security, and server acceptance levels. The recommended setting is "Send NTLMv2 response only. Refuse LM & NTLM." Earlier OS versions sent weaker LM responses, making passwords easier to intercept. Windows 95, 98, and NT systems can't use Kerberos and default to LM and NTLM in Windows Server 2003 domains. Enforcing NTLMv2 increases security. Despite NTLMv2 use for older systems, domain members use Kerberos with Windows Server 2003 or newer Domain Controllers, so restricting LM and NTLM (non-v2) is strongly advised.

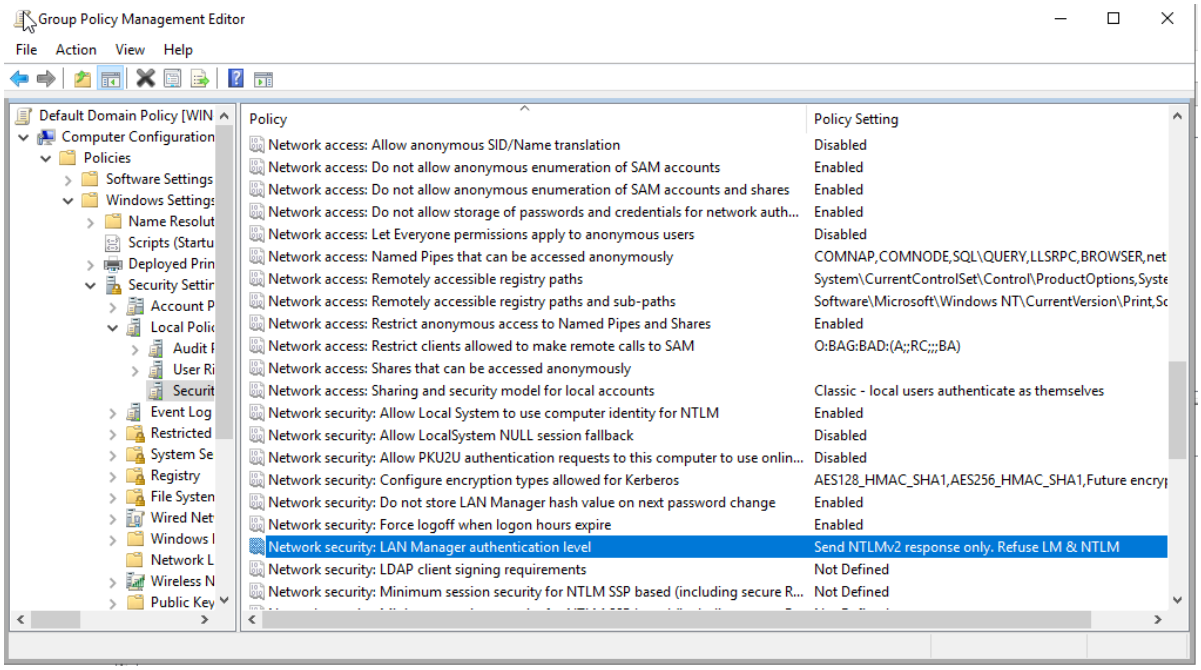


Image 93-Ensure 'Network security: LAN Manager authentication level' is set to 'Send NTLMv2 response only. Refuse LM & NTLM'

3.2.8.8 Ensure 'Network security: LDAP client signing requirements' is set to 'Negotiate signing' or higher

This policy setting controls the level of data signing required for LDAP BIND requests from clients. It does not affect LDAP simple binds (ldap_simple_bind) or LDAP simple binds over SSL (ldap_simple_bind_s), as no Microsoft LDAP clients in Windows XP Professional use these methods for Domain Controller communication. The recommended configuration is "Negotiate signing," though setting it to "Require signing" also meets the benchmark standards.

Unsigned network traffic is vulnerable to man-in-the-middle attacks, where an attacker intercepts and alters packets between the client and server, potentially leading the server to act on incorrect or tampered data from LDAP queries. To mitigate this risk, it's essential to enforce strong physical network security and require digital signatures on all network packets using IPsec authentication headers.

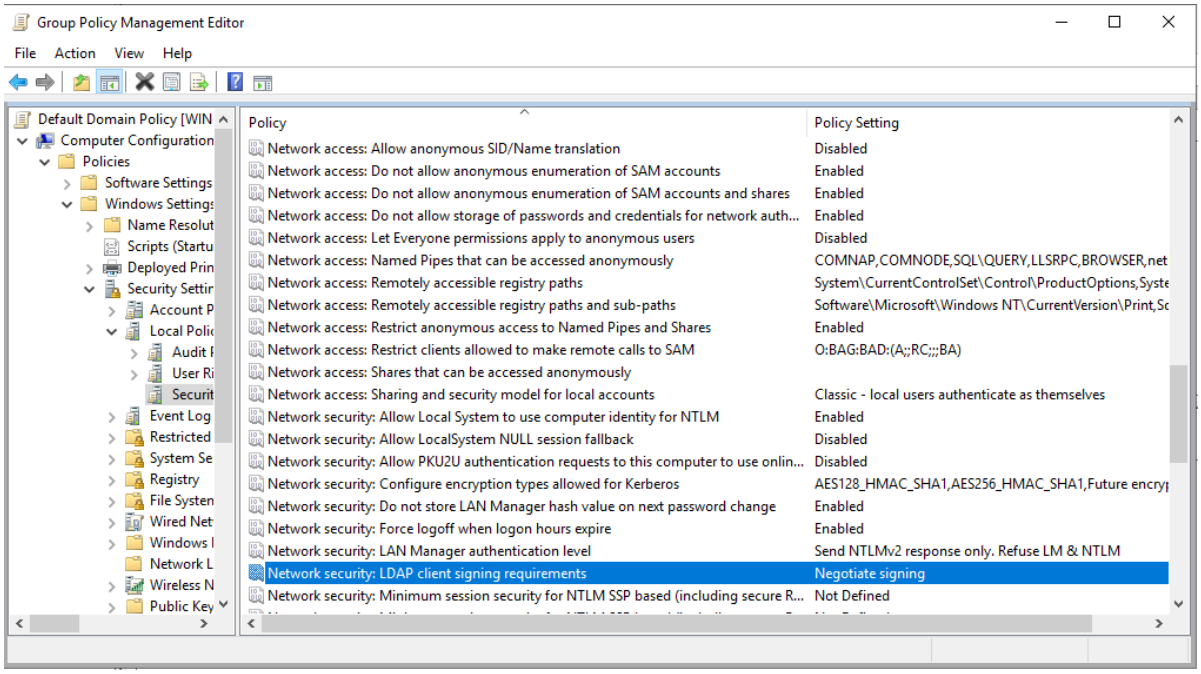


Image 94-Ensure 'Network security: LDAP client signing requirements' is set to 'Negotiate signing' or higher

3.2.8.9 Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' is set to 'Require NTLMv2 session security, Require 128-bit encryption'

This policy setting governs the allowed behaviors for clients using the NTLM Security Support Provider (SSP) for authentication services. It doesn't change the authentication process itself but mandates specific behaviors in applications that use the SSPI. The recommended configuration is to "Require NTLMv2 session security" and "Require 128-bit encryption."

These settings are influenced by the "Network security: LAN Manager Authentication Level" configuration. Enabling both options helps secure network traffic using NTLM SSP by protecting it from exposure or tampering, thereby mitigating risks associated with man-in-the-middle attacks.

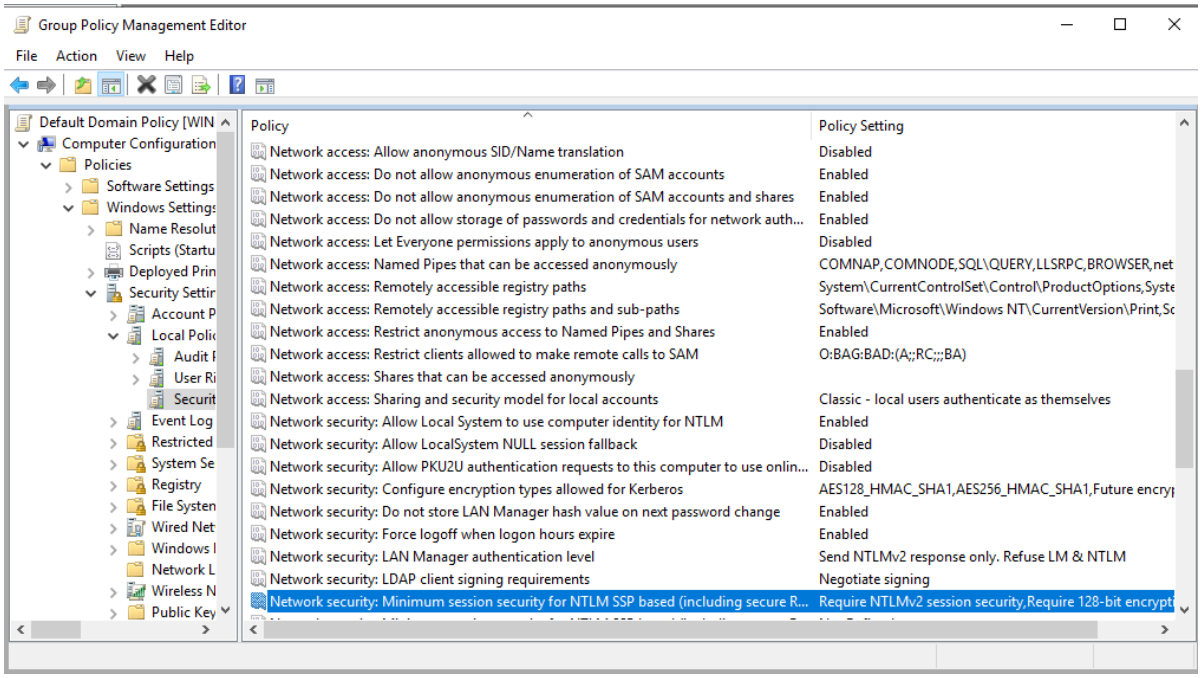


Image 95-Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' is set to 'Require NTLMv2 session security, Require 128-bit encryption'

3.2.8.10 Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require NTLMv2 session security, Require 128-bit encryption'

This policy setting controls the behaviors permitted by servers for applications utilizing the NTLM Security Support Provider (SSP). While it does not alter the authentication process itself, it enforces specific requirements for applications using the SSPI. The recommended configuration is to "Require NTLMv2 session security" and "Require 128-bit encryption." These settings are linked to the "Network security: LAN Manager Authentication Level" configuration. Enabling these options enhances protection for network traffic that uses NTLM SSP, reducing the risk of exposure or tampering by attackers and defending against man-in-the-middle attacks.

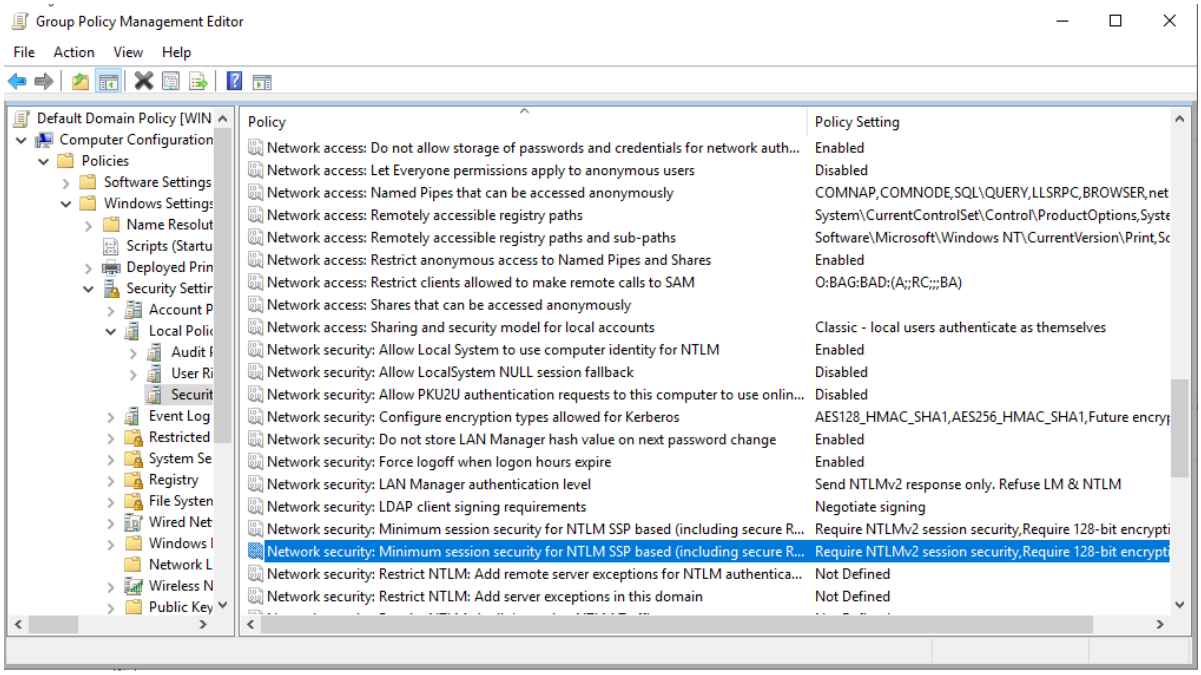


Image 96-Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require NTLMv2 session security, Require 128-bit encryption'

3.2.8.11 Ensure 'Network security: Restrict NTLM: Audit Incoming NTLM Traffic' is set to 'Enable auditing for all accounts'

This policy setting enables the auditing of incoming NTLM traffic, with events logged in the operational event log (e.g., Applications and Services Log\Microsoft\Windows\NTLM). The recommended configuration is to enable auditing for all accounts. Auditing NTLM traffic helps identify systems using this outdated authentication protocol, allowing for remediation to more secure alternatives like Kerberos. Additionally, the log data is valuable for forensic investigations following malicious attacks. NTLM and NTLMv2 are susceptible to various attacks, such as SMB relay, man-in-the-middle, and brute force attacks. Reducing or eliminating NTLM authentication lowers the risk of attackers accessing network systems.

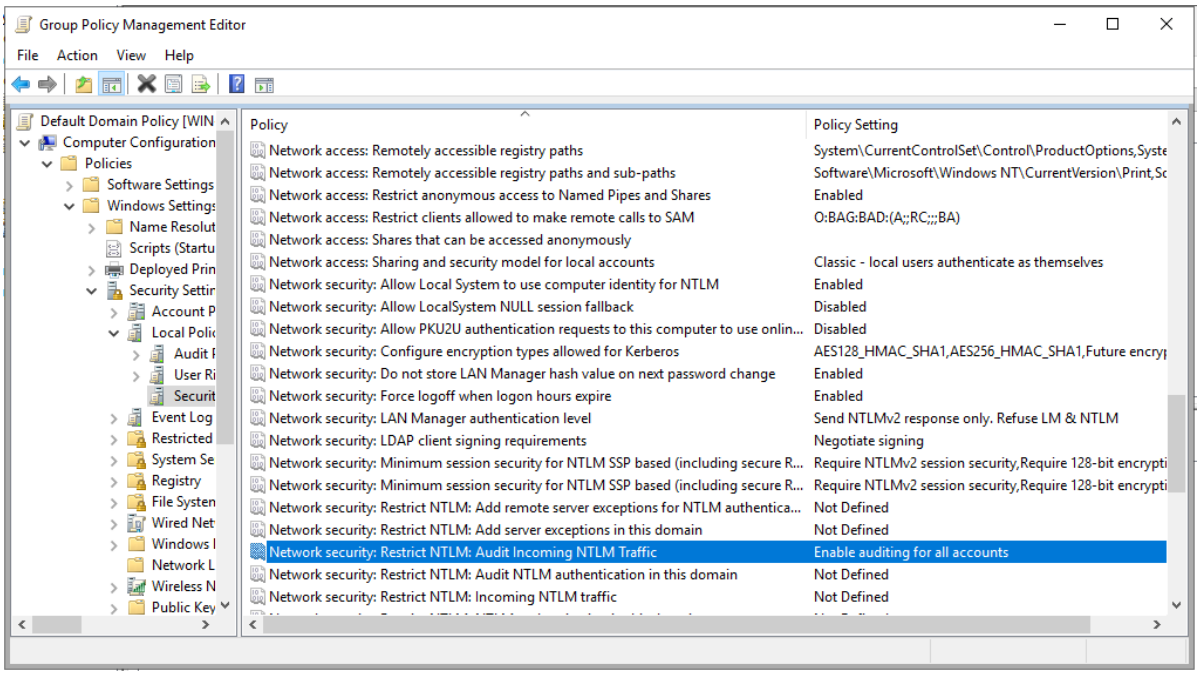


Image 97-Ensure 'Network security: Restrict NTLM: Audit Incoming NTLM Traffic' is set to 'Enable auditing for all accounts'

3.2.8.12 Ensure 'Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers' is set to 'Audit all' or higher

This policy setting enables the auditing of outgoing NTLM traffic, with events logged in the operational event log (e.g., Applications and Services Log\Microsoft\Windows\NTLM). The recommended configuration is to audit all traffic. Alternatively, setting it to Deny All is also acceptable but may affect applications that still rely on NTLM. Thorough testing is advised before implementing the Deny All setting. Auditing NTLM traffic helps identify and address systems using this outdated protocol, facilitating the transition to more secure protocols like Kerberos. Additionally, the logged information aids in forensic investigations following attacks. Since NTLM and NTLMv2 are vulnerable to various attacks such as SMB relay, man-in-the-middle, and brute force, reducing or eliminating their use minimizes the risk of unauthorized access to network systems.

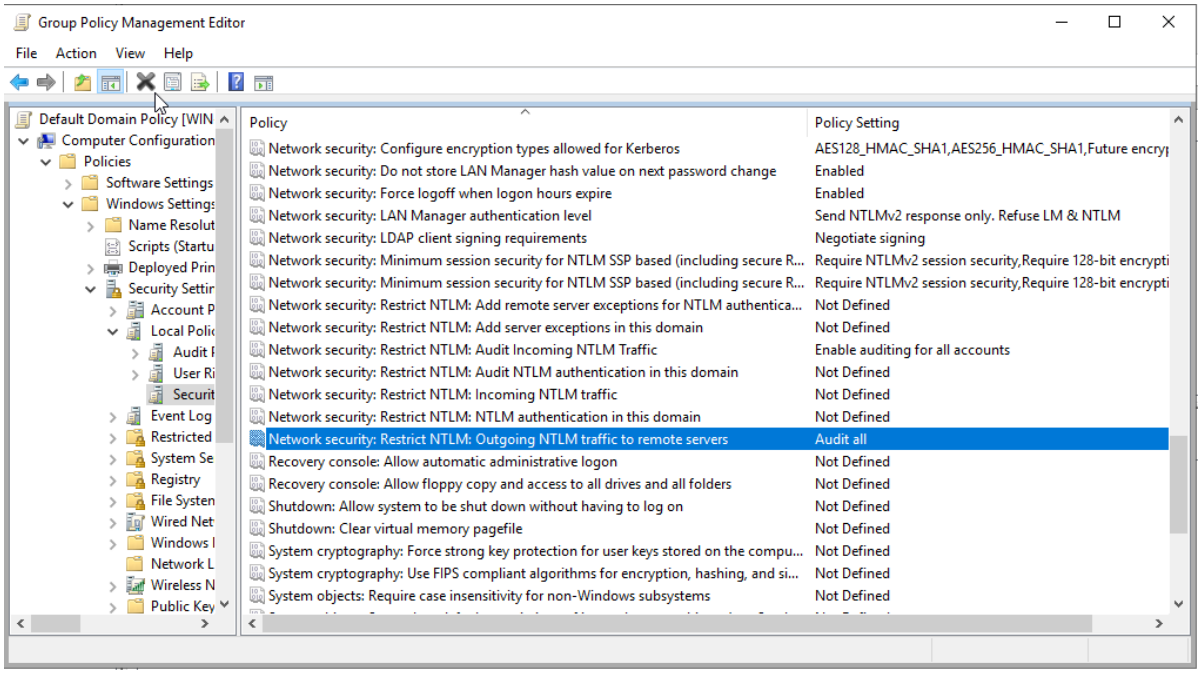


Image 98-Ensure 'Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers' is set to 'Audit all' or higher

3.2.9 Shutdown

3.2.9.1 Ensure 'Shutdown: Allow system to be shut down without having to log on' is set to 'Disabled'

This policy setting controls whether a computer can be shut down when no user is logged on. Enabling this setting makes the shutdown command available on the Windows logon screen. It is recommended to disable this setting to limit shutdown capabilities to users with valid credentials. The preferred configuration is: Disabled.

Previously, in Server 2008 R2 and earlier versions, this setting only affected the local console and did not impact Remote Desktop (RDP) or Terminal Services sessions. However, starting with Windows Server 2012 (non-R2), enabling this setting also allows RDP sessions to shut down or restart the server.

The rationale for disabling this setting is to prevent unauthorized users from shutting down or restarting the server, either locally or remotely. Attackers could exploit this capability to cause a temporary denial of service (DoS), making applications and services unavailable. The risk of such attacks is notably higher in Windows Server 2012 (non-R2) and later, where remote users can also perform these actions from an RDP logon screen.

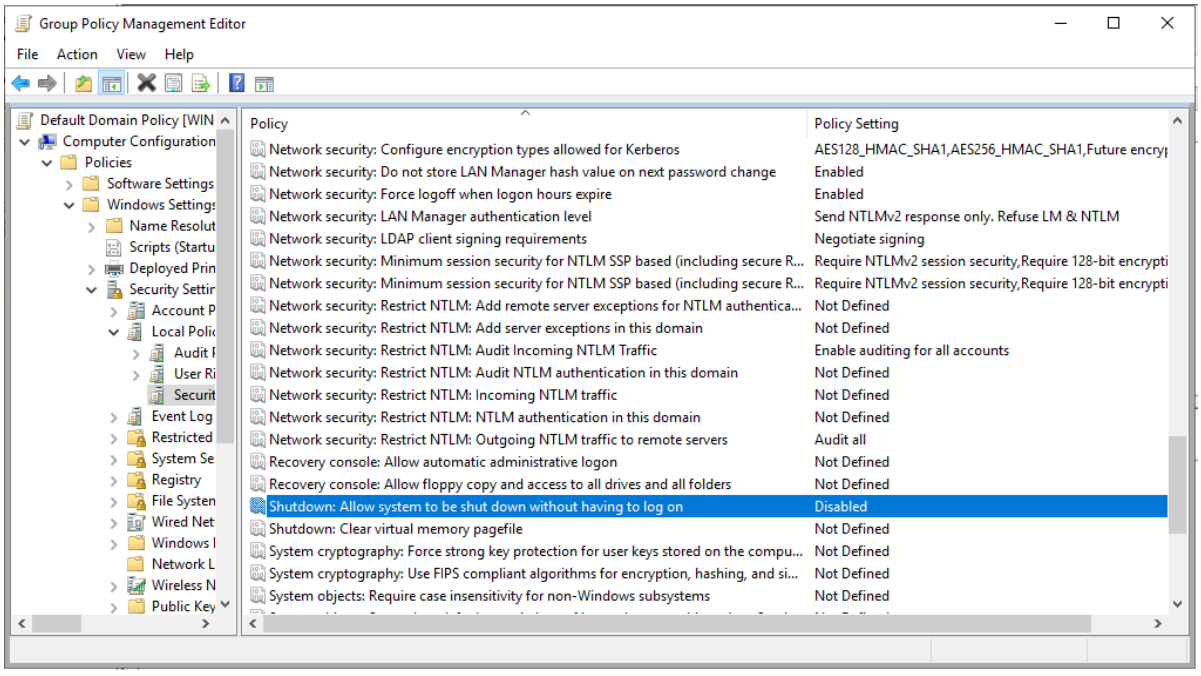


Image 99-Ensure 'Shutdown: Allow system to be shut down without having to log on' is set to 'Disabled'

3.2.10 System objects

3.2.10.1 Ensure 'System objects: Require case insensitivity for non-Windows subsystems' is set to 'Enabled'

This policy setting determines whether case insensitivity is enforced across all subsystems. While the Microsoft Win32 subsystem is case insensitive, the kernel supports case sensitivity in subsystems like the Portable Operating System Interface for UNIX (POSIX). Without this policy setting enabled, a user of the POSIX subsystem could create files with names differing only in case, which could cause issues for users accessing these files through Win32 tools, as only one version of the file would be visible.

The recommended configuration for this setting is: Enabled.

The rationale for enabling this setting is to prevent confusion and access issues arising from the creation of files with identical names but different cases in the POSIX subsystem. Without enforcement, users may encounter problems when accessing these files through standard Win32 tools, as only one version will be accessible.

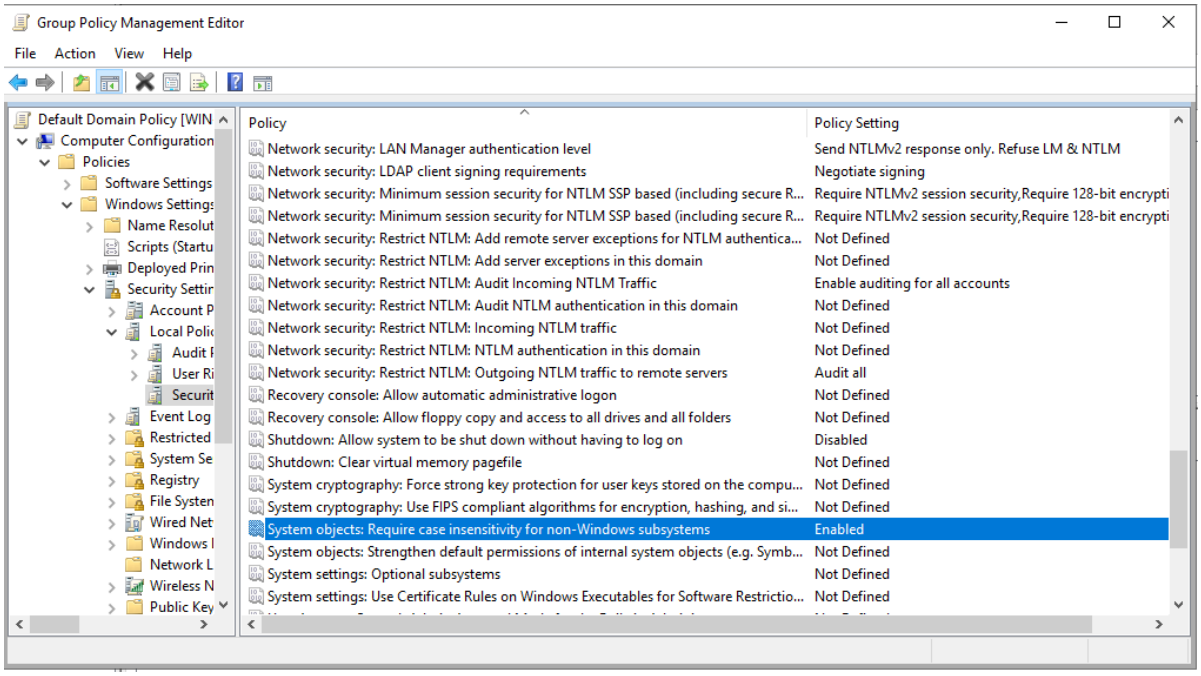


Image 100-Ensure 'System objects: Require case insensitivity for non-Windows subsystems' is set to 'Enabled'

3.2.10.2 Ensure 'System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)' is set to 'Enabled'

This policy setting controls the strength of the default discretionary access control list (DACL) for objects. Active Directory manages a global list of shared system resources, such as DOS device names, mutexes, and semaphores, allowing objects to be located and shared between processes. Each object type is assigned a default DACL that defines access permissions and user rights.

The recommended configuration for this setting is: Enabled.

The rationale is that this setting governs the robustness of the default DACL for objects. Windows uses a global list to facilitate the sharing and location of objects among processes, with each object type created with a default DACL that outlines who can access it and the level of permissions granted.

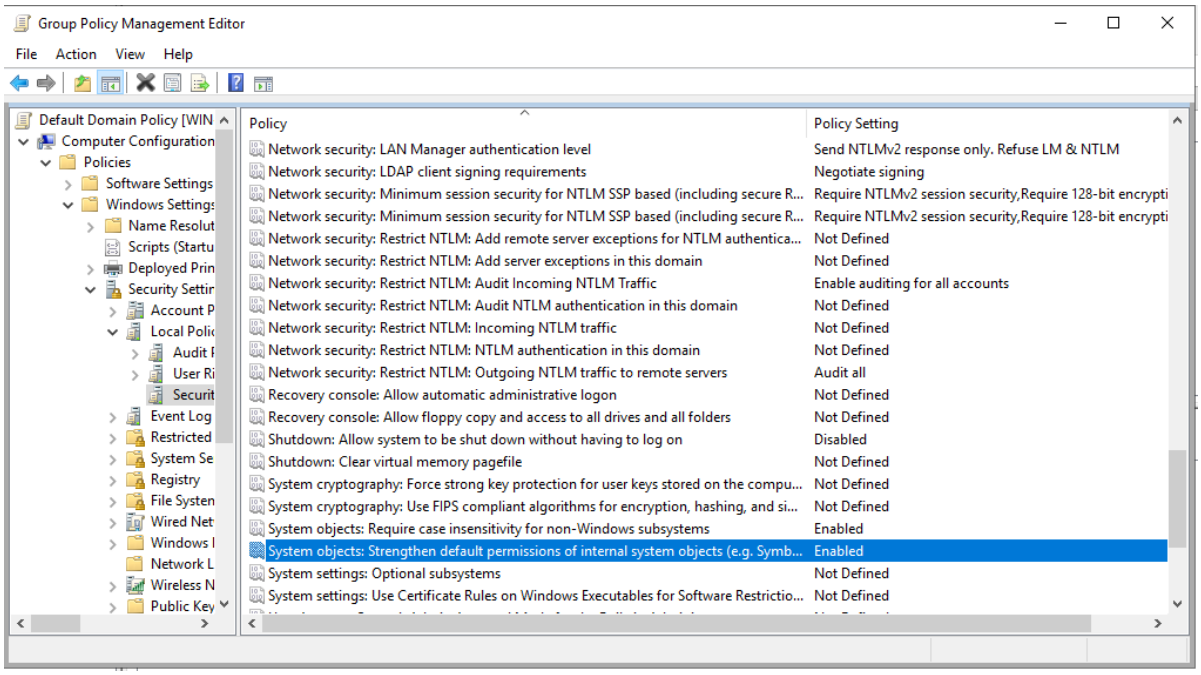


Image 101-Ensure 'System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)' is set to 'Enabled'

3.2.11 User Account Control

3.2.11.1 Ensure 'User Account Control: Admin Approval Mode for the Built-in Administrator account' is set to 'Enabled'

This policy setting manages the behavior of Admin Approval Mode for the built-in Administrator account.

The recommended configuration for this setting is: Enabled.

The rationale behind this is that User Account Control (UAC), introduced with Windows Vista, aims to mitigate risks associated with malicious software running under elevated credentials without the user's or administrator's awareness. One such risk was the potential for attackers to exploit the default "Administrator" account, which is created with every Windows installation. To address this, the built-in Administrator account is disabled by default starting with Windows Vista. When a new computer is set up:

- If not domain-joined, the first user account created has local administrator privileges.
- If domain-joined, local administrator accounts are not created initially; instead, an Enterprise or Domain Administrator must log in to create one if necessary.

Even though the built-in Administrator account can be enabled manually after installation, it is strongly advised to keep it disabled for security reasons.

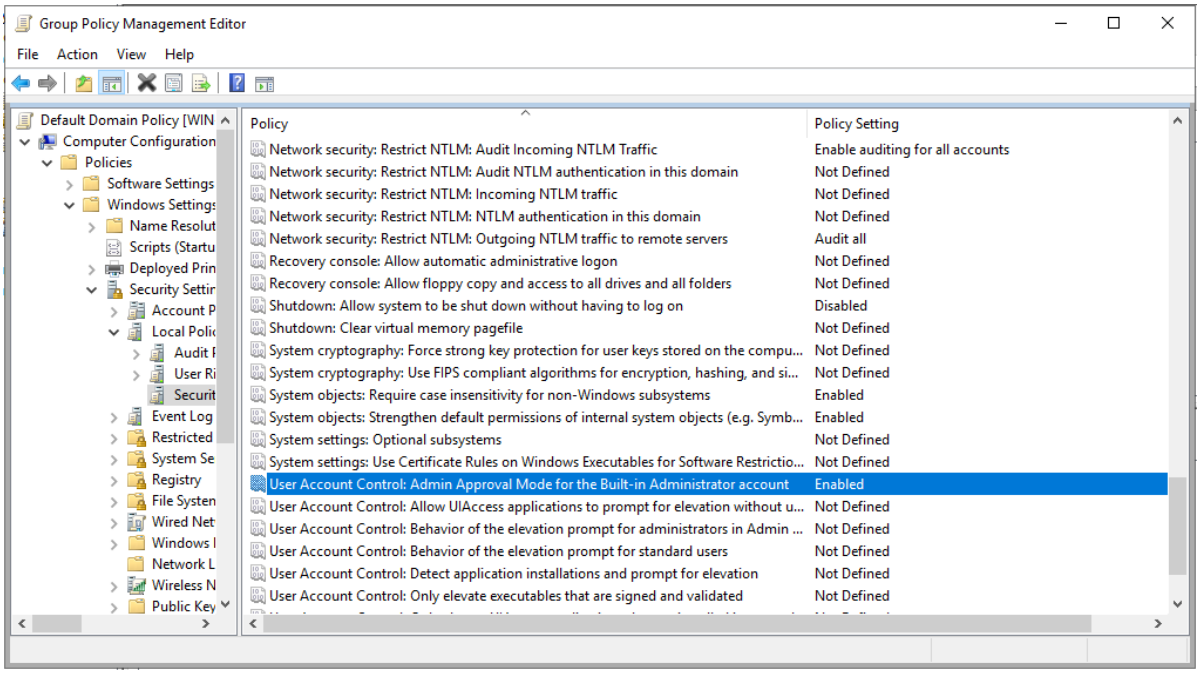


Image 102-Ensure 'User Account Control: Admin Approval Mode for the Built-in Administrator account' is set to 'Enabled'

3.2.11.2 Ensure 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' is set to 'Prompt for consent on the secure desktop' or higher

This policy setting manages the behavior of the elevation prompt for administrators.

The recommended configuration for this setting is: Prompt for consent on the secure desktop. Setting it to Prompt for credentials on the secure desktop is also acceptable.

The rationale for this is that the User Account Control (UAC) feature introduced with Windows Vista aims to mitigate the risk of malicious software running with elevated privileges without the user's or administrator's knowledge. This setting helps increase administrator awareness of operations requiring elevated privileges and enables them to prevent unauthorized privilege escalation by malicious programs attempting to gain elevated access.

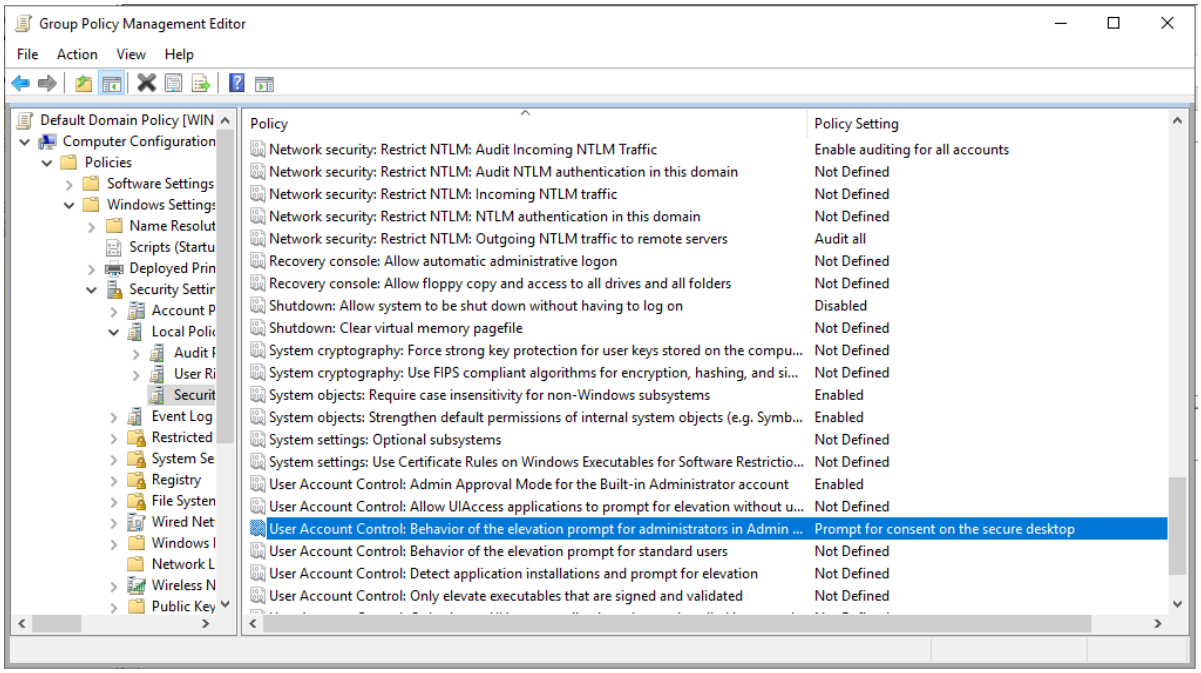


Image 103-Ensure 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' is set to 'Prompt for consent on the secure desktop' or higher

3.2.11.3 Ensure 'User Account Control: Behavior of the elevation prompt for standard users' is set to 'Automatically deny elevation requests'

This policy setting governs how elevation prompts are handled for standard users.

The recommended configuration is: Automatically deny elevation requests.

The rationale is that the User Account Control (UAC) feature in Windows Vista aims to reduce the risk of malicious software operating with elevated privileges without user or administrator knowledge. This setting alerts users when a program attempts to use elevated privileges and requires them to provide administrative credentials for the program to run.

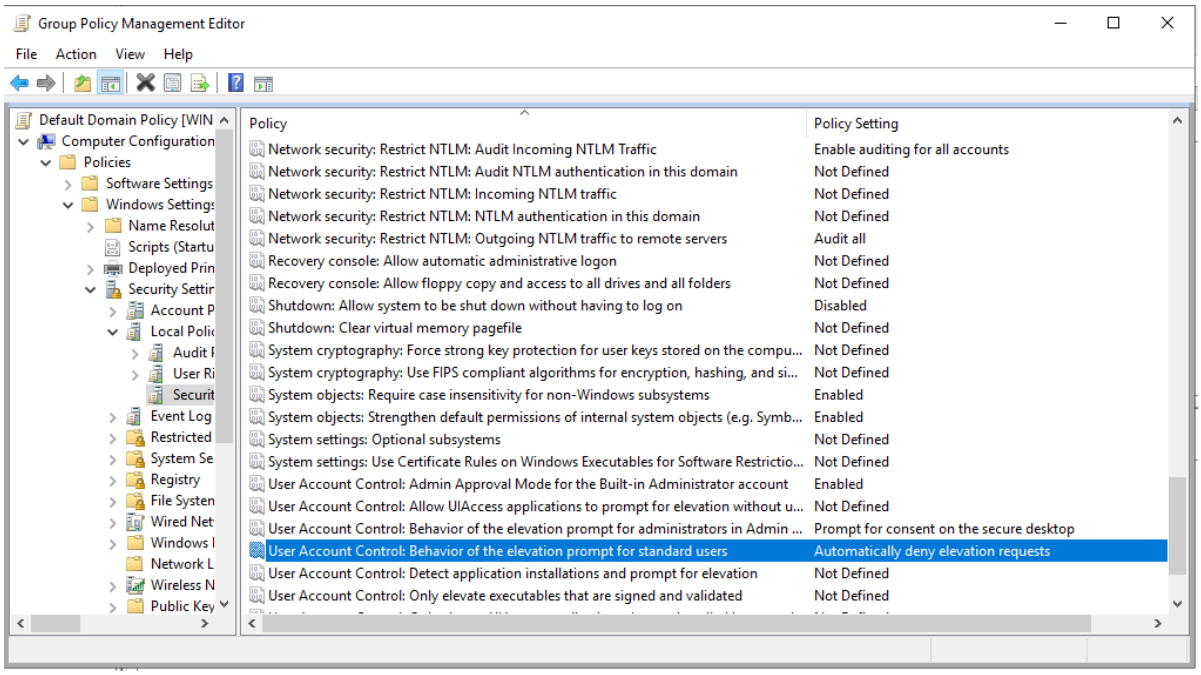


Image 104-Ensure 'User Account Control: Behavior of the elevation prompt for standard users' is set to 'Automatically deny elevation requests'

3.2.11.4 Ensure 'User Account Control: Detect application installations and prompt for elevation' is set to 'Enabled'

This policy setting manages how application installation detection is handled on the computer.

The recommended configuration is: Enabled.

The rationale is that certain malicious software may try to install itself after being granted permission to run, especially if it masquerades as a trusted application. By enabling this setting, you create an additional layer of defense, as it helps detect and block unauthorized installations of unknown components, thereby preventing potential damage from such software.

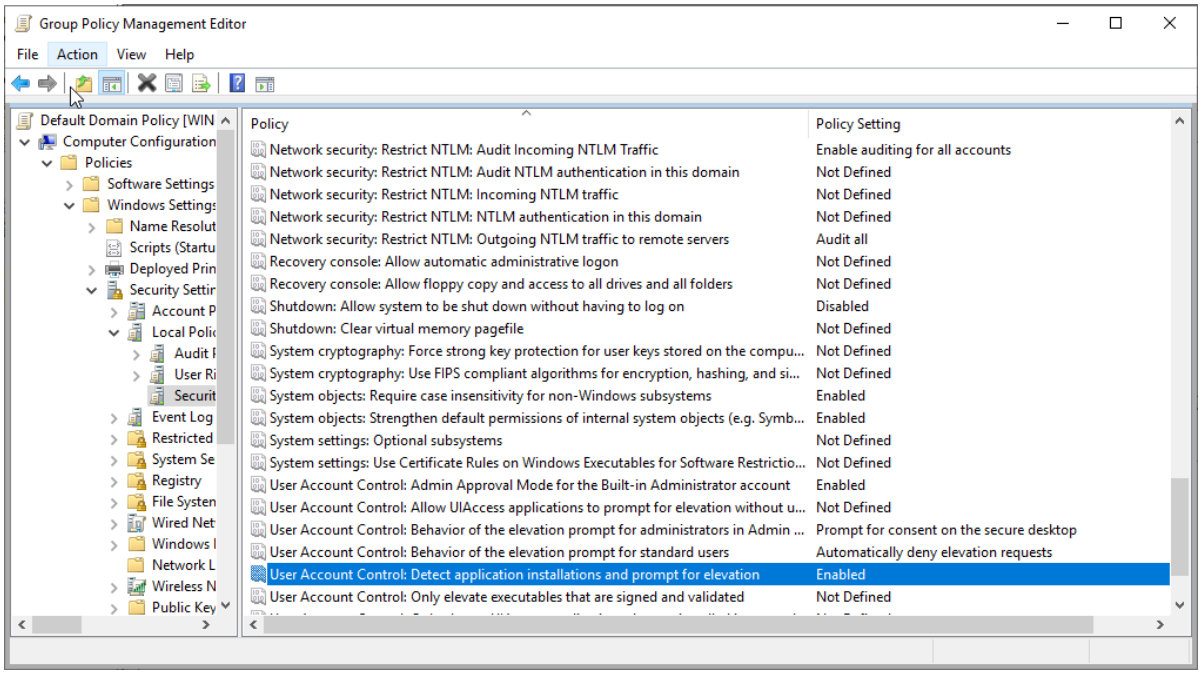


Image 105-Ensure 'User Account Control: Detect application installations and prompt for elevation' is set to 'Enabled'

3.2.11.5 Ensure 'User Account Control: Only elevate UIAccess applications that are installed in secure locations' is set to 'Enabled'

This policy setting determines whether applications that request to run with a User Interface (UIAccess) integrity level must be located in a secure directory within the file system.

Windows requires a public key infrastructure (PKI) signature check for any interactive application requesting to run with a UIAccess integrity level, regardless of this security setting's configuration.

UIAccess Integrity allows an application to bypass User Interface Privilege Isolation (UIPI) restrictions when it is elevated from a standard user to an administrator. This feature is essential for supporting accessibility tools, such as screen readers, which need to interact with user interfaces in various ways. Applications running with UIAccess rights can:

- Set the foreground window
- Control any application window using the SendInput function
- Access input from all integrity levels through low-level hooks, raw input, GetKeyState, GetAsyncKeyState, and GetKeyboardInput
- Set journal hooks
- Use AttachThreadInput to connect a thread to a higher integrity input queue

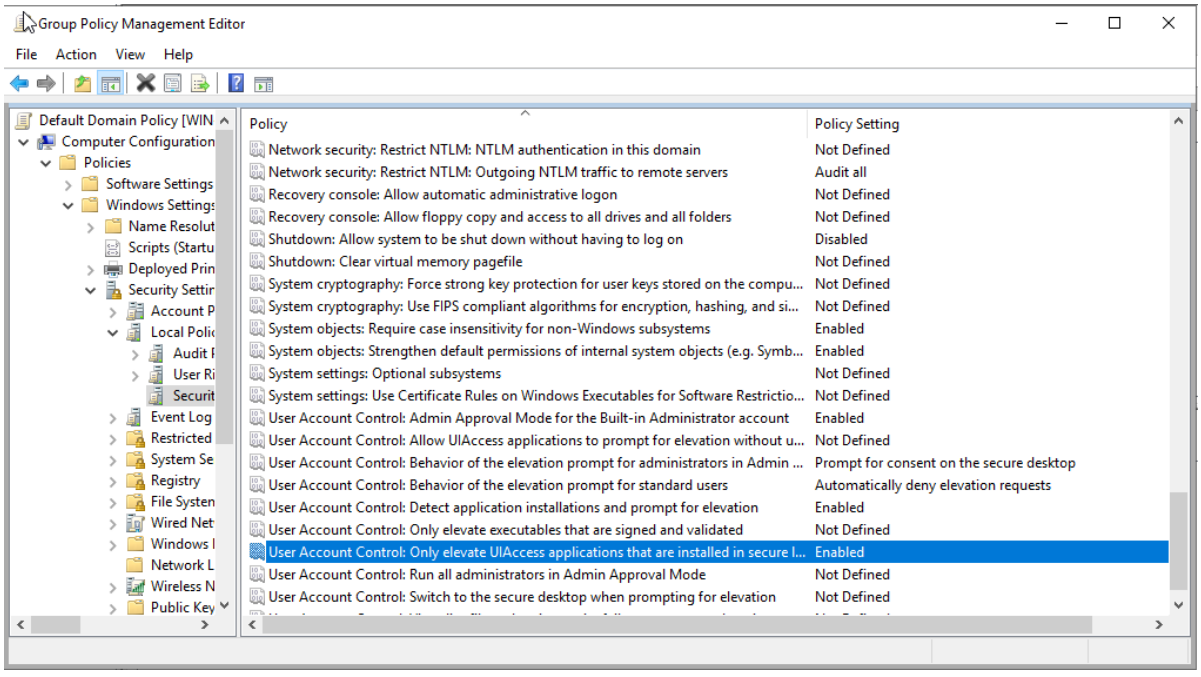


Image 106-Ensure 'User Account Control: Only elevate UIAccess applications that are installed in secure locations' is set to 'Enabled'

3.2.11.6 Ensure 'User Account Control: Run all administrators in Admin Approval Mode' is set to 'Enabled'

This policy setting controls the overall behavior of User Account Control (UAC) on the computer, and changes to this setting require a system restart to take effect. The recommended state for this setting is Enabled. Disabling this policy will trigger a notification from the Security Center, indicating a reduction in the operating system's security. If UAC is disabled, the system will lose the security benefits and risk mitigations that UAC provides, potentially increasing the system's vulnerability.

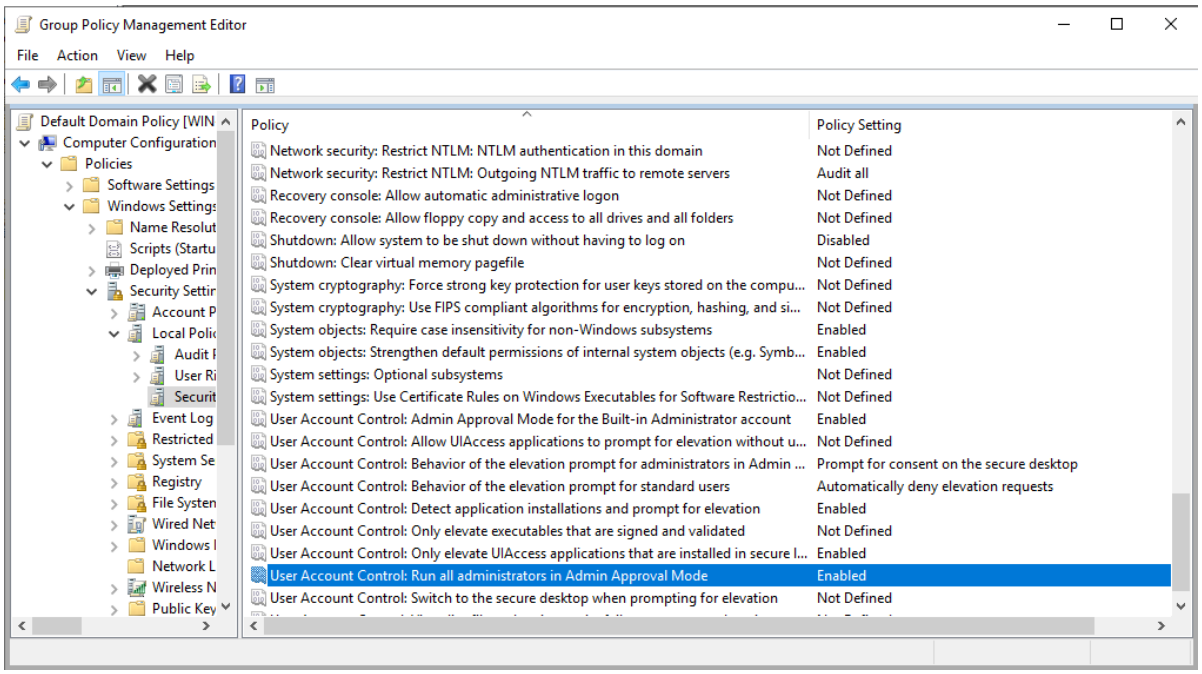


Image 107-Ensure 'User Account Control: Run all administrators in Admin Approval Mode' is set to 'Enabled'

3.2.11.7 Ensure 'User Account Control: Switch to the secure desktop when prompting for elevation' is set to 'Enabled'.

This policy setting determines whether elevation request prompts are shown on the interactive user's desktop or the secure desktop. The recommended configuration for this setting is Enabled. Standard elevation prompts can be spoofed, potentially leading users to disclose their passwords to malicious software. The secure desktop offers a more distinct appearance for elevation prompts, with a dimmed user desktop and a more prominent prompt UI. This design helps users recognize and avoid spoofed prompts, making it less likely that they will fall for malicious tricks.

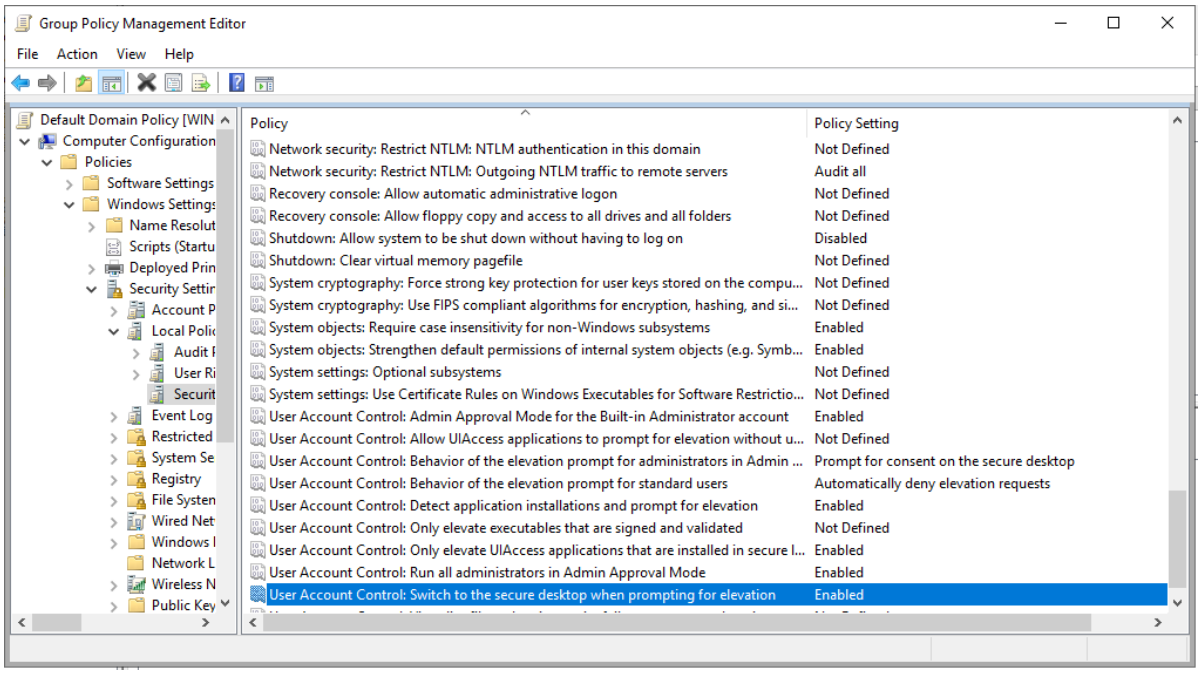


Image 108-Ensure 'User Account Control: Switch to the secure desktop when prompting for elevation' is set to 'Enabled'

3.2.11.8 Ensure 'User Account Control: Virtualize file and registry write failures to per-user locations' is set to 'Enabled'

This policy setting determines whether failures in application writes are redirected to specific registry and file system locations. It addresses situations where applications running with administrative privileges attempt to write runtime data to locations such as:

- %ProgramFiles%
- %windir%
- %windir%\System32
- HKEY_LOCAL_MACHINE\SOFTWARE

The recommended configuration for this setting is Enabled. This approach minimizes vulnerabilities by ensuring that legacy applications are restricted to writing data only to approved locations.

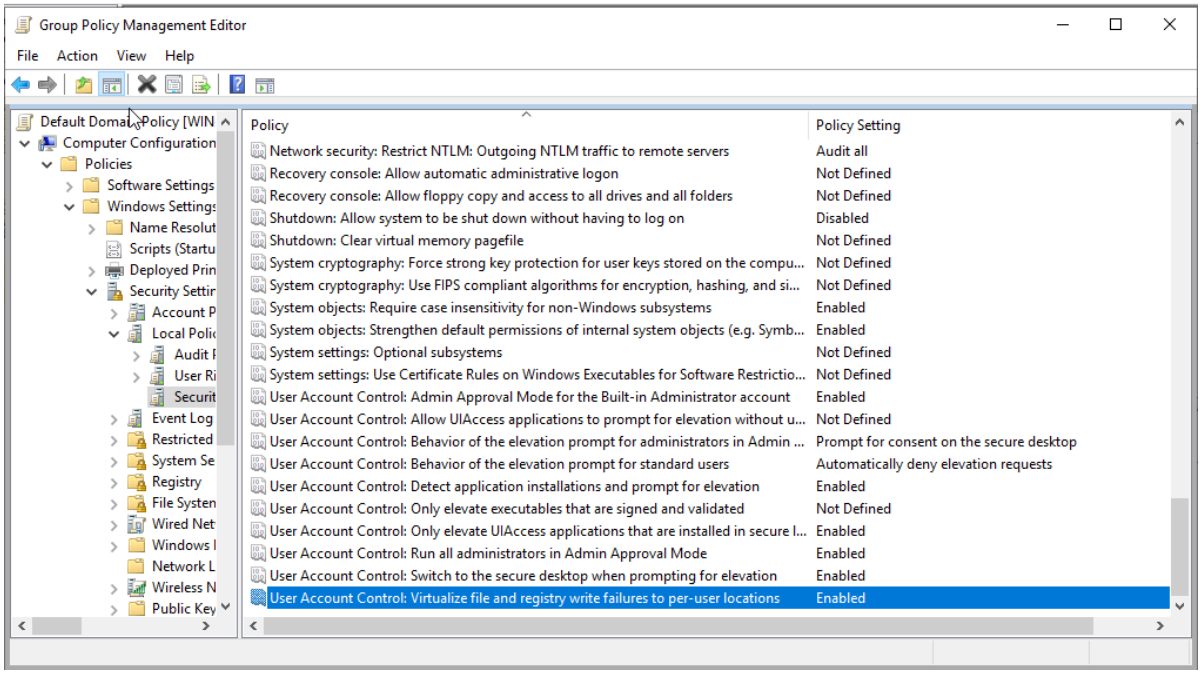


Image 109-Ensure 'User Account Control: Virtualize file and registry write failures to per-user locations' is set to 'Enabled'

4 System Services

System services are essential components of an operating system that run in the background to perform various tasks and manage system operations. These services handle critical functions such as networking, security, file management, and hardware communication, ensuring that the system operates smoothly and efficiently. System services can be started automatically during system boot or manually by users and are often configured to run with specific permissions to maintain system stability and security. They help maintain system performance by managing resource allocation, executing scheduled tasks, and providing necessary functionalities for applications and user interactions.

4.1 Ensure 'Print Spooler (Spooler)' is set to 'Disabled'

This service manages print jobs and facilitates communication with printers. The recommended configuration for this setting is to disable the Print Spooler service. Disabling this service helps protect against vulnerabilities such as PrintNightmare (CVE-2021-34527) and other potential threats targeting the service.

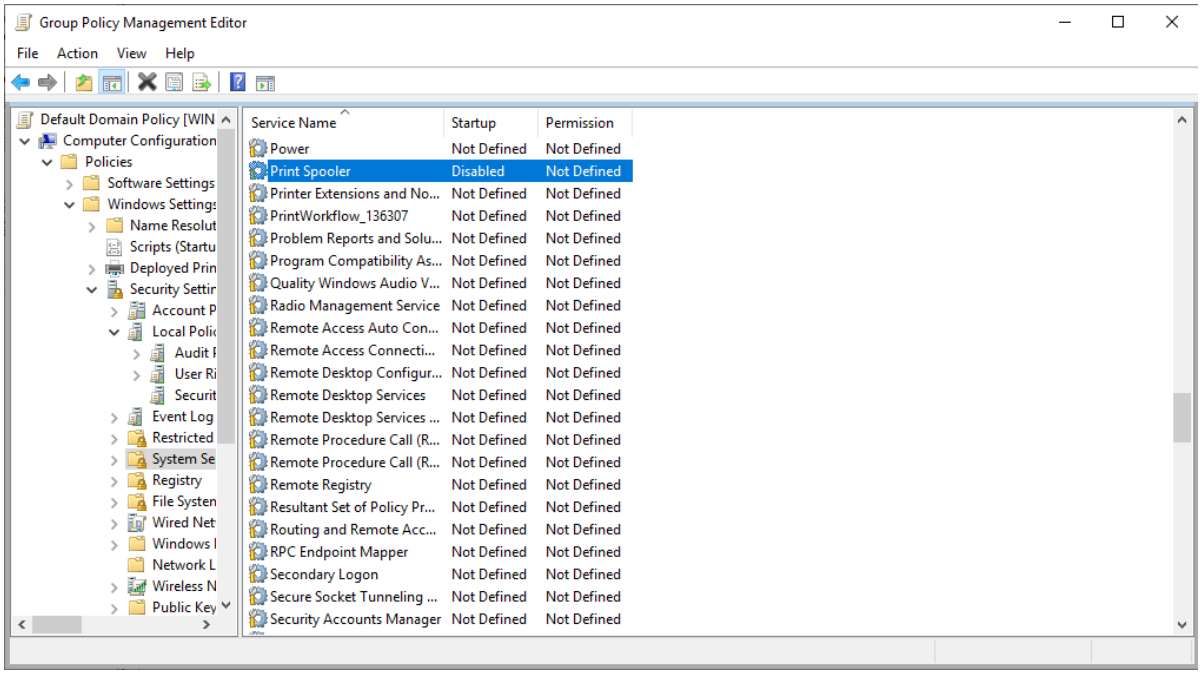


Image 110-Ensure 'Print Spooler (Spooler)' is set to 'Disabled'

5 Windows Defender Firewall with Advanced Security

Windows Defender Firewall with Advanced Security is a robust network security feature built into Windows that helps protect your computer from unauthorized access and cyber threats. It offers advanced filtering capabilities to control incoming and outgoing network traffic based on configurable rules and policies. By setting up custom rules, administrators can define which applications, ports, and protocols are allowed or blocked, enhancing overall system security. This firewall also provides monitoring and logging tools to track network activity and potential threats, making it a crucial component in safeguarding a computer or network against malicious attacks and ensuring a secure computing environment.

5.1 Private Profile

A Private Profile Group Policy ensures enhanced privacy and security by restricting access and limiting visibility of user profiles. It isolates sensitive data, controls sharing, and maintains confidentiality, providing a secure environment for user information within the network.

5.1.1 Ensure 'Windows Firewall: Private: Firewall state' is set to 'On (recommended)'

To ensure that Windows Firewall with Advanced Security applies the appropriate settings for filtering network traffic, select "On (recommended)." If set to "Off," the firewall will not enforce any rules for this profile. The recommended state for this setting is "On (recommended)." Disabling the firewall allows unrestricted access to the system, which increases the risk of remote exploitation of network service vulnerabilities.

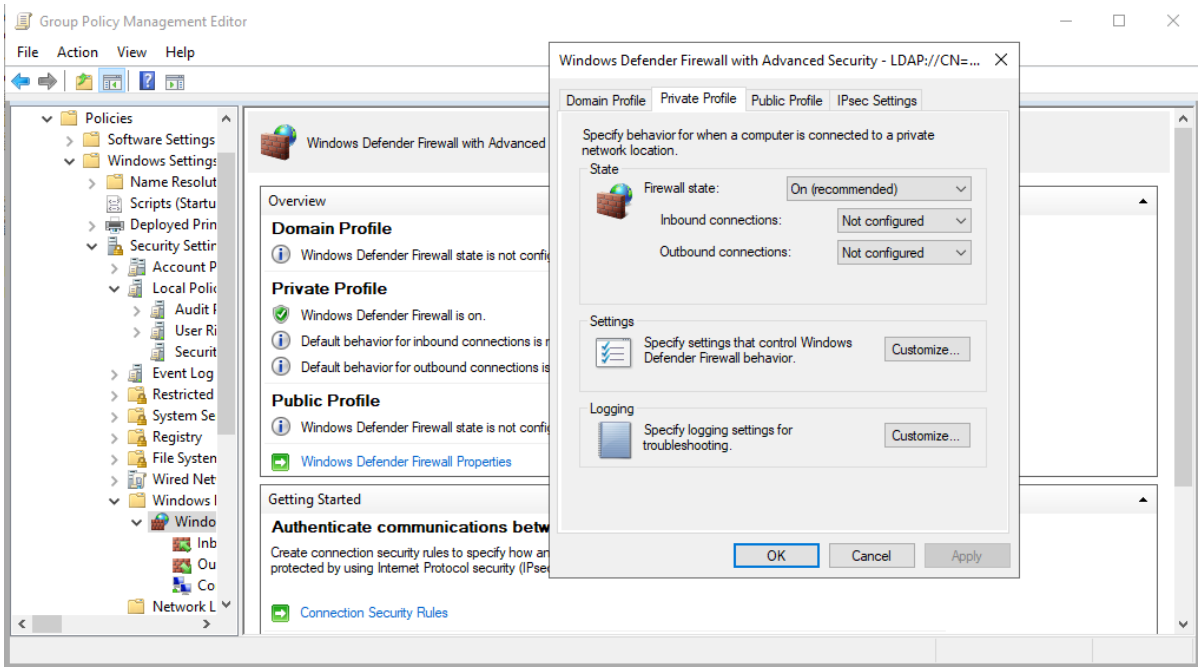


Image 111-Ensure 'Windows Firewall: Private: Firewall state' is set to 'On (recommended)'

5.1.2 Ensure 'Windows Firewall: Private: Inbound connections' is set to 'Block (default)'

This setting defines how the system handles inbound connections that do not align with any existing inbound firewall rules. The recommended configuration for this setting is "Block (default)." Allowing unrestricted inbound traffic could make it easier for attackers to exploit vulnerabilities in network services remotely.

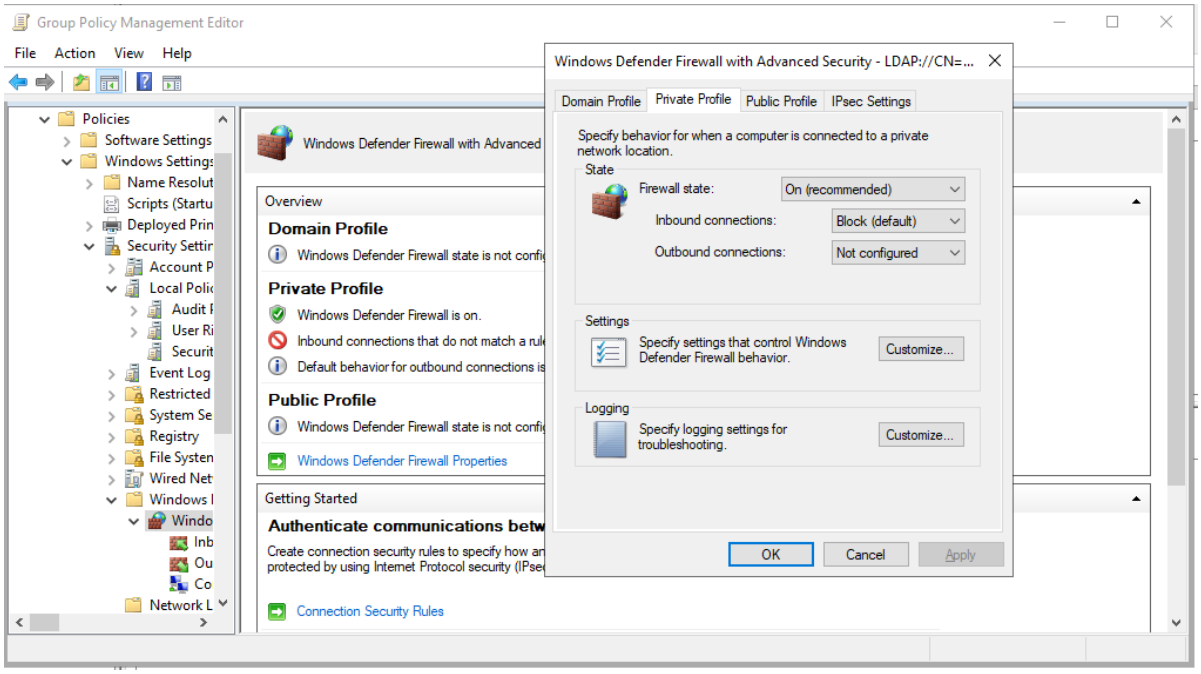


Image 112-Ensure 'Windows Firewall: Private: Inbound connections' is set to 'Block (default)'

5.1.3 Ensure 'Windows Firewall: Private: Outbound connections' is set to 'Allow (default)'

This setting controls how the system handles outbound connections that do not match any existing outbound firewall rules. The recommended configuration for this setting is "Allow (default)." Note that if outbound connections are set to "Block" and this policy is deployed via a Group Policy Object (GPO), computers receiving these settings may not be able to receive future Group Policy updates unless an outbound rule is created to permit this. Ensure that predefined outbound rules for Core Networking, which allow Group Policy to function, are active, and thoroughly test firewall profiles before deployment. Blocking all outbound connections by default may lead to numerous prompts for user authorization and is generally considered less effective, as an attacker who has compromised the system can bypass firewall restrictions.

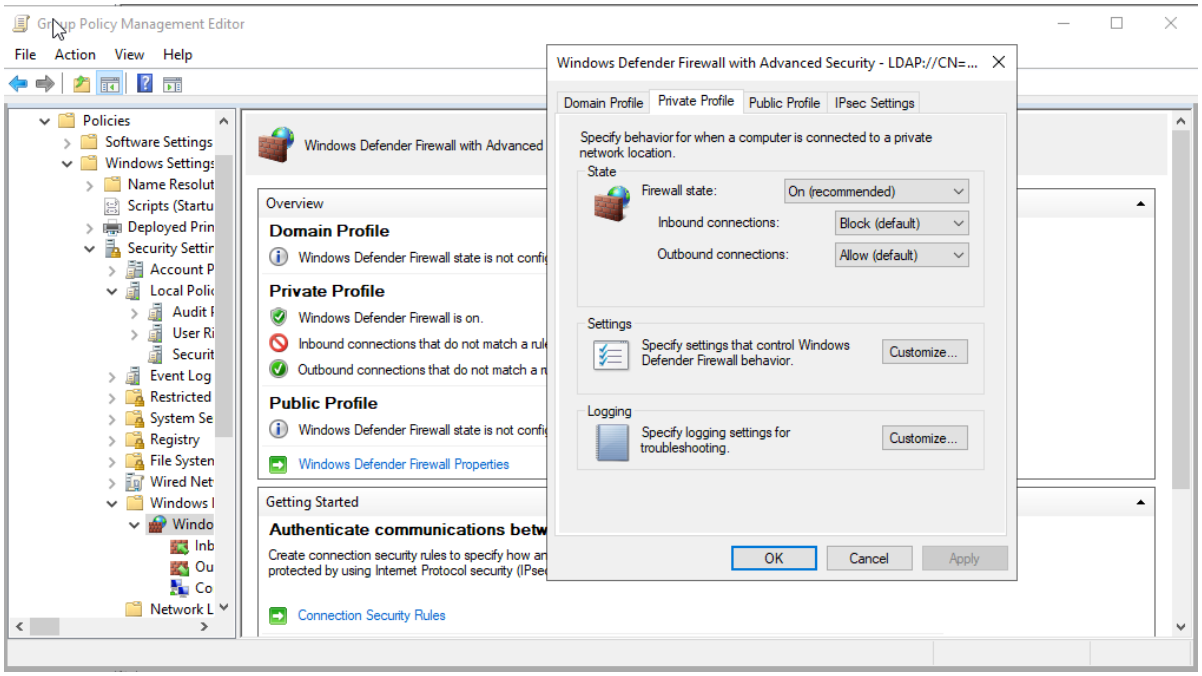


Image 113-Ensure 'Windows Firewall: Private: Outbound connections' is set to 'Allow (default)'

5.1.4 Ensure 'Windows Firewall: Private: Settings: Display a notification' is set to 'No'

Choose this option if you want Windows Firewall with Advanced Security to notify users when a program is blocked from receiving inbound connections. The recommended setting for this option is "No." If the "Apply local firewall rules" setting is configured to "No," it is also advised to set the "Display a notification" option to "No." This prevents users from receiving prompts to unblock restricted inbound connections, as their responses will not be acknowledged. Notifications about firewall activities can be confusing for users who may not be equipped to handle them effectively.

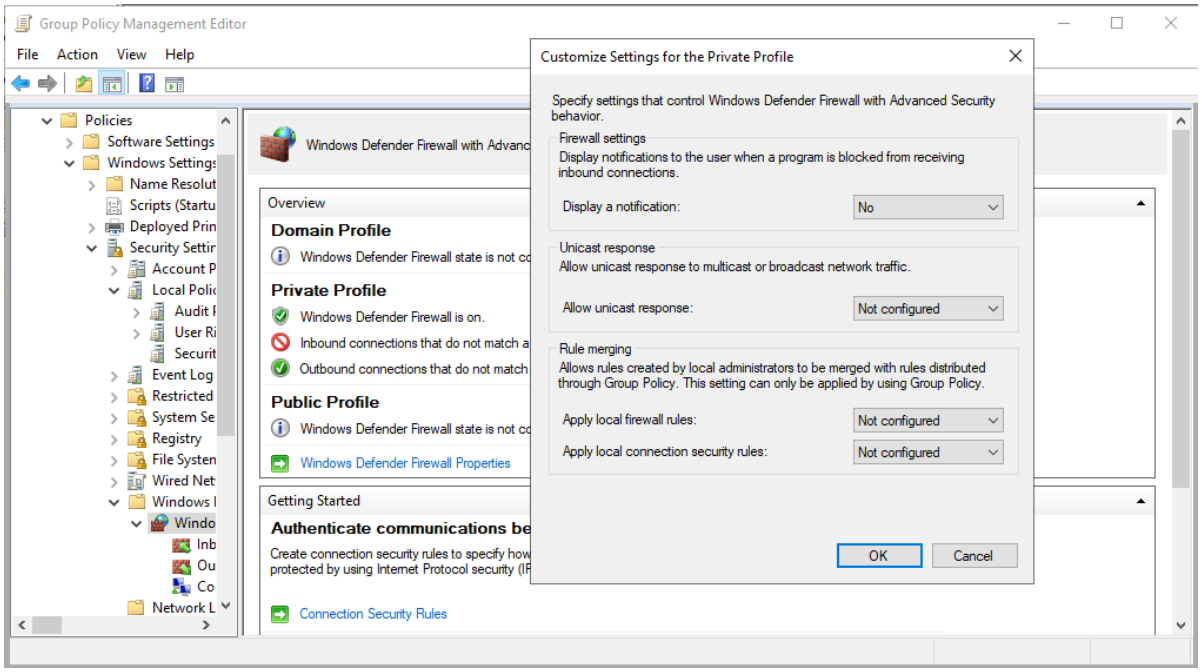


Image 114-Ensure 'Windows Firewall: Private: Settings: Display a notification' is set to 'No'

5.1.5 Ensure 'Windows Firewall: Private: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\privatefw.log'

Choose this option to define the path and name of the file where Windows Firewall will save its log data. Without proper logging of Windows Firewall events, it can be challenging for administrators to investigate system problems or unauthorized activities. By default, Microsoft logs all firewall events in a single file (`pfirewall.log`). For better organization and to facilitate issue identification, it is recommended to separate logs for each firewall profile (domain, private, public) into individual files (e.g., `domainfw.log`, `privatefw.log`, `publicfw.log`).

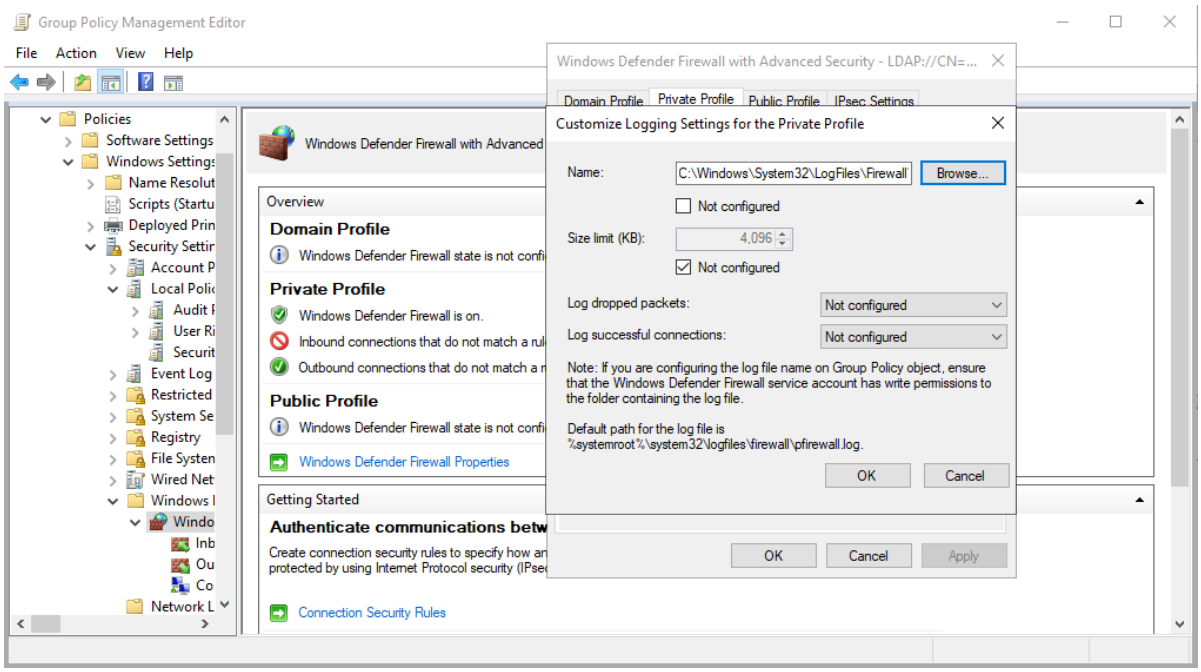


Image 115-Ensure 'Windows Firewall: Private: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\privatefw.log'

5.1.6 Ensure 'Windows Firewall: Private: Logging: Size limit (KB)' is set to '16,384 KB or greater'

Choose this option to set the maximum file size for Windows Firewall log files. The recommended size limit is 16,384 KB or larger. Adequate log file size is crucial for capturing all relevant events; without sufficient logging, identifying the root cause of system issues or unauthorized activities can be challenging or impossible.

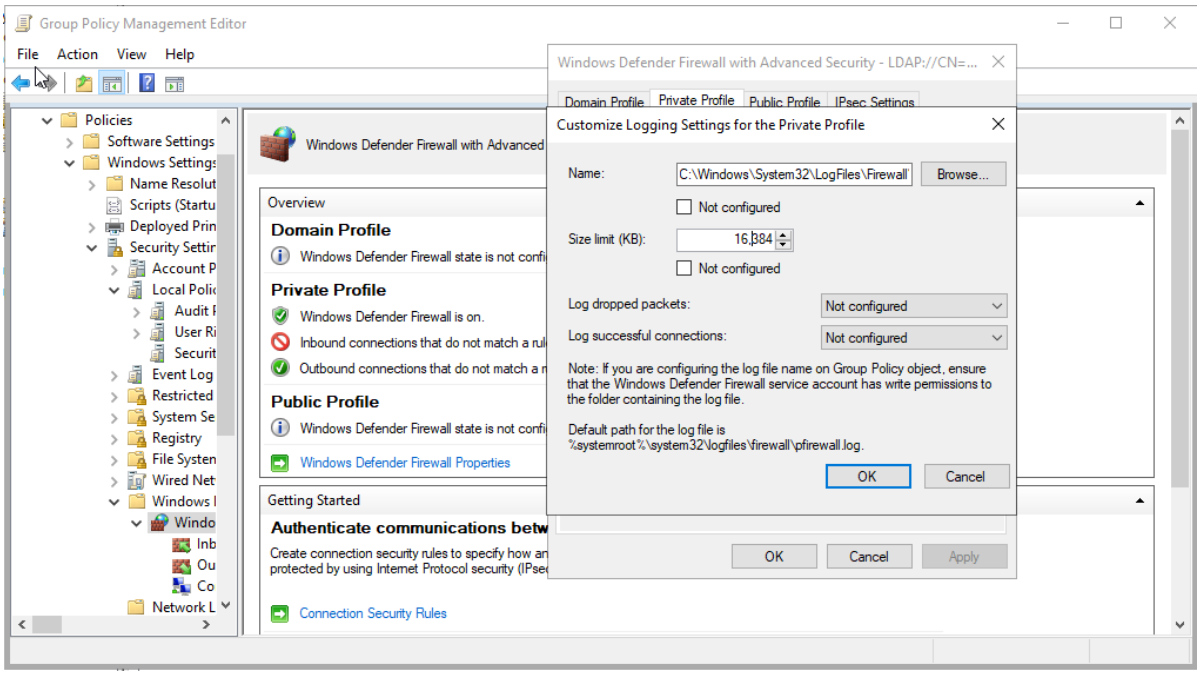


Image 116-Ensure 'Windows Firewall: Private: Logging: Size limit (KB)' is set to '16,384 KB or greater'

5.1.7 Ensure 'Windows Firewall: Private: Logging: Log dropped packets' is set to 'Yes'

Enable this option to log instances when Windows Firewall with Advanced Security discards an inbound packet, including the reasons and timing of the packet drops. Check the log for entries with "DROP" in the action column. The recommended setting for this option is: Yes. Logging such events is essential for diagnosing system issues or unauthorized activities, as it helps identify the underlying causes of problems.

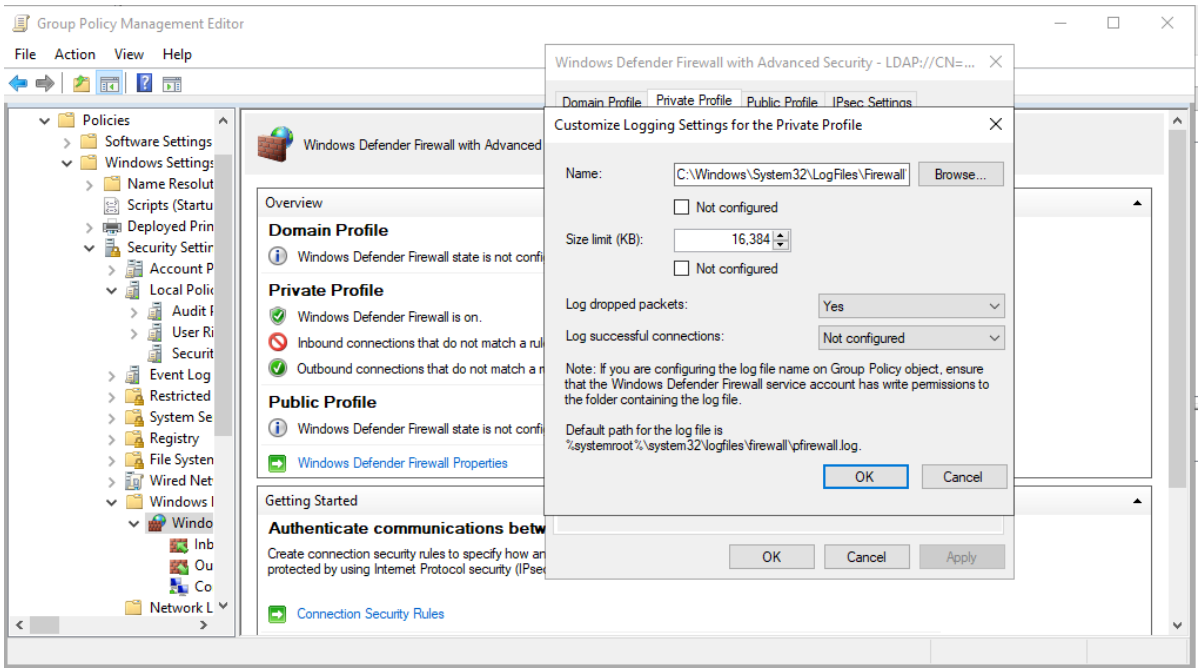


Image 117-Ensure 'Windows Firewall: Private: Logging: Log dropped packets' is set to 'Yes'

5.1.8 Ensure 'Windows Firewall: Private: Logging: Log successful connections' is set to 'Yes'

Enable this option to log when Windows Firewall with Advanced Security permits an inbound connection, capturing the details of why and when the connection was allowed. Check the log for entries with "ALLOW" in the action column. The recommended setting is: Yes. Recording these events is crucial for identifying the root causes of system issues or unauthorized activities, as it provides essential information for troubleshooting and security analysis.

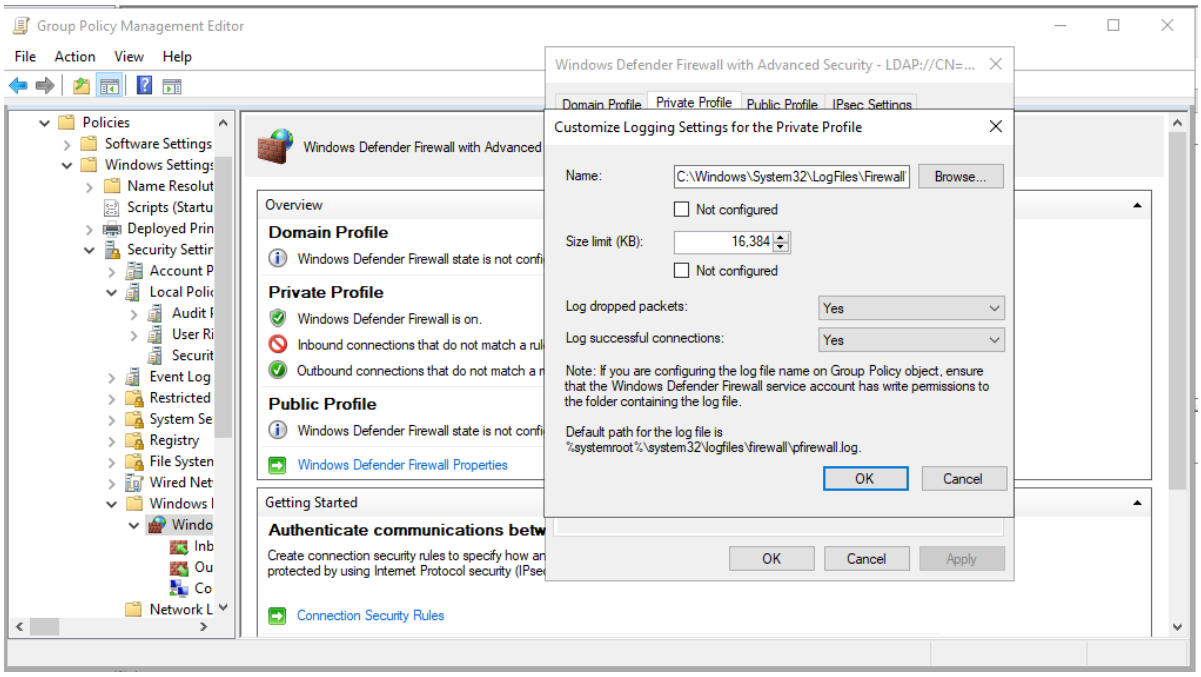


Image 118-Ensure 'Windows Firewall: Private: Logging: Log successful connections' is set to 'Yes'

5.2 Private Profile

A Private Profile Group Policy ensures enhanced privacy and security by restricting access and limiting visibility of user profiles. It isolates sensitive data, controls sharing, and maintains confidentiality, providing a secure environment for user information within the network.

5.2.1 Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)'

Choose "On" (recommended) to ensure that Windows Firewall with Advanced Security applies the settings for this profile to manage network traffic. If set to "Off," the firewall will not enforce any rules or security policies for this profile. The recommended setting is "On" to prevent unauthorized access, as turning off the firewall can leave the system exposed to potential remote attacks exploiting network vulnerabilities.

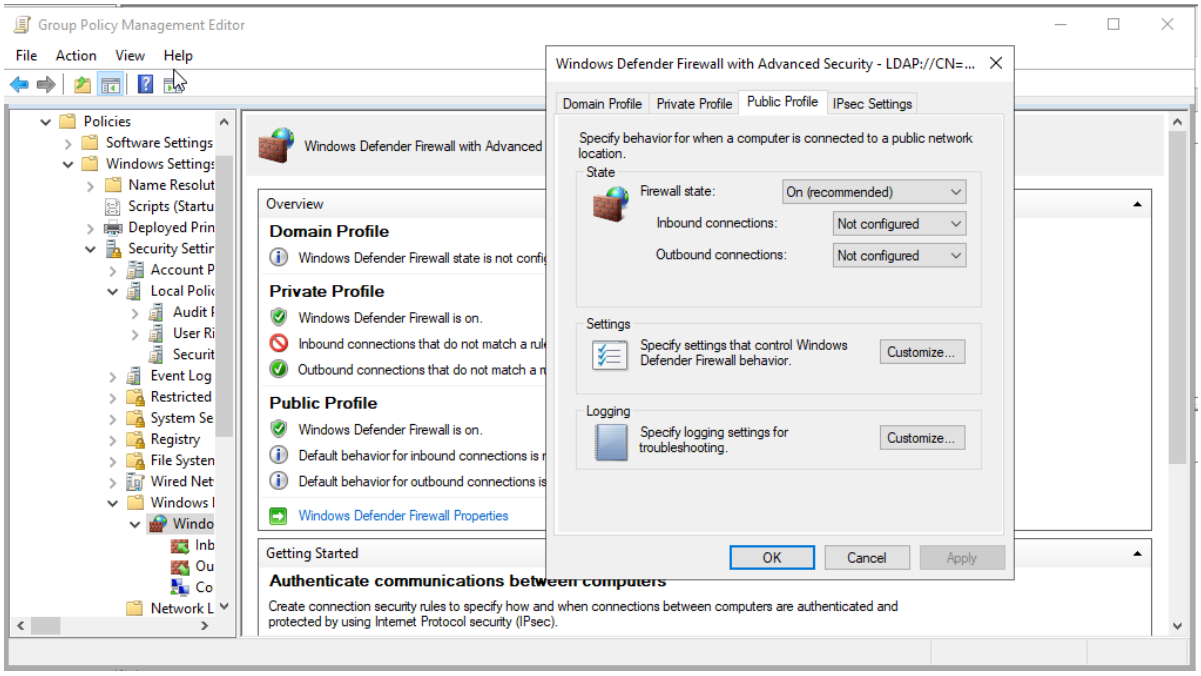


Image 119-Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)'

5.2.2 Ensure 'Windows Firewall: Public: Inbound connections' is set to 'Block (default)'

This setting controls how the system handles inbound connections that don't match any existing firewall rules. The recommended configuration is to set this to "Block" (default). Allowing unrestricted traffic could make the system more vulnerable to remote exploitation of network service weaknesses.

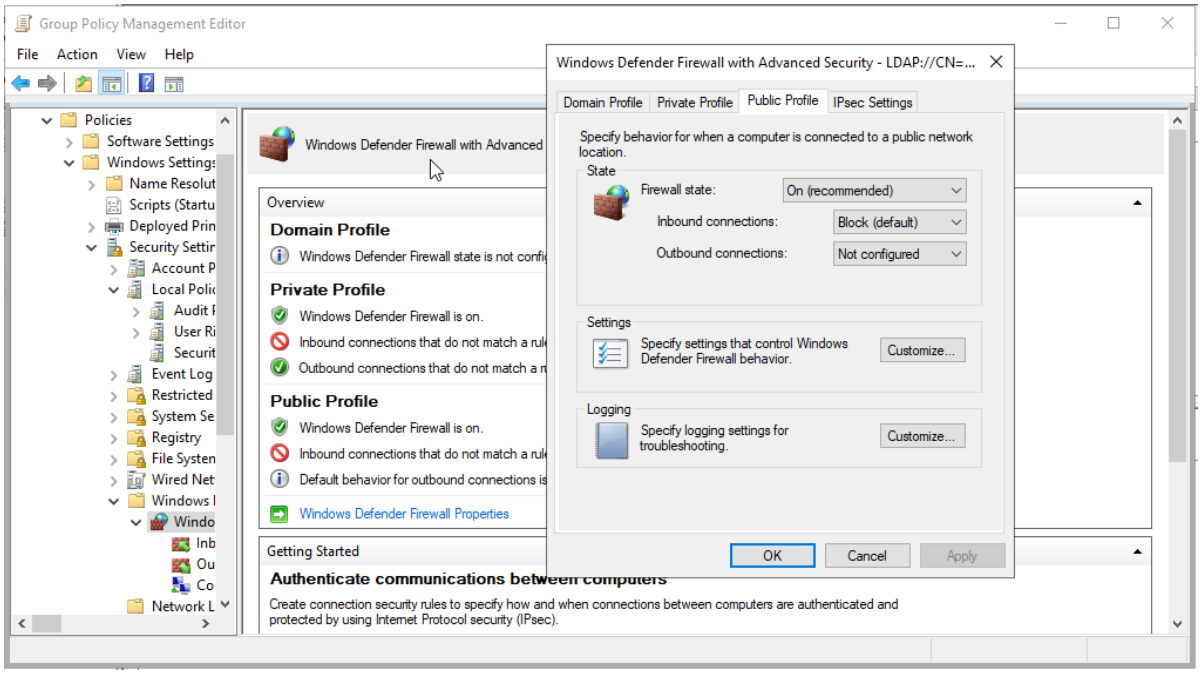


Image 120-Ensure 'Windows Firewall: Public: Inbound connections' is set to 'Block (default)'

5.2.3 Ensure 'Windows Firewall: Public: Outbound connections' is set to 'Allow (default)'

This setting controls how the system handles outbound connections that do not match any defined firewall rules. The recommended configuration is to set this to "Allow" (default). If you choose to block outbound connections and deploy this policy using a Group Policy Object (GPO), computers receiving these settings might not be able to get further Group Policy updates unless you create an outbound rule that allows Group Policy to function. Ensure that predefined outbound rules for Core Networking are active and test firewall profiles thoroughly before deployment.

Microsoft recommends allowing outbound connections by default to avoid frequent user prompts for authorization and to prevent potential issues with essential applications like web browsers and instant messaging software. Blocking outbound traffic can offer limited security benefits, as an attacker who has compromised the system could potentially reconfigure the firewall.

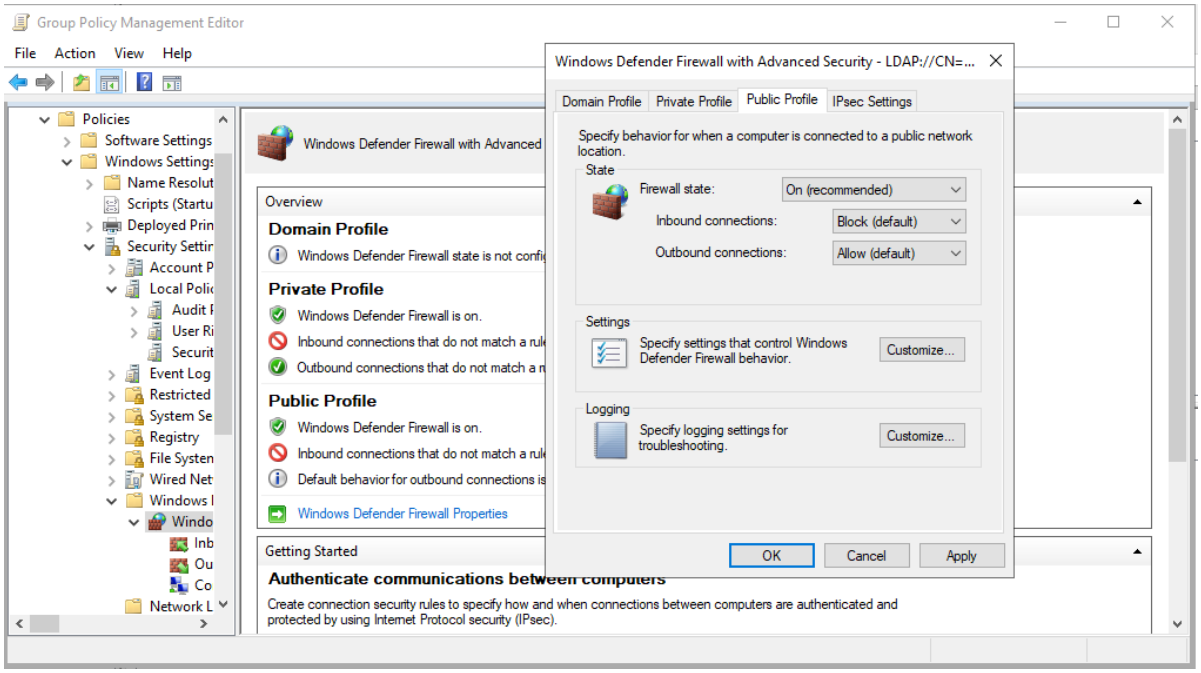


Image 121-Ensure 'Windows Firewall: Public: Outbound connections' is set to 'Allow (default)'

5.2.4 Ensure 'Windows Firewall: Public: Settings: Display a notification' is set to 'No'

Choose this option to have Windows Firewall with Advanced Security show notifications when a program is prevented from receiving inbound connections. The recommended setting is to disable this option. Some organizations might prefer not to alert users when firewall rules block specific network activities to avoid causing unnecessary concern. However, notifications can be useful for troubleshooting network issues related to the firewall.

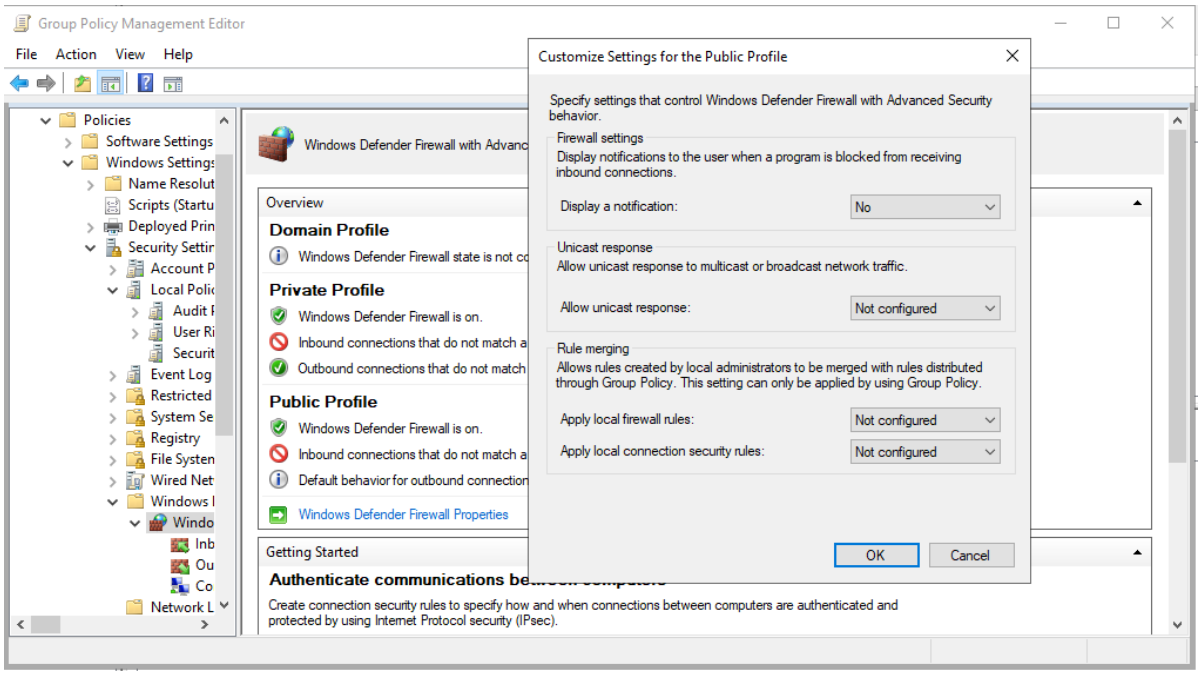


Image 122-Ensure 'Windows Firewall: Public: Settings: Display a notification' is set to 'No'

5.2.5 Ensure 'Windows Firewall: Public: Settings: Apply local firewall rules' is set to 'No'

This setting controls whether local administrators can create local firewall rules that work alongside those set by Group Policy. The recommended state for this setting is: No. If local firewall rules are not applied, it is also advisable to set the Display a notification option to No. Otherwise, users may receive prompts asking if they want to unblock restricted inbound connections, even though their responses will be disregarded. In a Public profile, there should be no individual local firewall exceptions; all settings should be managed through a centralized policy.

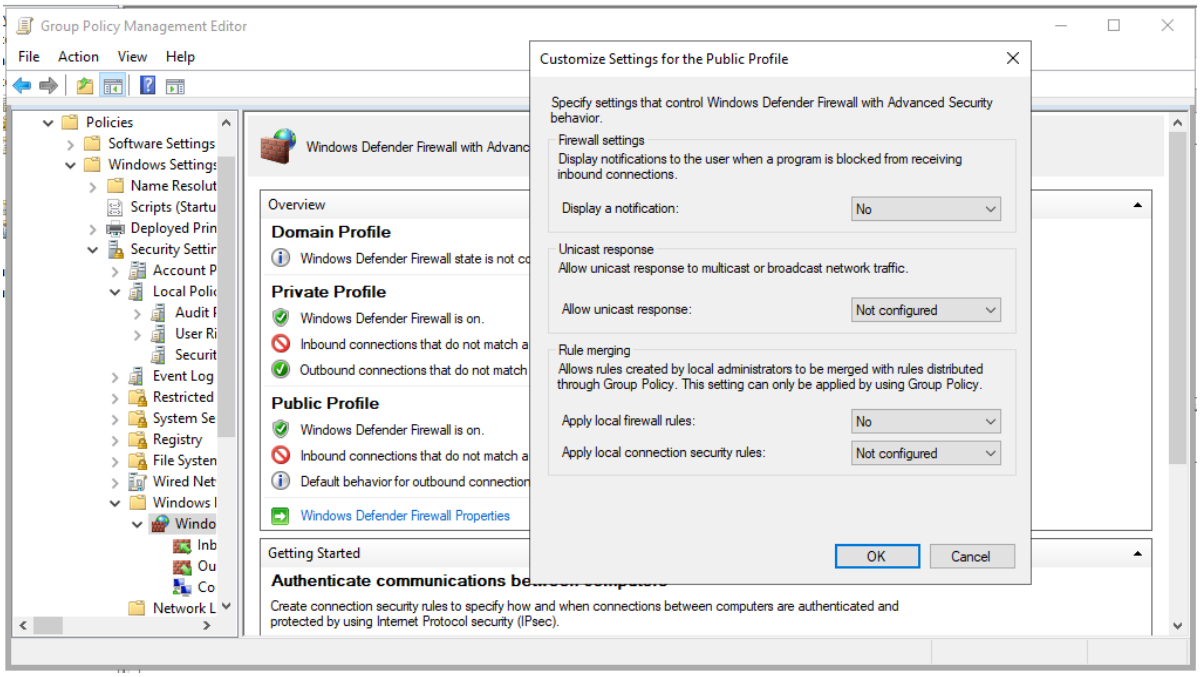


Image 123-Ensure 'Windows Firewall: Public: Settings: Apply local firewall rules' is set to 'No'

5.2.6 Ensure 'Windows Firewall: Public: Settings: Apply local connection security rules' is set to 'No'

This setting determines if local administrators are permitted to create connection security rules that function alongside the rules set by Group Policy. The recommended state for this setting is: No. Allowing administrators to create their own connection security rules could lead to vulnerabilities, potentially exposing the system to remote attacks.

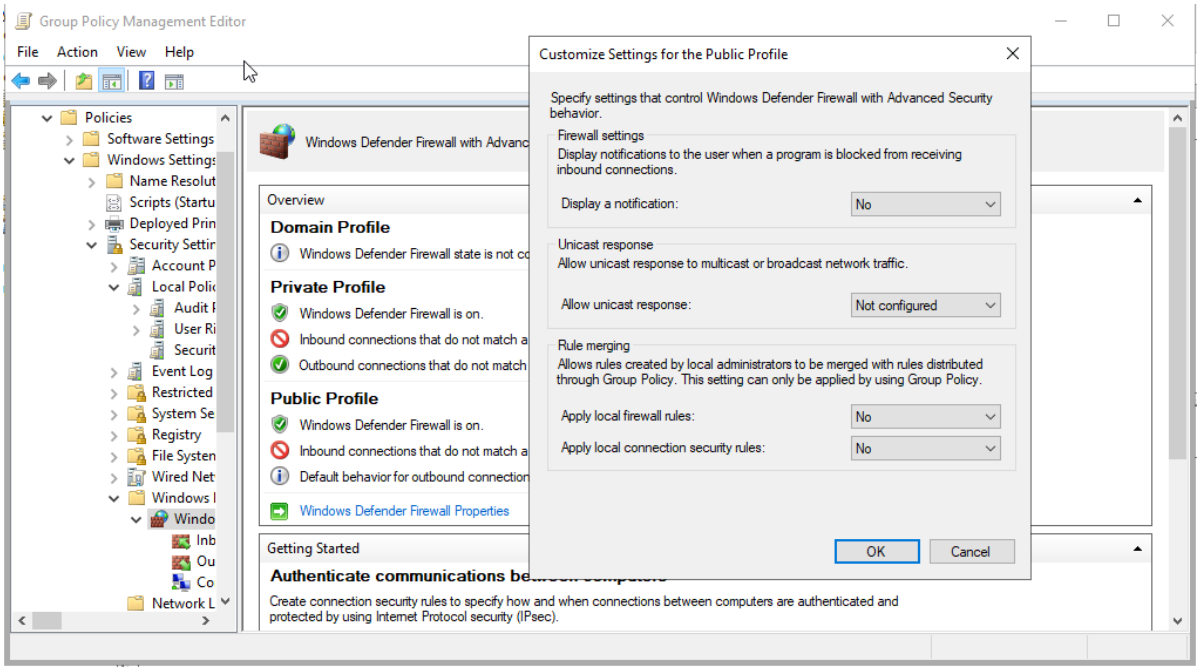


Image 124-Ensure 'Windows Firewall: Public: Settings: Apply local connection security rules' is set to 'No'

5.2.7 Ensure 'Windows Firewall: Public: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\publicfw.log'

This option allows you to specify the path and filename for Windows Firewall's log file. The recommended setting is: %SystemRoot%\System32\logfiles\firewall\publicfw.log. Recording Windows Firewall events is crucial for administrators to analyze system issues or detect unauthorized activities. By default, Microsoft consolidates all firewall events into a single file (pfirewall.log). For better organization and issue identification, it's beneficial to separate the logs by firewall profile (domain, private, public) into distinct files, such as domainfw.log, privatefw.log, and publicfw.log.

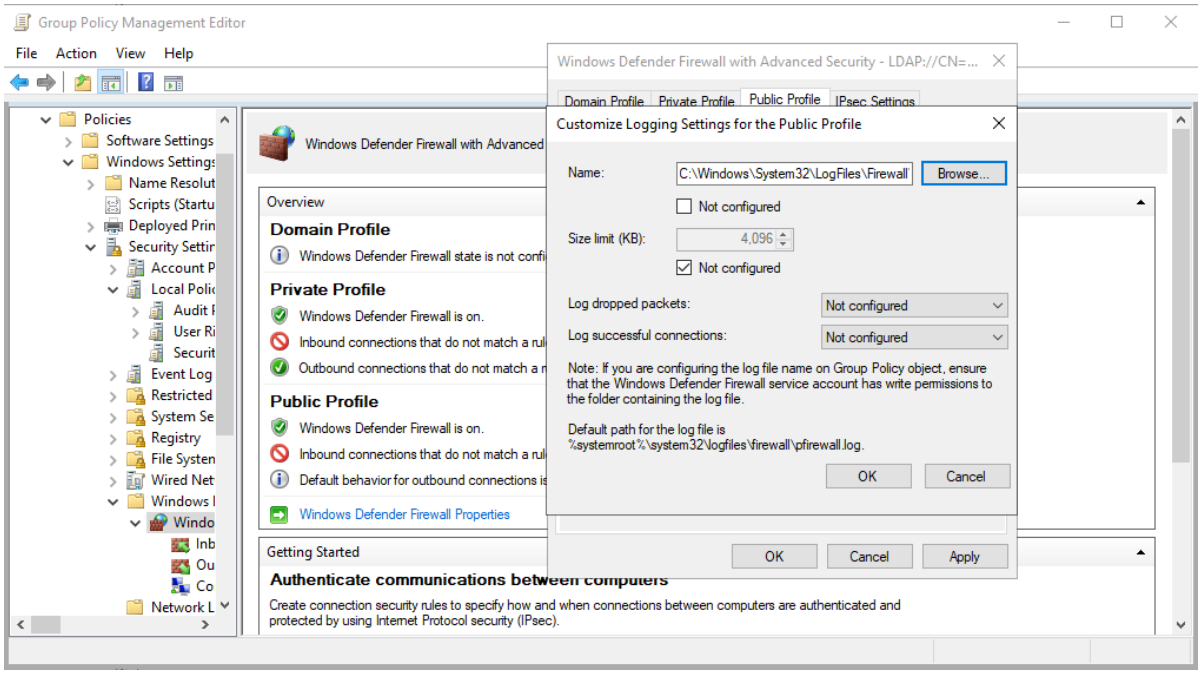


Image 125-Ensure 'Windows Firewall: Public: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\publicfw.log'

5.2.8 Ensure 'Windows Firewall: Public: Logging: Size limit (KB)' is set to '16,384 KB or greater'

This option allows you to set the size limit for the file where Windows Firewall logs its information. The recommended size for this setting is 16,384 KB or more. Recording events is essential for diagnosing system issues or detecting unauthorized activities. Without adequate logging, identifying the root cause of problems or malicious actions becomes challenging.

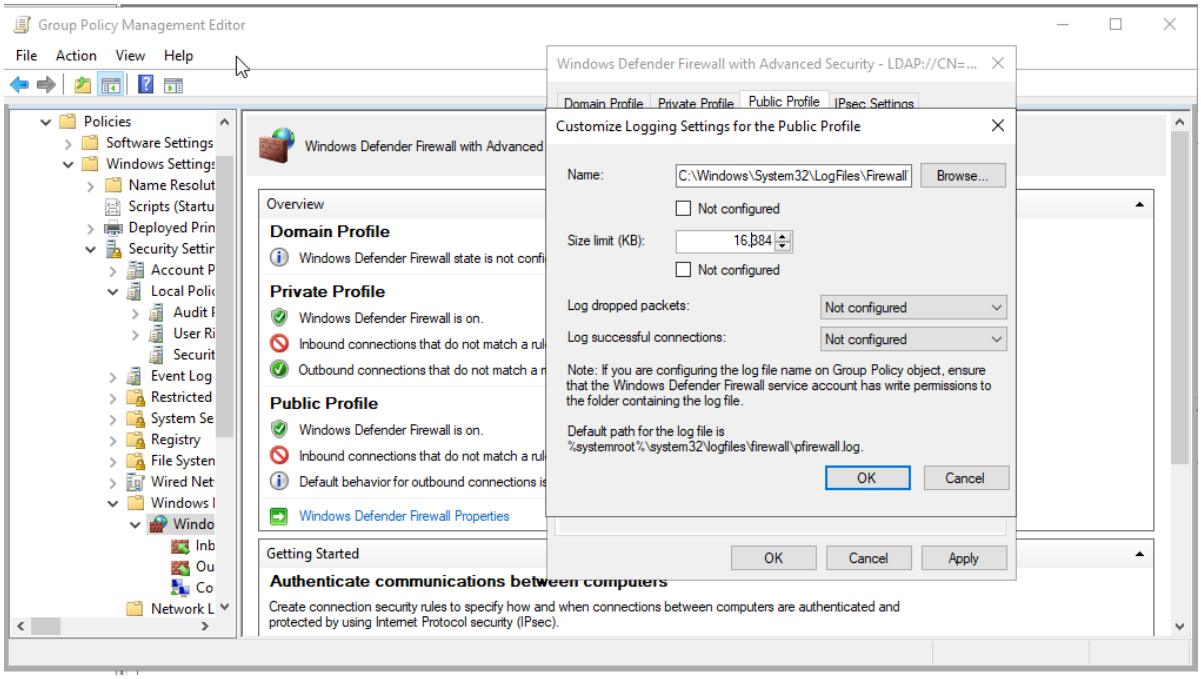


Image 126-Ensure 'Windows Firewall: Public: Logging: Size limit (KB)' is set to '16,384 KB or greater'

5.2.9 Ensure 'Windows Firewall: Public: Logging: Log dropped packets' is set to 'Yes'

This option enables logging for instances when Windows Firewall with Advanced Security discards an inbound packet. The log captures details on why and when a packet was dropped, with entries marked as DROP in the action column. The recommended setting for this is: Yes. Proper logging is crucial for diagnosing system issues and identifying unauthorized activities, as failing to record these events can make it challenging to determine the root cause of problems.

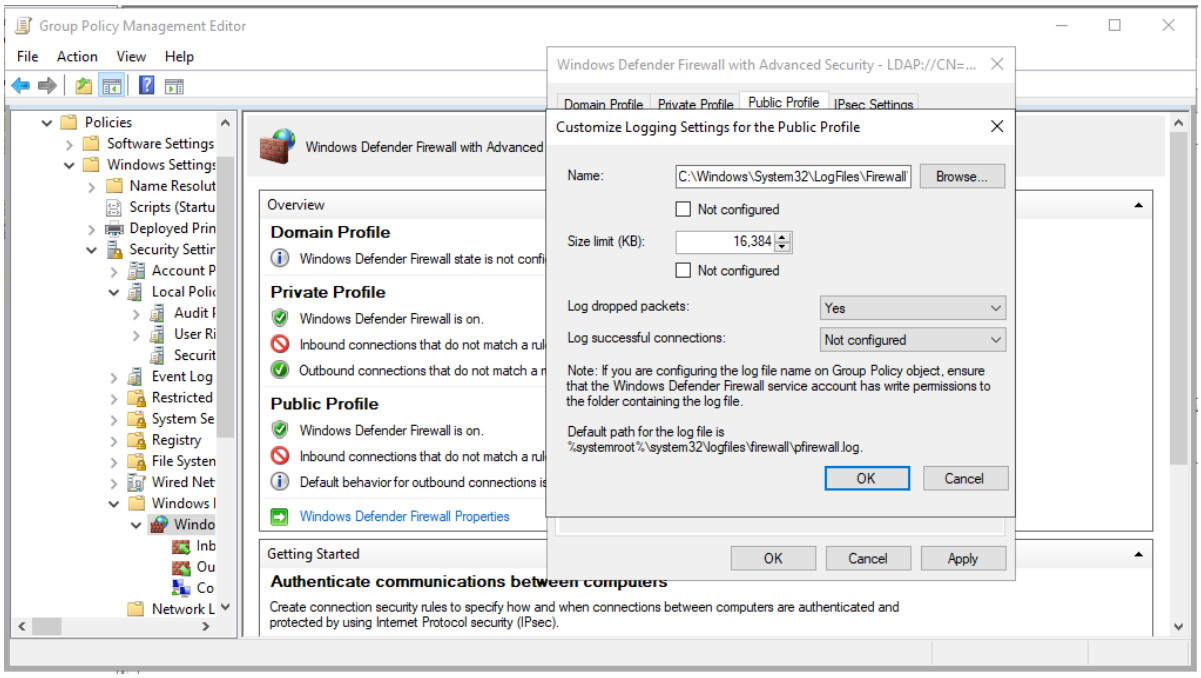


Image 127-Ensure 'Windows Firewall: Public: Logging: Log dropped packets' is set to 'Yes'

5.2.10 Ensure 'Windows Firewall: Public: Logging: Log successful connections' is set to 'Yes'

This setting enables logging for instances when Windows Firewall with Advanced Security permits an inbound connection. The log details the reasons and timing of each allowed connection, with entries marked as ALLOW in the action column. The recommended configuration for this setting is: Yes. Recording these events is essential for diagnosing system issues and tracking unauthorized activities, as failing to log them can make it challenging to pinpoint the causes of problems.

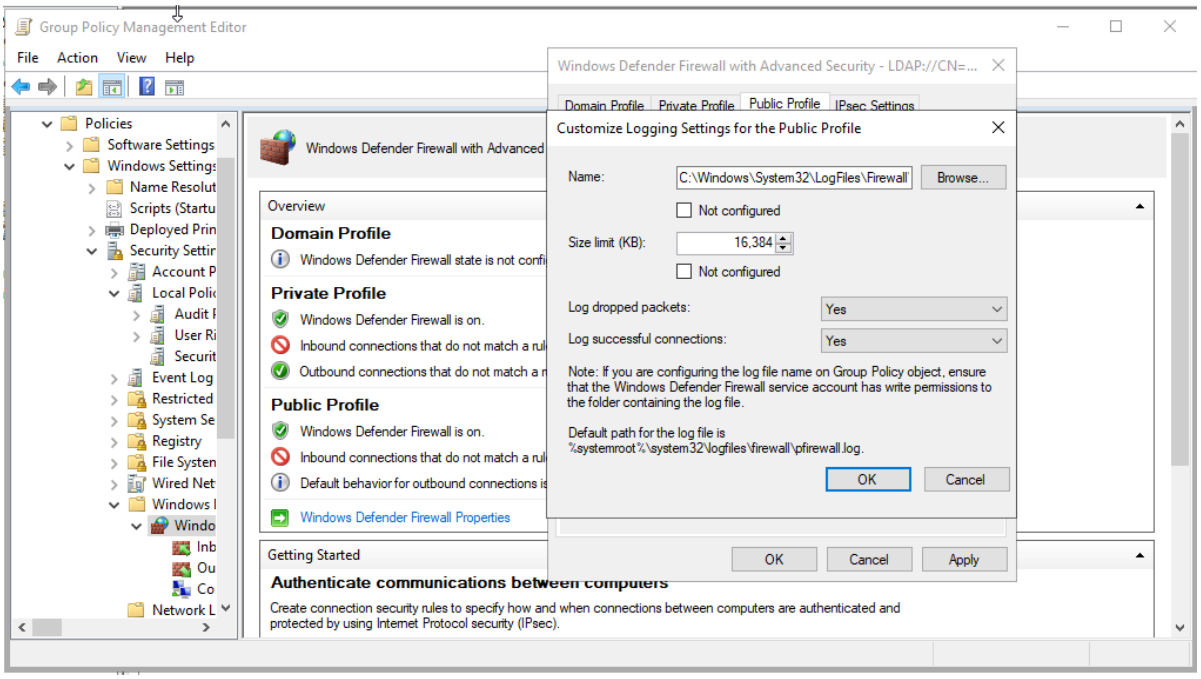


Image 128-Ensure 'Windows Firewall: Public: Logging: Log successful connections' is set to 'Yes'

6 Advanced Audit Policy Configuration

Windows Advanced Audit Policy Configuration allows administrators to define detailed and granular audit policies for tracking and recording security-related events on a system. This feature enables the monitoring of specific activities such as logon attempts, access to sensitive data, changes to system settings, and the use of administrative privileges. By configuring advanced audit policies, organizations can enhance their security posture by ensuring comprehensive event logging, facilitating compliance with regulatory requirements, and providing valuable insights for incident investigation and response.

6.1 Account Logon

The Account Logon Group Policy manages the authentication process for accessing systems. It defines policies for verifying user credentials, such as passwords or smart cards, ensuring secure logon procedures. By enforcing strong authentication measures, it helps protect against unauthorized access and secures the organization's systems and data.

6.1.1 Ensure 'Audit Credential Validation' is set to 'Success and Failure'

This subcategory logs the results of validation tests on credentials submitted for user account logon requests, occurring on the computer authoritative for the credentials—Domain Controllers for domain accounts and the local computer for local accounts. In domain environments, most Account Logon events are logged in the Domain Controllers' Security log, but they can also occur on other computers when local accounts are used.

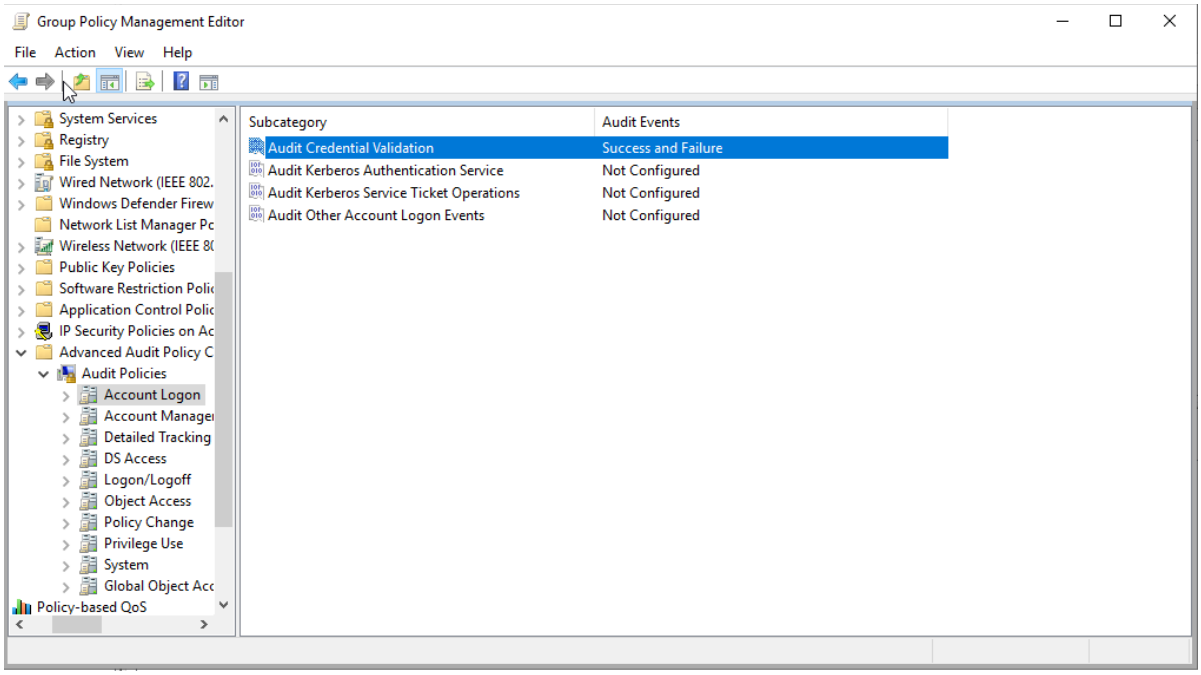


Image 129-Ensure 'Audit Credential Validation' is set to 'Success and Failure'

6.1.2 Ensure 'Audit Kerberos Authentication Service' is set to 'Success and Failure'

This subcategory logs events generated after a Kerberos authentication TGT request. Kerberos is a distributed authentication service that allows a client to prove its identity to a server without sending data across the network, helping prevent impersonation. Relevant events include:

- 4768: A Kerberos authentication ticket (TGT) was requested.
- 4771: Kerberos pre-authentication failed.
- 4772: A Kerberos authentication ticket request failed.

The recommended state for this setting is: Success and Failure.

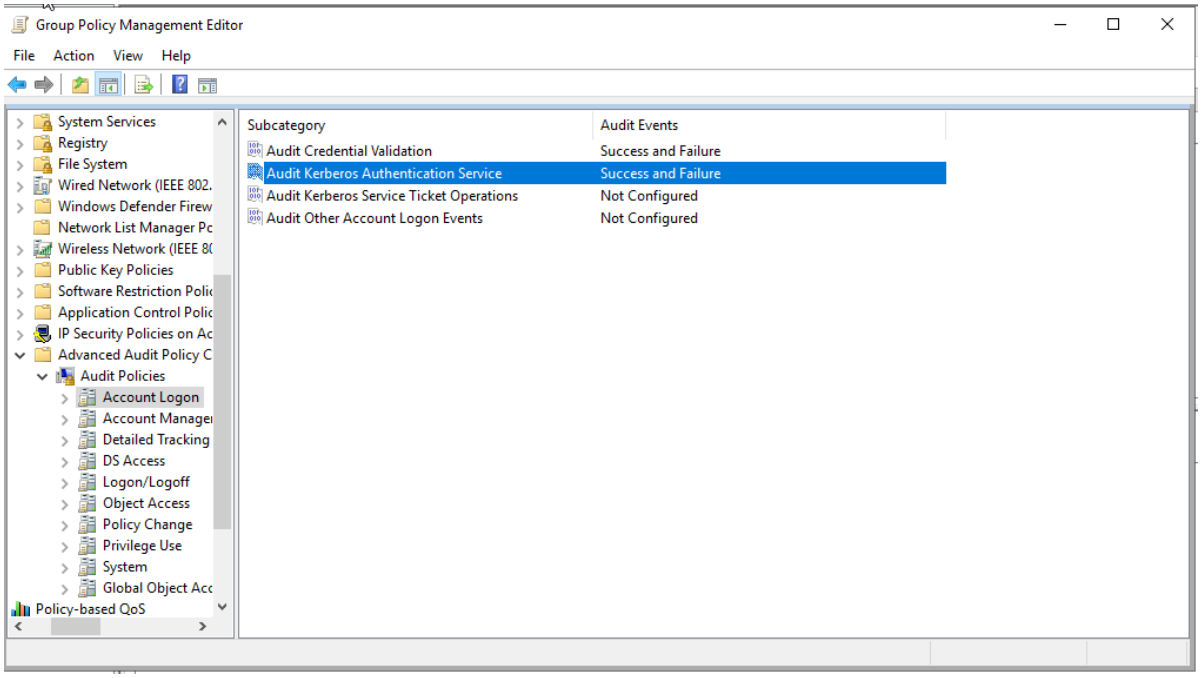


Image 130-Ensure 'Audit Kerberos Authentication Service' is set to 'Success and Failure'

6.1.3 Ensure 'Audit Kerberos Service Ticket Operations' is set to 'Success and Failure'

This subcategory logs events generated by Kerberos authentication ticket-granting ticket (TGT) requests and service ticket (TGS) requests, which occur during service use and access requests by specific accounts. Auditing these events captures the IP address from which the TGS was requested, the time of the request, and the encryption type used. Relevant events include:

- 4769: A Kerberos service ticket was requested.
- 4770: A Kerberos service ticket was renewed.
- 4773: A Kerberos service ticket request failed.

The recommended state for this setting is: Success and Failure.

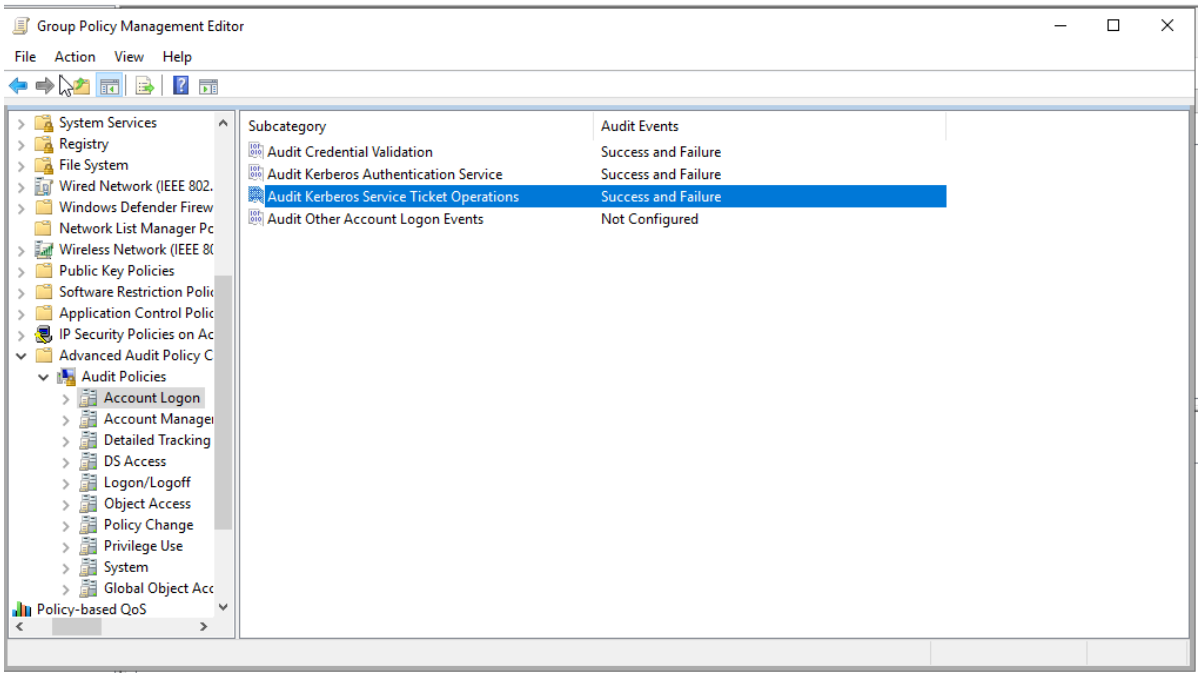


Image 131-Ensure 'Audit Kerberos Service Ticket Operations' is set to 'Success and Failure'

6.2 Account Management

The Account Management Group Policy controls the creation, modification, and deletion of user accounts. It includes policies for managing account properties, such as password requirements, account lockout settings, and permissions. This ensures proper oversight of user accounts, enhancing security and reducing the risk of unauthorized access to the organization's resources.

6.2.1 Ensure 'Audit Application Group Management' is set to 'Success and Failure'

This policy setting audits events related to changes in application groups, such as:

- Creation, modification, or deletion of an application group.
- Addition or removal of a member from an application group.

Application groups are used by Windows Authorization Manager, a framework for integrating role-based access control (RBAC) into applications. For more information, visit MSDN - Windows Authorization Manager.

The recommended state for this setting is: Success and Failure. Auditing these events can be useful when investigating incidents.

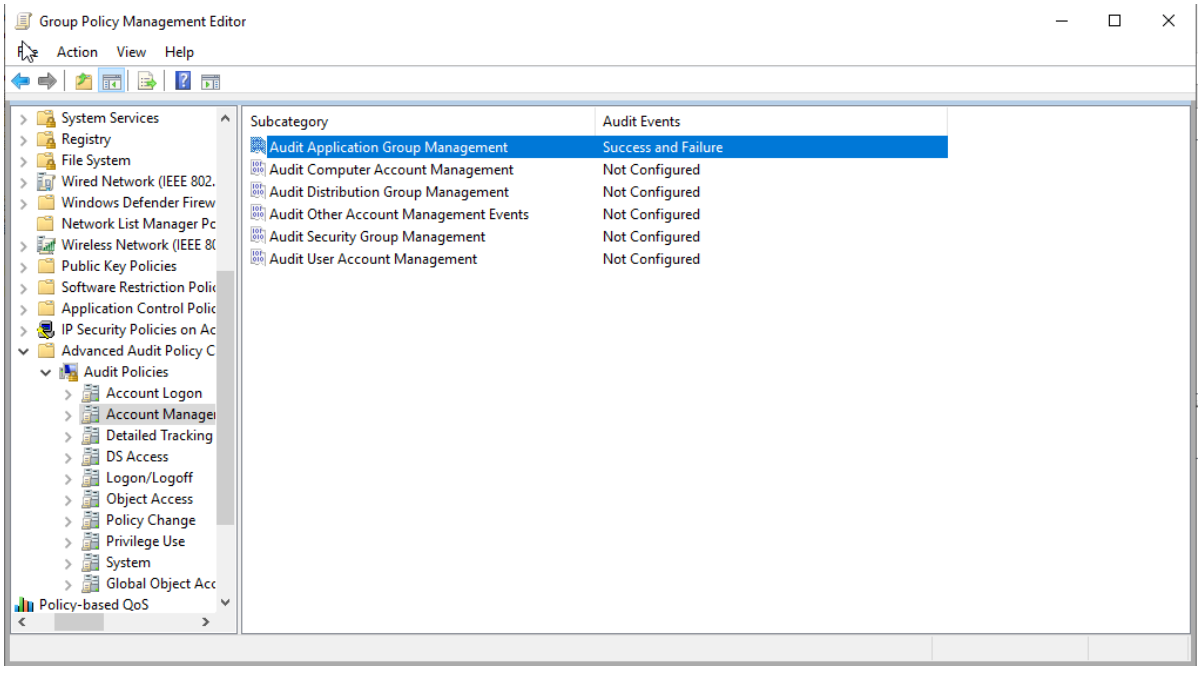


Image 132-Ensure 'Audit Application Group Management' is set to 'Success and Failure'

6.2.2 Ensure 'Audit Computer Account Management' is set to include 'Success'

This subcategory logs events related to computer account management, including the creation, modification, deletion, renaming, disabling, or enabling of computer accounts. Key events include:

- 4741: A computer account was created.
- 4742: A computer account was changed.
- 4743: A computer account was deleted.

The recommended state for this setting is: Success. Auditing these events can be useful for investigating incidents.

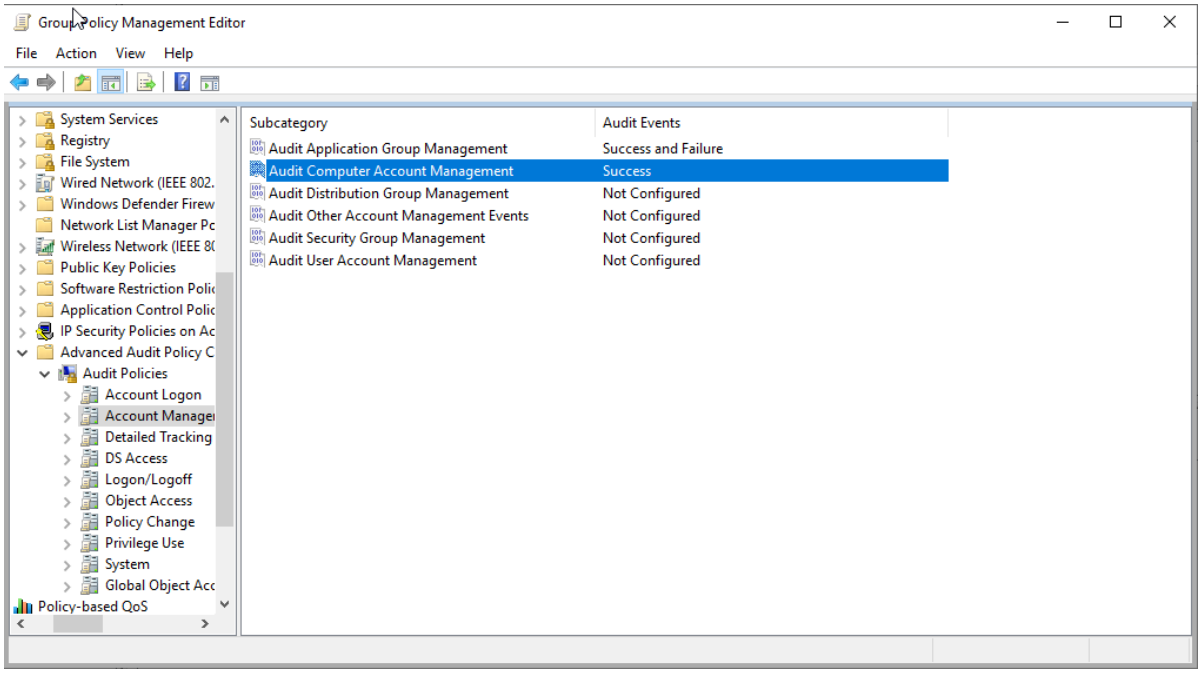


Image 133-Ensure 'Audit Computer Account Management' is set to include 'Success'

6.2.3 Ensure 'Audit Distribution Group Management' is set to include 'Success'

This subcategory logs events related to distribution group management, such as creating, modifying, and deleting groups, and adding or removing group members. Key events include:

- 4744-4748: Security-disabled local group events.
- 4749-4753: Security-disabled global group events.
- 4759-4763: Security-disabled universal group events.

The recommended state for this setting is: Success. Auditing these events helps organizations investigate incidents like unauthorized additions to sensitive groups.

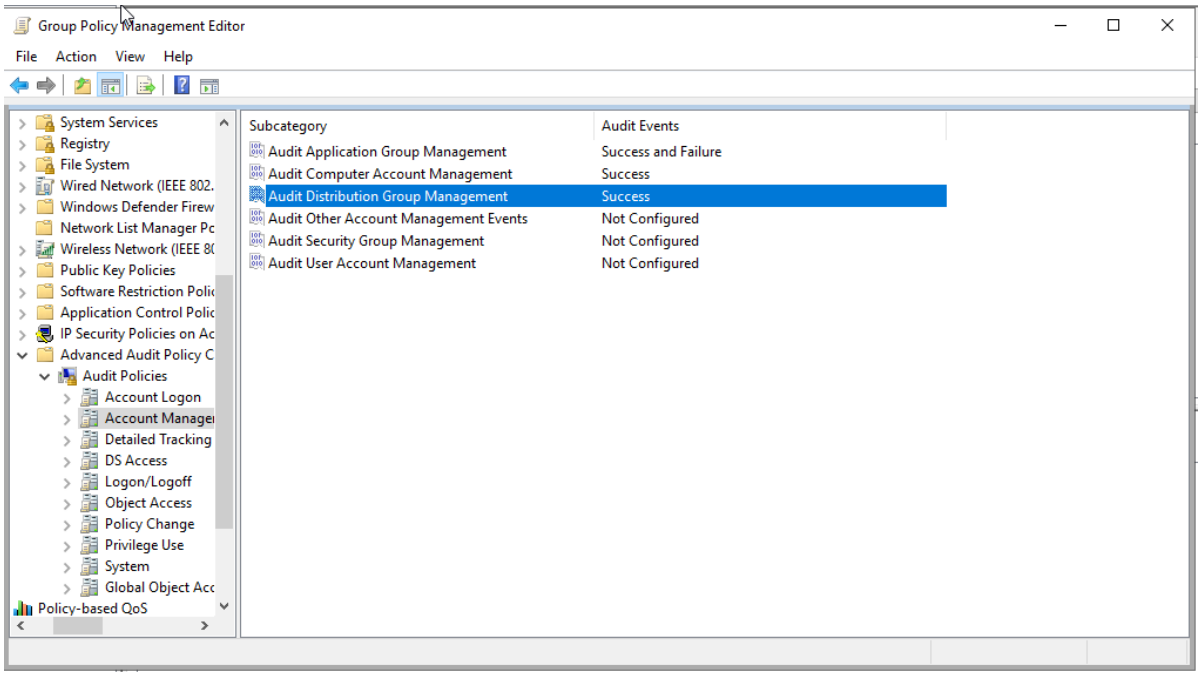


Image 134-Ensure 'Audit Distribution Group Management' is set to include 'Success'

6.2.4 Ensure 'Audit Other Account Management Events' is set to include 'Success'

This subcategory logs other account management events, including:

- 4782: Access to an account's password hash.
- 4793: Invocation of the Password Policy Checking API.

The recommended state for this setting is: Success. Auditing these events can aid in investigating security incidents.

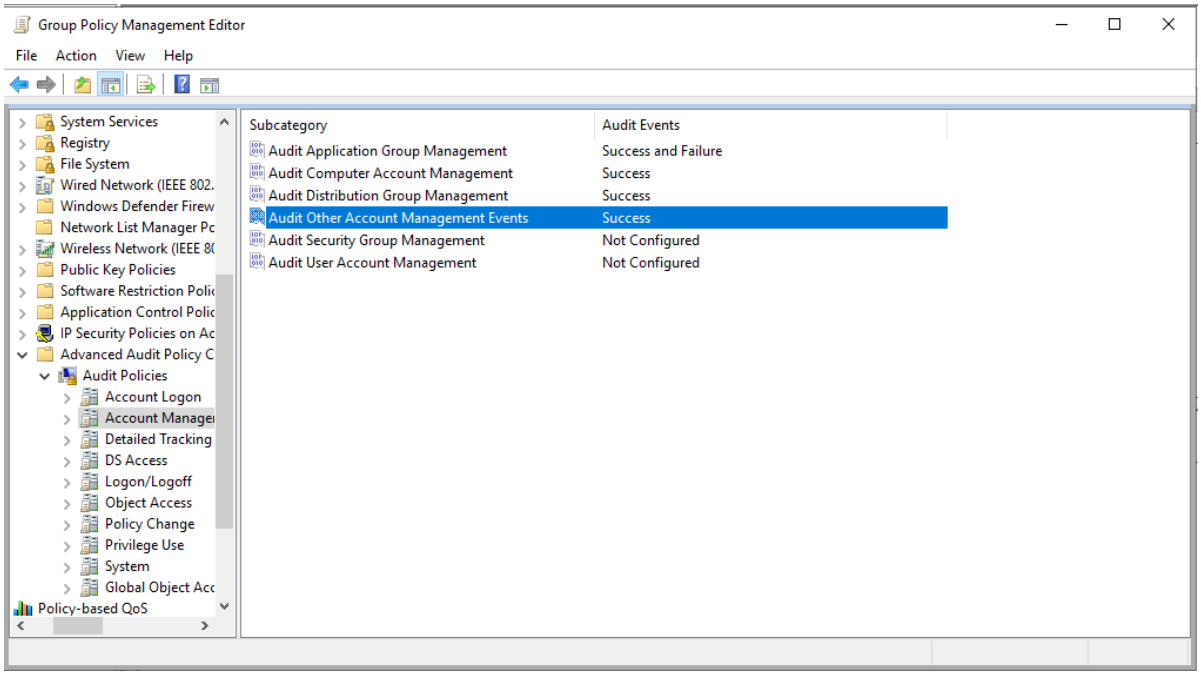


Image 135-Ensure 'Audit Other Account Management Events' is set to include 'Success'

6.2.5 Ensure 'Audit Security Group Management' is set to include 'Success'

This subcategory tracks events related to security group management, such as creating, modifying, or deleting security groups, and adding or removing members.

The recommended state for this setting is: Success. Tracking these events helps in investigating security issues.

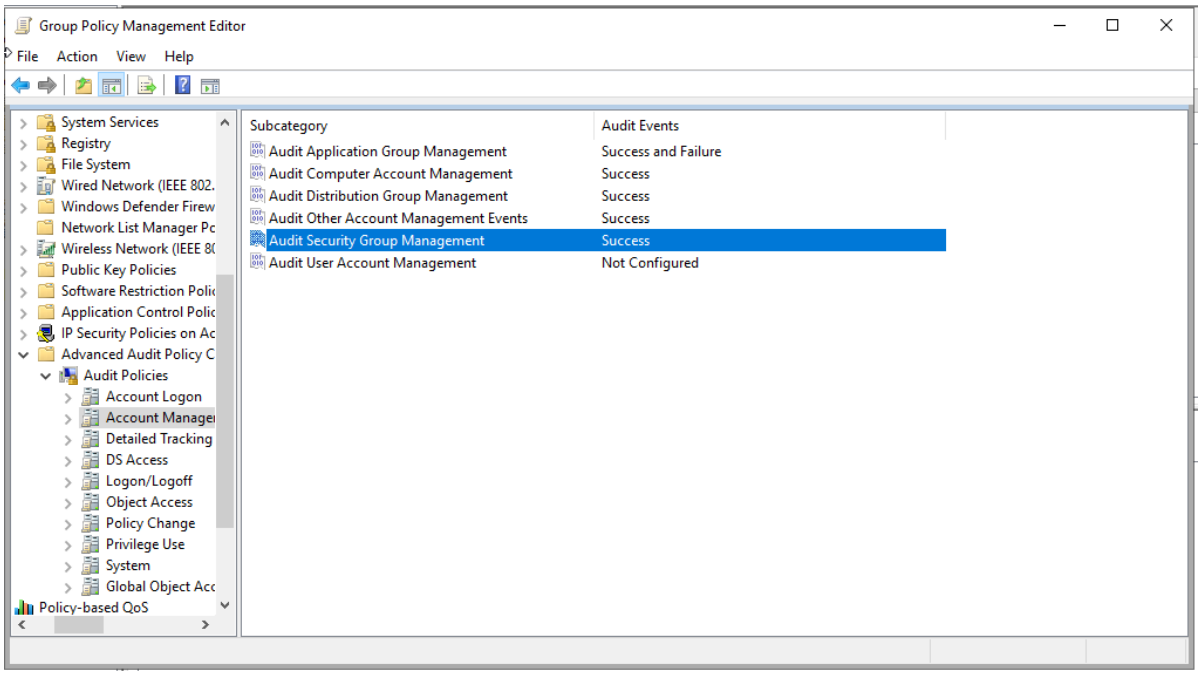


Image 136-Ensure 'Audit Security Group Management' is set to include 'Success'

6.2.6 Ensure 'Audit User Account Management' is set to 'Success and Failure'

This subcategory logs events related to user account management, including the creation, modification, and deletion of accounts, as well as changes to account status and passwords. Enabling this audit setting allows administrators to monitor and detect both authorized and unauthorized actions regarding user accounts.

The recommended setting is: Success and Failure. Monitoring these events can be crucial for investigating security incidents.

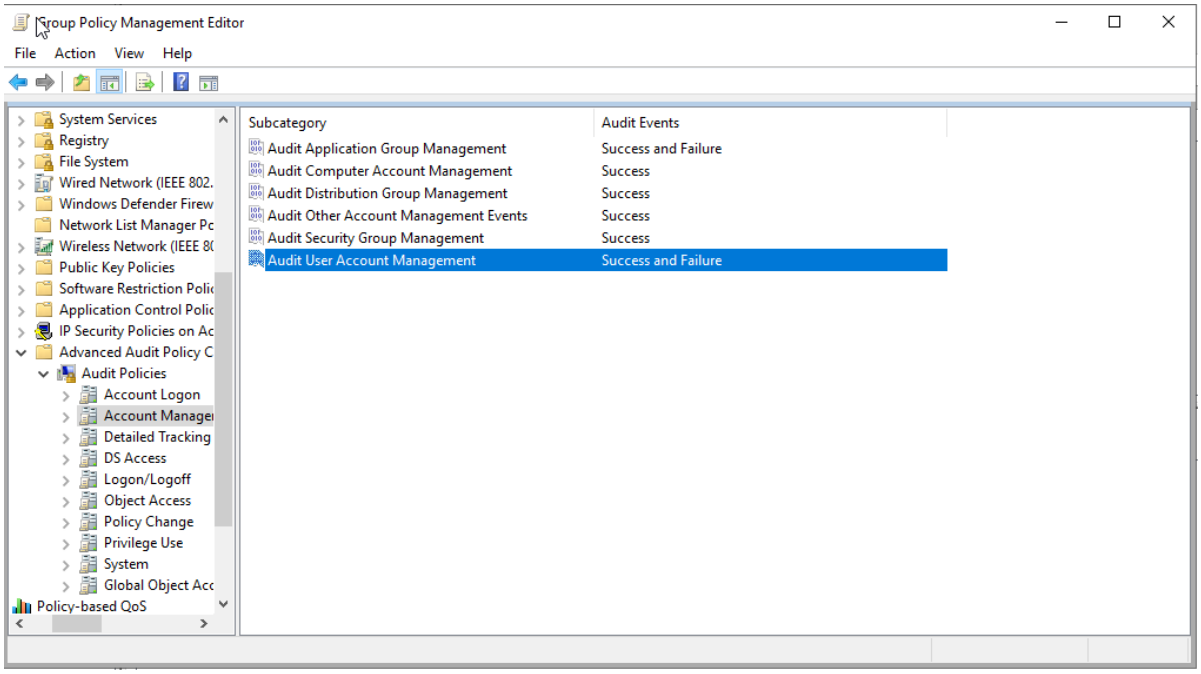


Image 137-Ensure 'Audit User Account Management' is set to 'Success and Failure'

6.3 Detailed Tracking

The Detailed Tracking Group Policy focuses on recording specific events related to system and application activities. This includes monitoring program execution, resource access, and user activities. By enabling detailed tracking, administrators can gain deeper insights into system behavior and detect potential security incidents, aiding in forensic analysis and ensuring compliance with organizational policies.

6.3.1 Ensure 'Audit PNP Activity' is set to include 'Success'

This policy setting enables auditing for events when the plug and play system detects an external device. The recommended configuration for this setting is to include: Success. Note that to access and configure this setting in Group Policy, a Windows 10, Server 2016, or later operating system is required. Enabling this setting helps IT staff monitor and detect when devices are connected to the system, which can be useful for identifying unauthorized or unapproved devices.

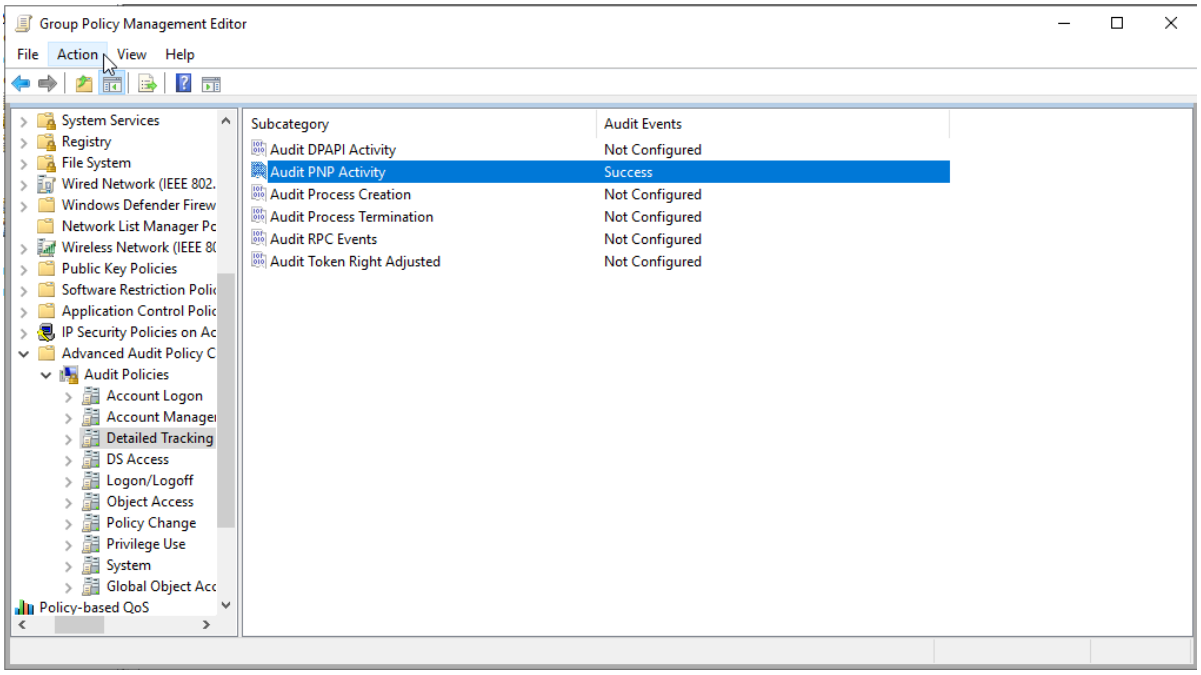


Image 138-Ensure 'Audit PNP Activity' is set to include 'Success'

6.3.2 Ensure 'Audit Process Creation' is set to include 'Success'

This subcategory tracks the creation of new processes, including details about the program or user that initiated them. Events covered in this subcategory are:

- 4688: A new process was created.
- 4696: A primary token was assigned to a process.

For the latest details on this setting, consult Microsoft Knowledge Base article 947226: Description of Security Events in Windows Vista and Windows Server 2008. The recommended configuration is to include: Success. Auditing these events can be valuable for investigating security incidents.

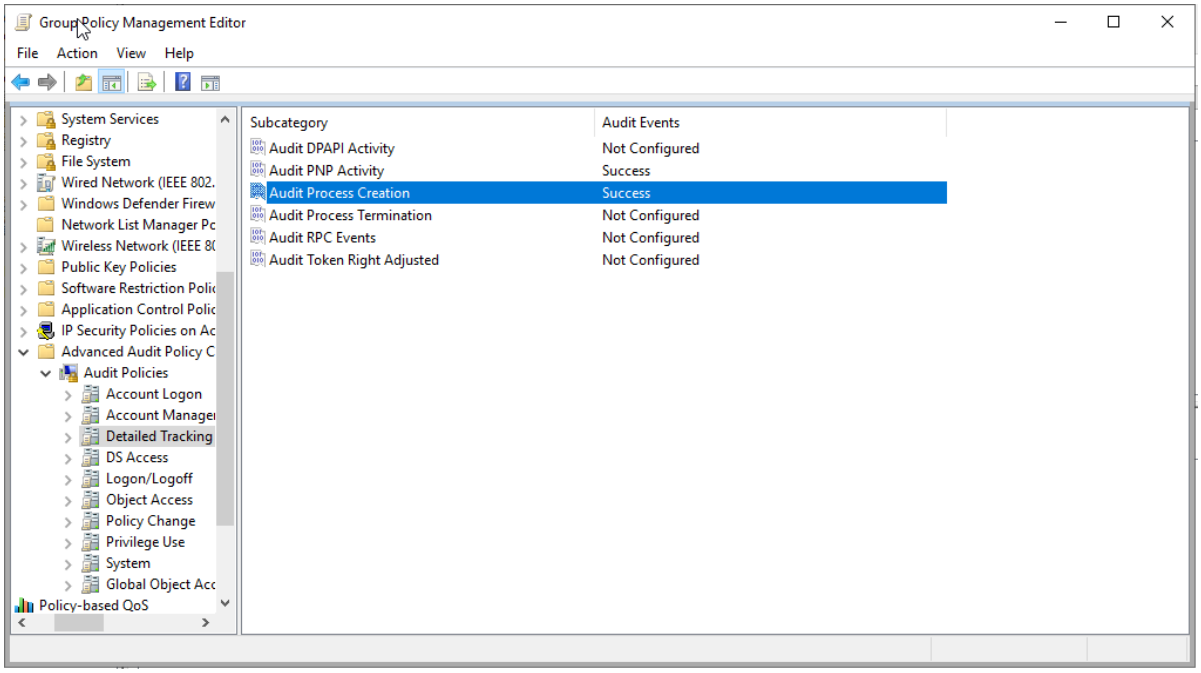


Image 139-Ensure 'Audit Process Creation' is set to include 'Success'

6.4 DS Access

The DS Access Group Policy governs the auditing of access to directory services, such as Active Directory. This policy setting allows administrators to track and log changes to directory objects, including modifications to user accounts, group memberships, and other directory structures. By enabling DS Access auditing, organizations can enhance security by detecting unauthorized access or changes, ensuring that directory services are monitored and protected.

6.4.1 Ensure 'Audit Directory Service Access' is set to include 'Failure'

This subcategory tracks access to Active Directory Domain Services (AD DS) objects, but only for objects with System Access Control Lists (SACLs) that trigger audit events when accessed in a manner specified by their SACL. This is similar to directory service access events in earlier versions of Windows Server and is applicable only to Domain Controllers. Events in this subcategory include:

- 4662: An operation was performed on an object.

The recommended setting is to include: Failure. Auditing these events can be valuable for investigating security incidents.

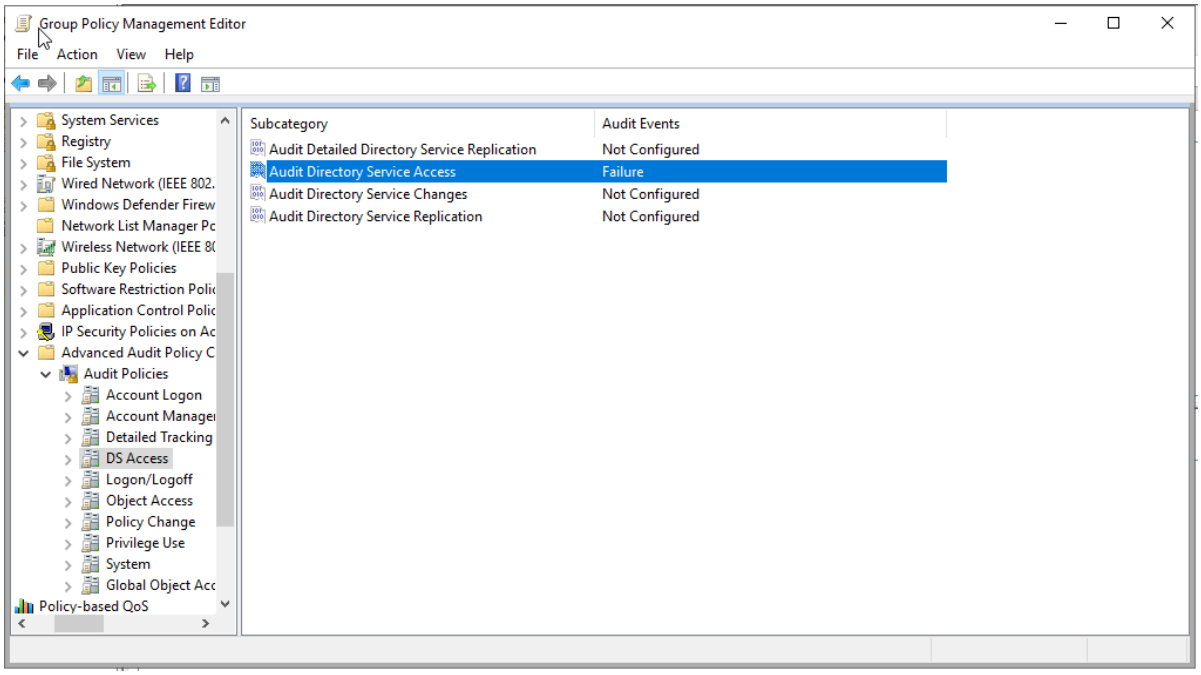


Image 140-Ensure 'Audit Directory Service Access' is set to include 'Failure'

6.4.2 Ensure 'Audit Directory Service Changes' is set to include 'Success'

This subcategory tracks changes to objects in Active Directory Domain Services (AD DS), including creation, modification, movement, and undeletion of objects. It reports on changes by showing the old and new values of the properties affected. Audit events are generated only for objects with System Access Control Lists (SACLs) when accessed according to their SACL specifications. Note that not all objects or properties may trigger audit events due to schema settings. This applies only to Domain Controllers. Relevant events include:

- 5136: A directory service object was modified.
- 5137: A directory service object was created.
- 5138: A directory service object was undeleted.
- 5139: A directory service object was moved.

The recommended setting is to include: Success. Auditing these events can assist in investigating security incidents.

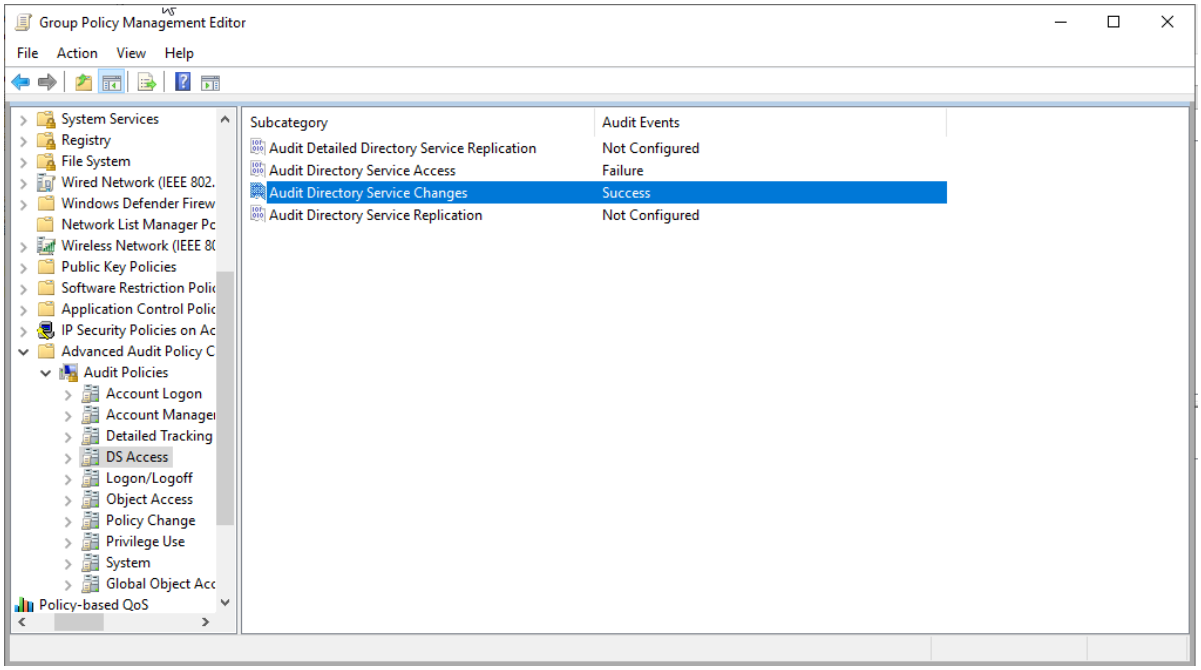


Image 141-Ensure 'Audit Directory Service Changes' is set to include 'Success'

6.5 Logon/Logoff

The Logon/Logoff Group Policy manages the auditing of user logon and logoff events on a system. This policy allows administrators to track user activity, including successful and failed login attempts, session duration, and network access. By enabling logon/logoff auditing, organizations can monitor access patterns, detect unauthorized attempts, and enhance overall security.

6.5.1 Ensure 'Audit Account Lockout' is set to include 'Failure'

This subcategory monitors instances where a user's account is locked out due to excessive failed login attempts. Relevant events include:

- 4625: An account failed to log on.

The recommended setting is to log: Failure. Auditing these events can be valuable for investigating security incidents.

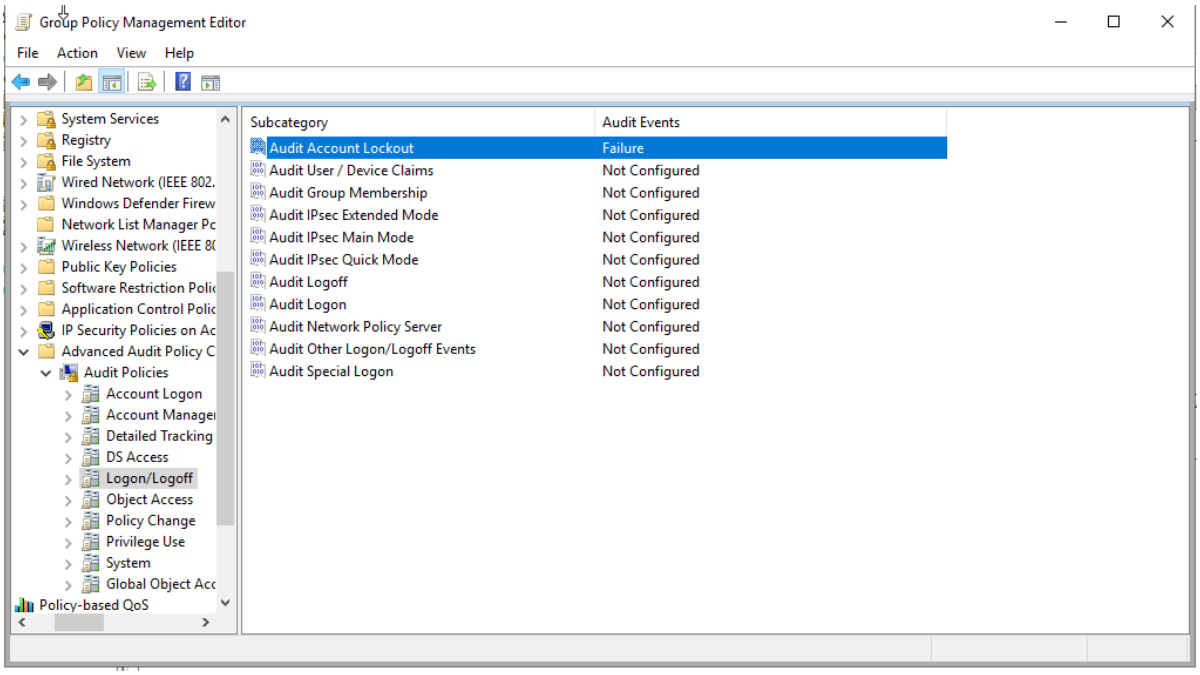


Image 142-Ensure 'Audit Account Lockout' is set to include 'Failure'

6.5.2 Ensure 'Audit Group Membership' is set to include 'Success'

This policy enables the auditing of group membership information within a user's logon token. Events are recorded on the computer where the logon session is initiated. For interactive logons, the security audit event is generated on the computer the user logs into. For network logons, such as when accessing a shared folder, the event is logged on the computer hosting the resource. The recommended setting is to log: Success. Note that Windows 10, Server 2016, or newer is required to configure this setting in Group Policy. Auditing these events can be helpful for investigating security incidents.

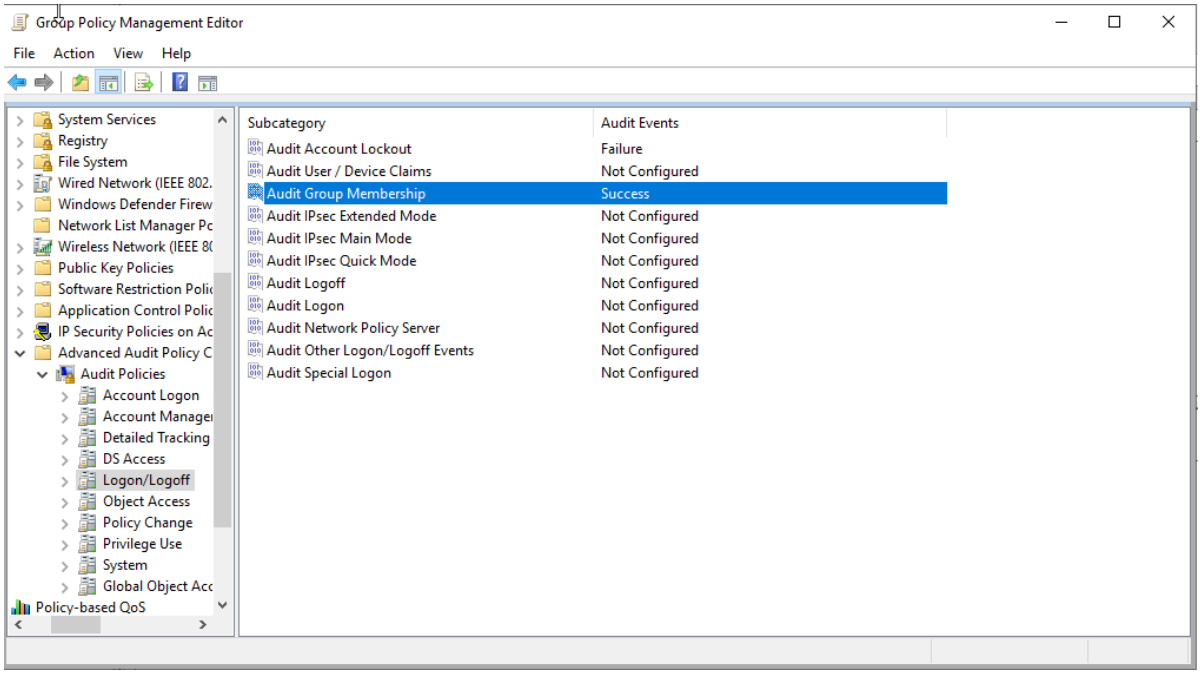


Image 143-Ensure 'Audit Group Membership' is set to include 'Success'

6.5.3 Ensure 'Audit Logoff' is set to include 'Success'

This subcategory tracks user logoff events from the system. These events are recorded on the computer where the logoff occurs. For interactive logons, the events are generated on the computer the user logs into, while for network logons accessing shared resources, the events are recorded on the computer hosting the resource. If this setting is configured to No auditing, it becomes challenging to determine which user accessed or attempted to access organizational computers. Events in this subcategory include:

• 4634: An account was logged off.

• 4647: User initiated logoff.

The recommended setting is to include: Success. Auditing these events can aid in investigating security incidents.

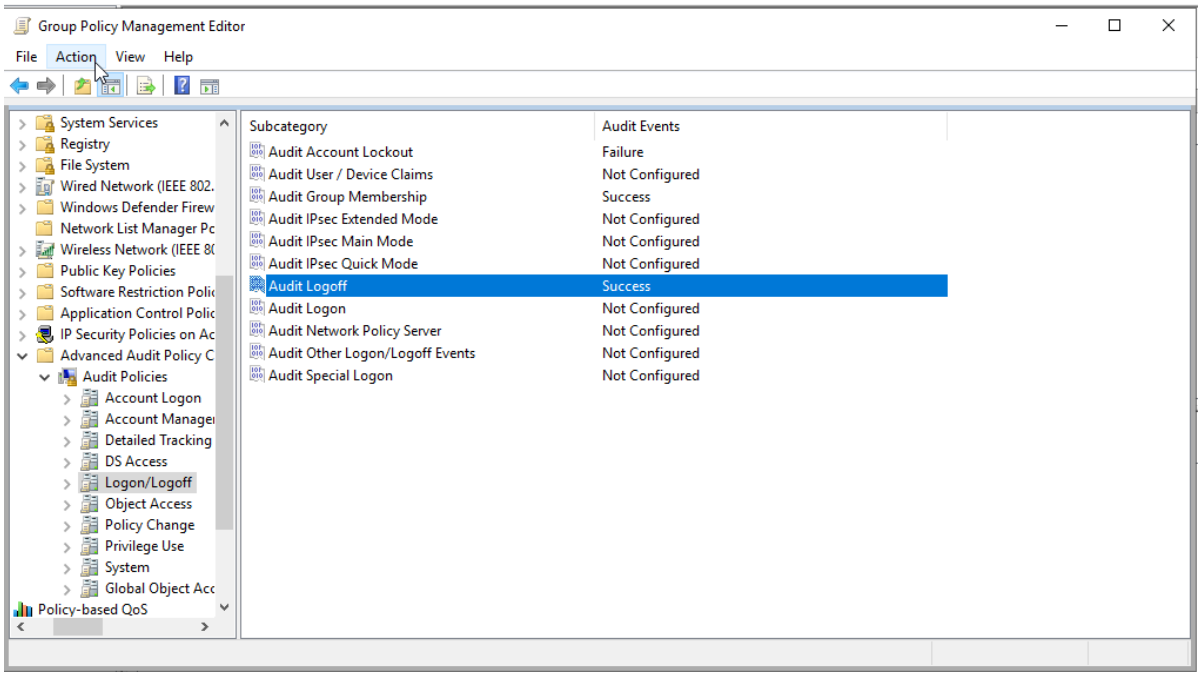


Image 144-Ensure 'Audit Logoff' is set to include 'Success'

6.5.4 Ensure 'Audit Logon' is set to 'Success and Failure'

This subcategory tracks user logon attempts to the system. Events are recorded on the computer where the logon attempt occurs. For interactive logons, the events are generated on the computer the user logs into, while for network logons accessing shared resources, the events are logged on the computer hosting the resource. Without auditing enabled, it becomes challenging to determine which users have accessed or attempted to access organizational computers. Events for this subcategory include:

• 4624: An account was successfully logged on.

• 4625: An account failed to log on.

• 4648: A logon attempt used explicit credentials.

• 4675: SIDs were filtered.

The recommended setting is to include: Success and Failure. Auditing these events can help in investigating security incidents.

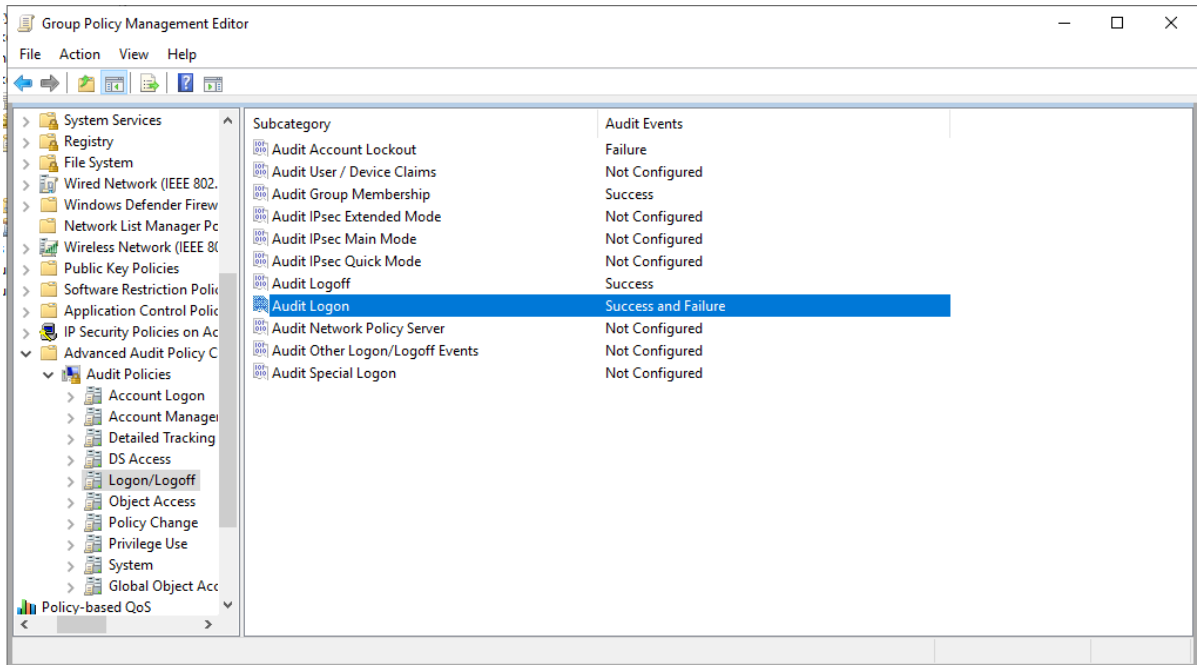


Image 145-Ensure 'Audit Logon' is set to 'Success and Failure'

6.5.5 Ensure 'Audit Other Logon/Logoff Events' is set to 'Success and Failure'

This subcategory tracks various logon and logoff-related events, including Remote Desktop Services session activities, using RunAs to execute processes under different accounts, and workstation locking and unlocking.

The recommended setting is to include: Success and Failure. Auditing these events is valuable for investigating security incidents.

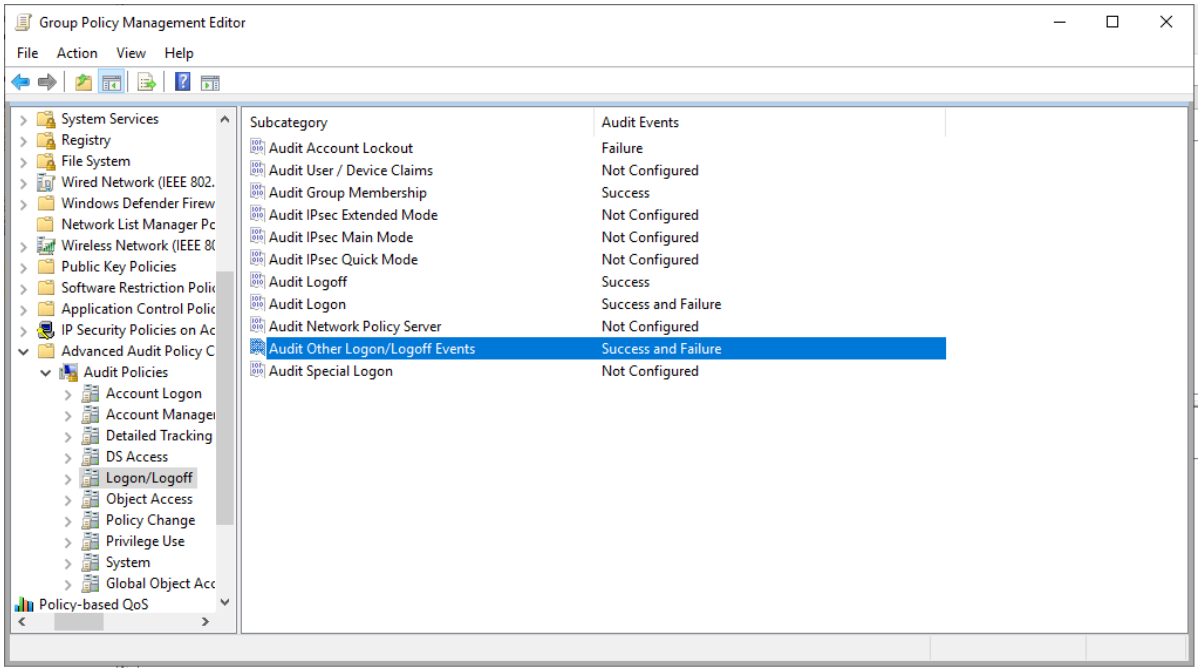


Image 146-Ensure 'Audit Other Logon/Logoff Events' is set to 'Success and Failure'

6.5.6 Ensure 'Audit Special Logon' is set to include 'Success'

This subcategory monitors instances of special logons, which are logons with administrator-equivalent privileges that allow elevation of processes to higher levels. Events reported in this subcategory include:

• 4964: Special groups were assigned to a new logon.

The recommended setting is to include: Success. Auditing these events is beneficial for investigating security incidents.

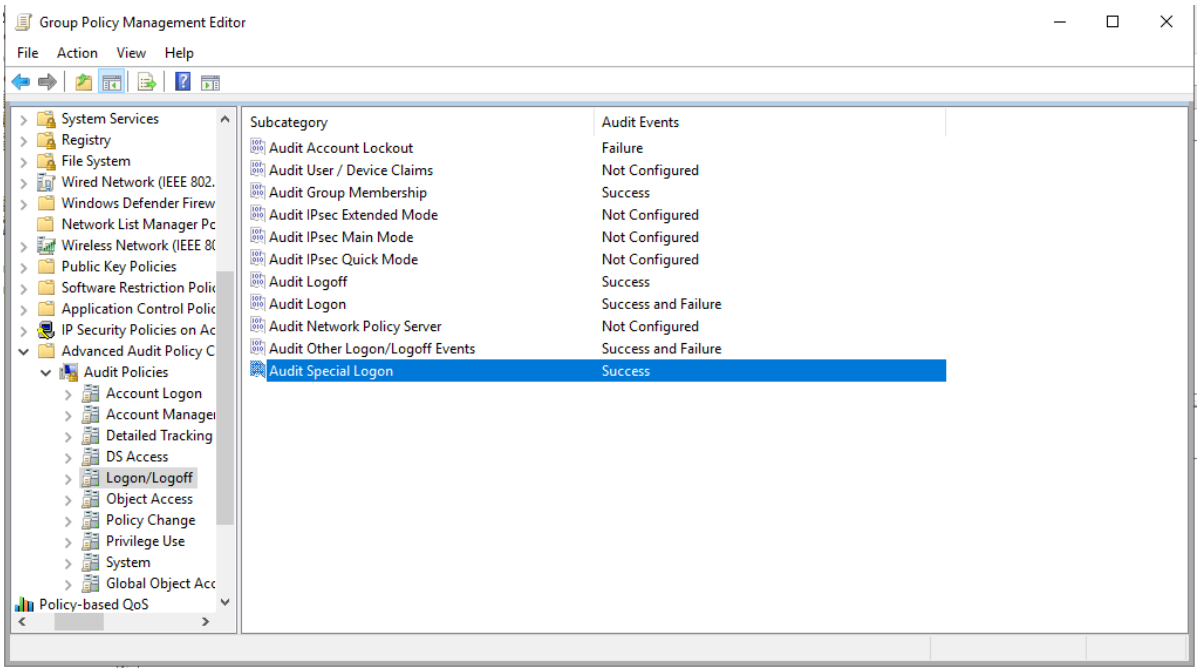


Image 147-Ensure 'Audit Special Logon' is set to include 'Success'

6.6 Object Access

The Object Access Group Policy manages the auditing of interactions with objects such as files, folders, registry keys, and printers. This policy allows administrators to track attempts to access, modify, or delete objects, providing detailed logs of successful and failed actions. Enabling object access auditing helps in detecting unauthorized access to sensitive data, ensuring compliance, and enhancing security monitoring.

6.6.1 Ensure 'Audit Detailed File Share' is set to include 'Failure'

This subcategory enables auditing of attempts to access files and folders on a shared network folder. Events tracked in this subcategory include:

• 5145: A network share object was queried to determine if the client could be granted the desired access.

The recommended setting is to include: Failure. Auditing these failures helps identify unauthorized users who tried—and failed—to access files or folders on the network, which may indicate potential malicious activity.

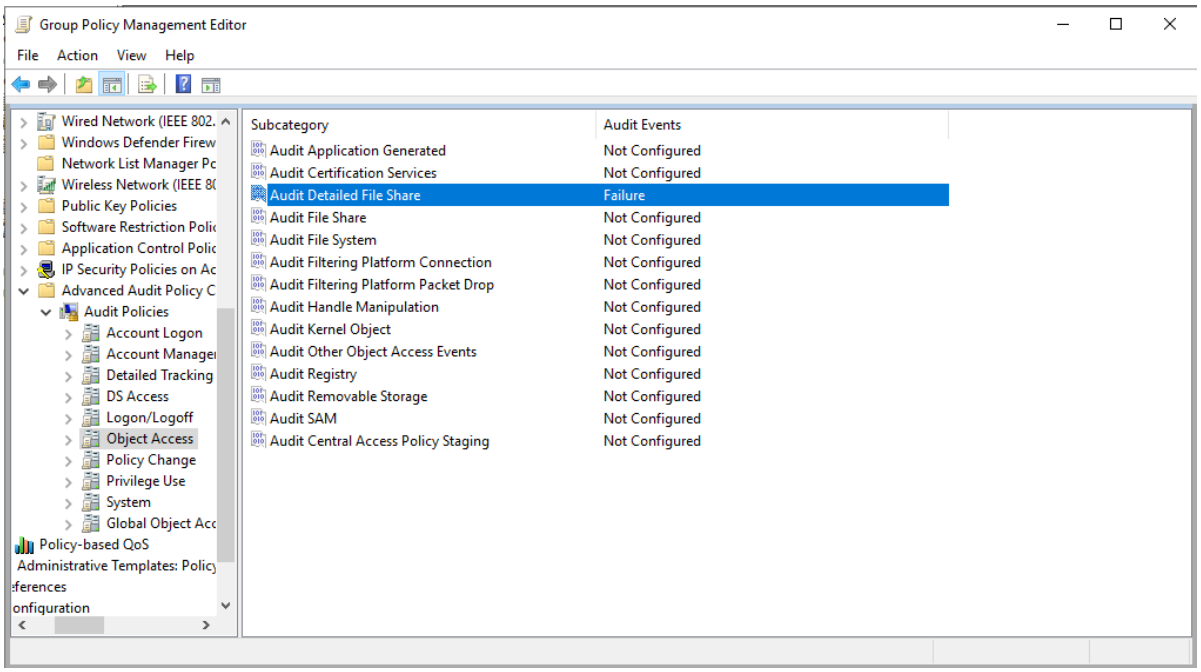


Image 148-Ensure 'Audit Detailed File Share' is set to include 'Failure'

6.6.2 Ensure 'Audit File Share' is set to 'Success and Failure'

This policy setting enables auditing of attempts to access shared folders. It is recommended to set this to: Success and Failure. Note that shared folders do not have system access control lists (SACLs); enabling this policy will audit access to all shared folders on the system. Tracking events such as deletion, creation, modification, and access of network shares is crucial in a managed enterprise environment, as it can help investigate unusual file sharing activities and potential malicious actions.

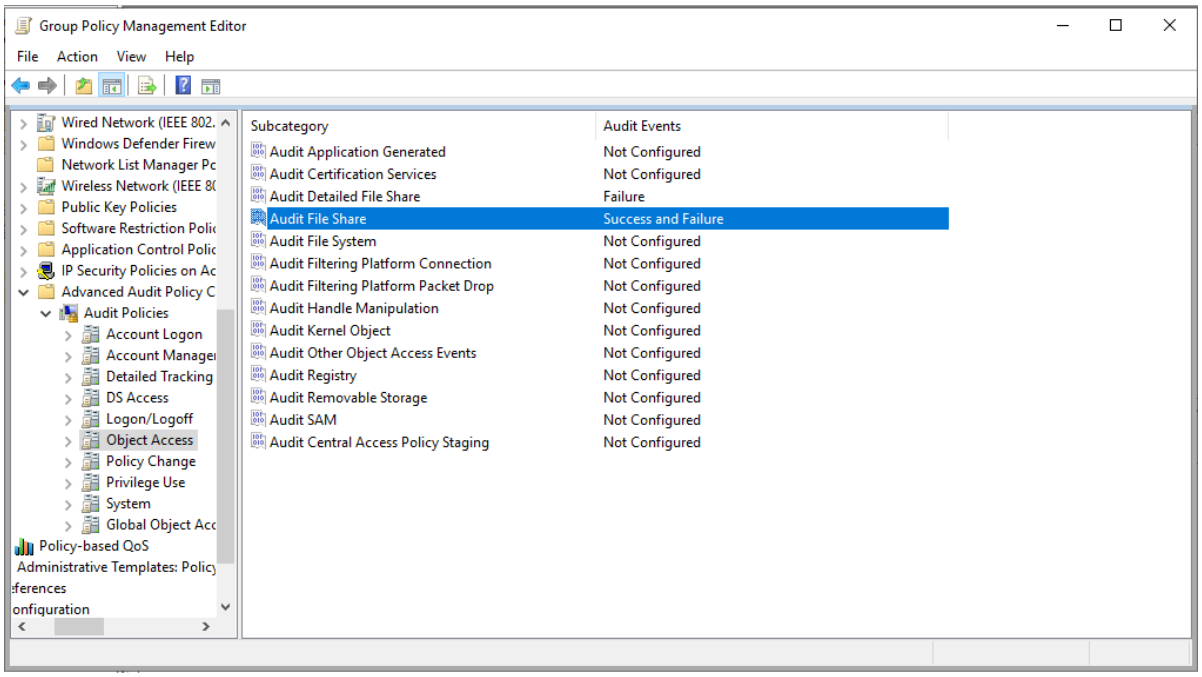


Image 149-Ensure 'Audit File Share' is set to 'Success and Failure'

6.6.3 Ensure 'Audit Other Object Access Events' is set to 'Success and Failure'

This policy setting enables auditing of events related to the management of task scheduler jobs and COM+ objects. For task scheduler jobs, the events tracked include job creation, deletion, enabling, disabling, and updates. For COM+ objects, auditing covers the addition, update, and deletion of catalog objects. The recommended setting for this policy is: Success and Failure. Monitoring these events is important as unexpected changes in scheduled tasks and COM+ objects could signal malicious activity. Although these events are typically infrequent, capturing them in audit logs can be valuable for investigations.

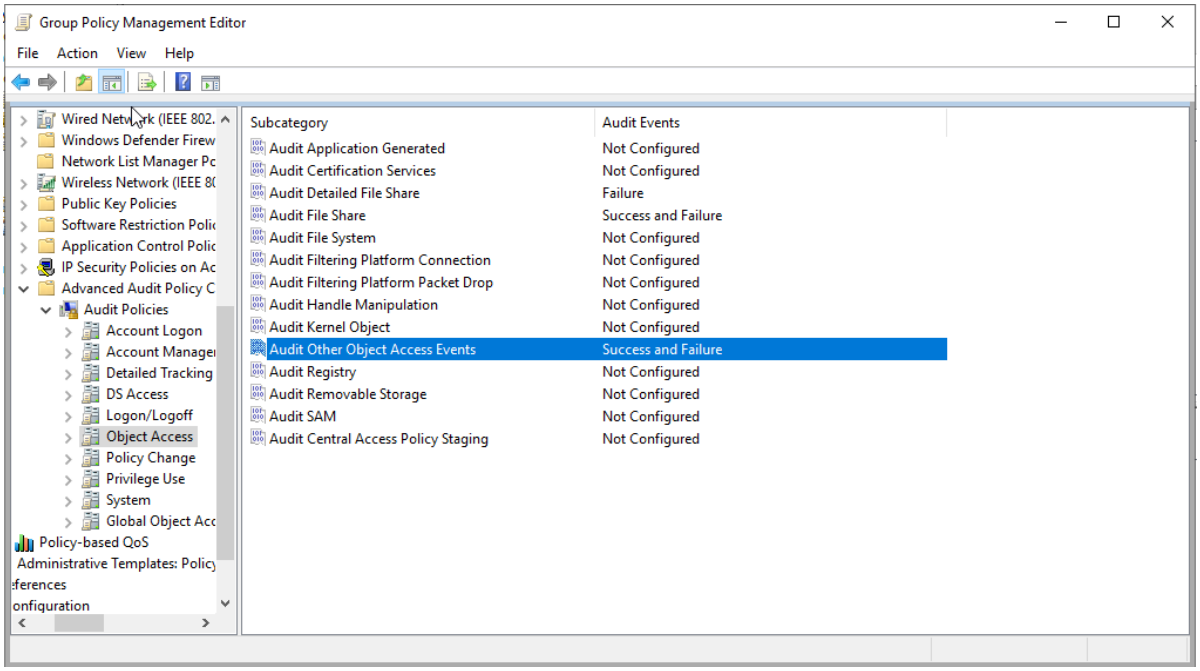


Image 150-Ensure 'Audit Other Object Access Events' is set to 'Success and Failure'

6.6.4 Ensure 'Audit Removable Storage' is set to 'Success and Failure'

This policy setting enables auditing of user attempts to access file system objects on removable storage devices. It generates security audit events for all types of access requests to these objects, with Success audits recording successful attempts and Failure audits recording unsuccessful ones. If this policy is not configured, no audit events will be generated for access to file system objects on removable storage. The recommended setting is: Success and Failure. Note that Windows 8.0, Server 2012 (non-R2), or newer is needed to configure this policy in Group Policy. Auditing removable storage can be valuable for investigating incidents, such as detecting if sensitive information has been copied to a USB drive.

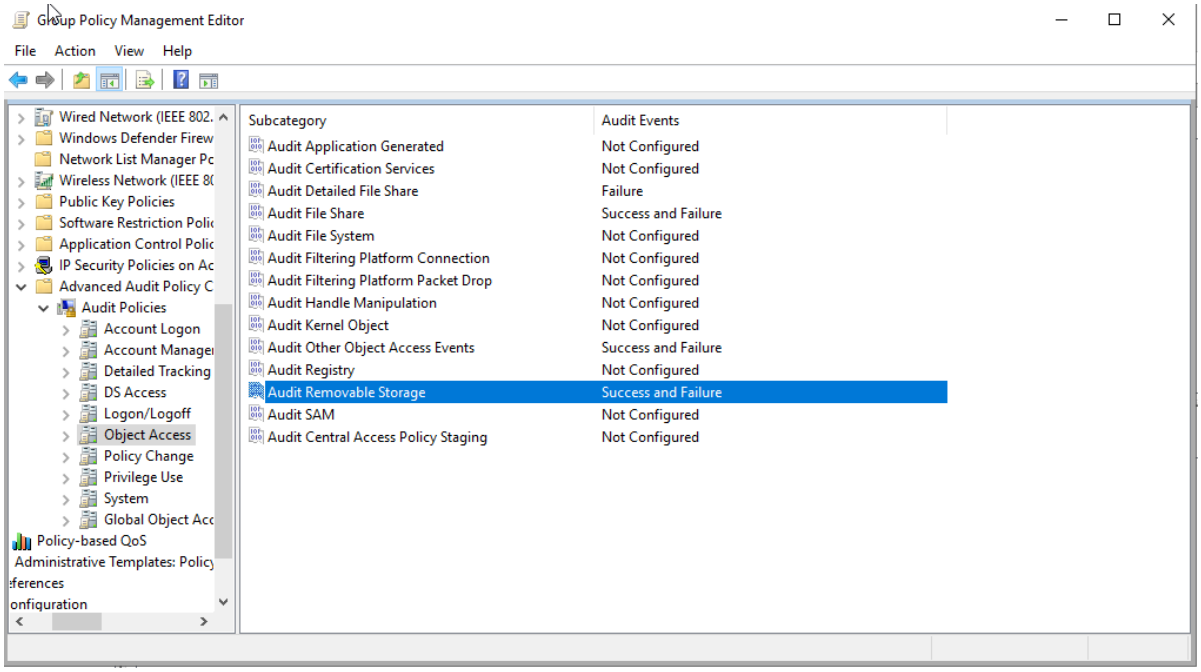


Image 151-Ensure 'Audit Removable Storage' is set to 'Success and Failure'

6.7 Policy Change

The Policy Change Group Policy tracks modifications to security policies, such as audit policies, user rights assignments, and trust policies. Enabling this policy helps administrators monitor and log changes that could affect the security configuration of the system, providing insight into who made the changes and when. This is crucial for maintaining security compliance and preventing unauthorized alterations to important settings.

6.7.1 Ensure 'Audit Audit Policy Change' is set to include 'Success'

This subcategory tracks changes to audit policies, including modifications to SACLs. The events logged under this subcategory include:

- 4715: Changes to the audit policy (SACL) on an object.
- 4719: Modifications to the system audit policy.
- 4902: Creation of the Per-user audit policy table.
- 4904: Attempt to register a security event source.
- 4905: Attempt to unregister a security event source.
- 4906: Changes to the CrashOnAuditFail setting.
- 4907: Alterations to auditing settings on objects.
- 4908: Modifications to the special Groups Logon table.
- 4912: Changes to Per User Audit Policy.

The recommended setting for this policy is to include: Success. Auditing these events can be beneficial for investigating security incidents.

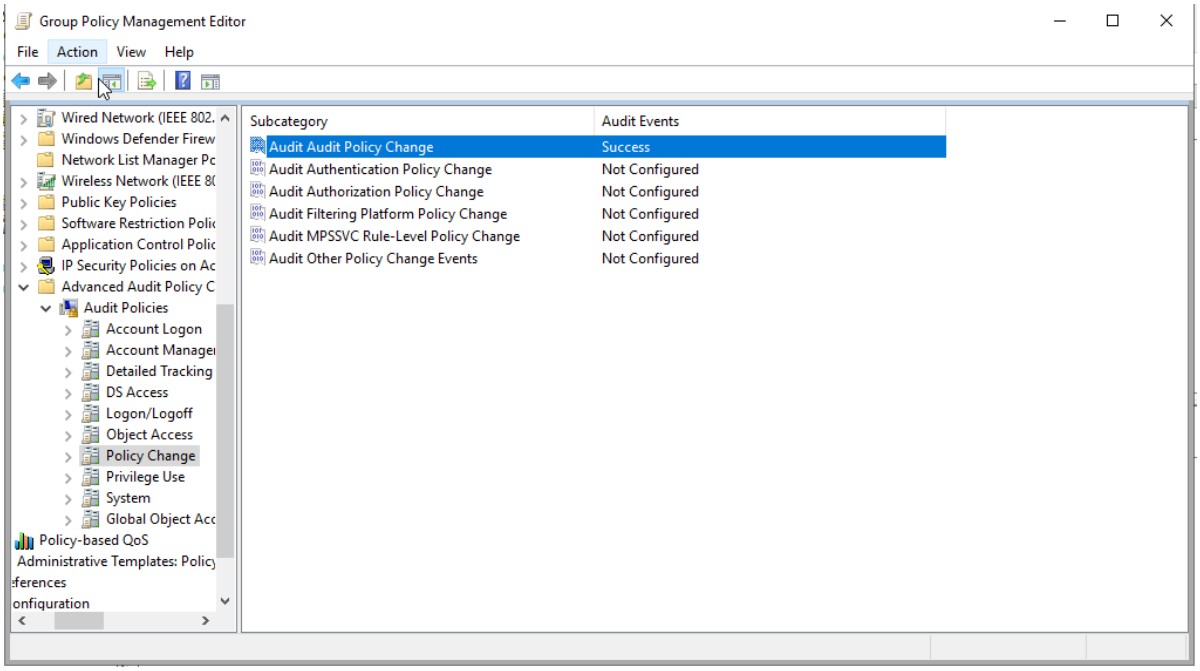


Image 152-Ensure 'Audit Audit Policy Change' is set to include 'Success'

6.7.2 Ensure 'Audit Authentication Policy Change' is set to include 'Success'

This subcategory tracks changes in authentication policies. The events included in this subcategory are:

- 4706: Creation of a new domain trust.
- 4707: Removal of a domain trust.
- 4713: Changes to Kerberos policy.
- 4716: Modification of trusted domain information.
- 4717: Granting system security access to an account.
- 4718: Removal of system security access from an account.
- 4739: Alterations to Domain Policy.
- 4864: Detection of a namespace collision.
- 4865: Addition of a trusted forest information entry.
- 4866: Removal of a trusted forest information entry.
- 4867: Modification of a trusted forest information entry.

The recommended setting for this policy is to include: Success. Monitoring these events can be crucial for investigating security incidents.

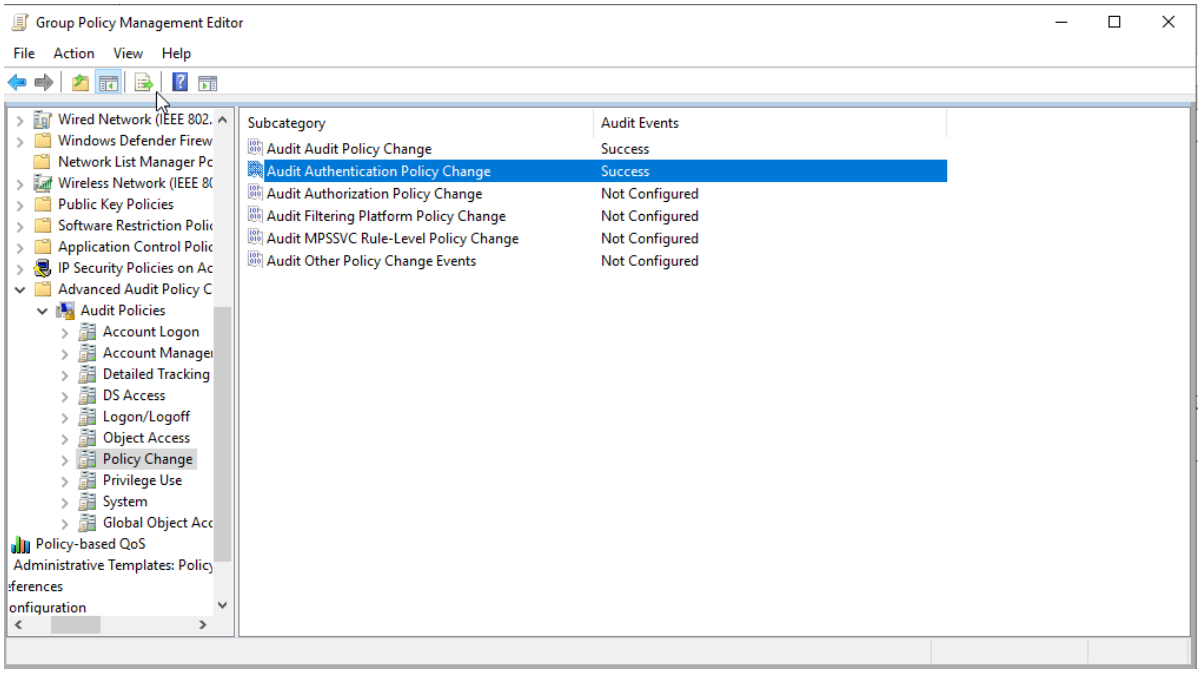


Image 153-Ensure 'Audit Authentication Policy Change' is set to include 'Success'

6.7.3 Ensure 'Audit Authorization Policy Change' is set to include 'Success'

This subcategory tracks changes in authorization policies. It includes events such as:

• 4703: Adjustment of a user right.

• 4704: Assignment of a user right.

• 4705: Removal of a user right.

• 4670: Modification of permissions on an object.

• 4911: Changes to resource attributes of an object.

• 4913: Alteration of Central Access Policy on an object.

The recommended setting for this policy is to include: Success. Monitoring these events can be valuable for investigating security incidents.

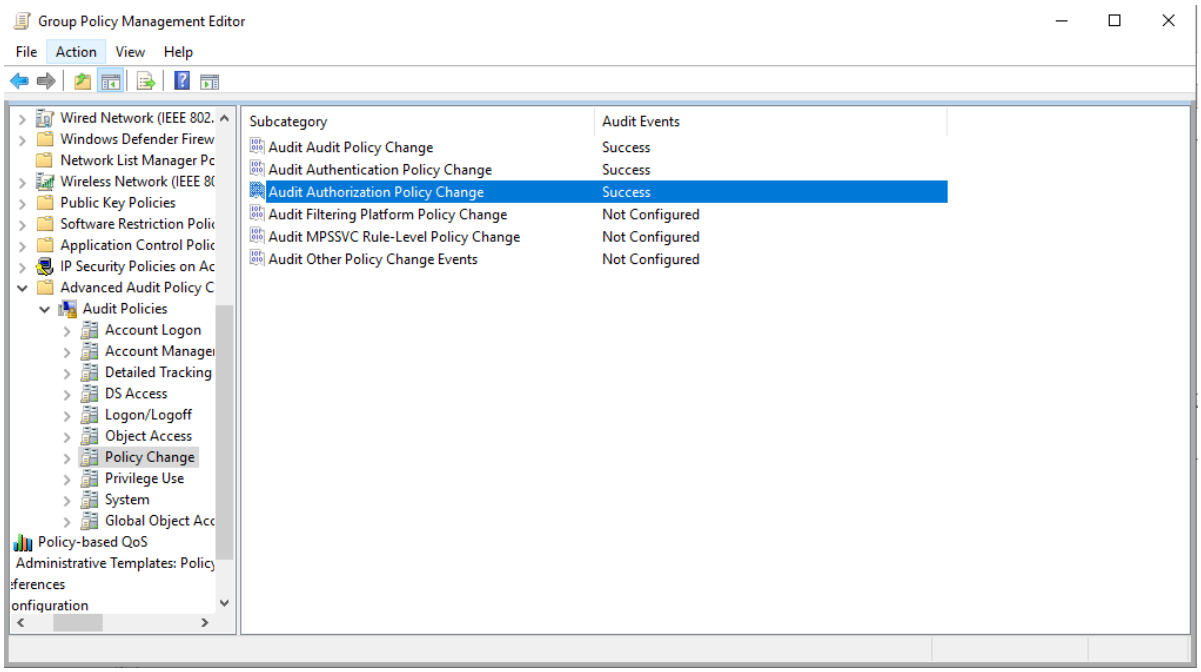


Image 154-Ensure 'Audit Authorization Policy Change' is set to include 'Success'

6.7.4 Ensure 'Audit MPSSVC Rule-Level Policy Change' is set to 'Success and Failure'

This subcategory tracks audit events related to changes in Microsoft Protection Service (MPSSVC.exe) policy rules. It covers:

- 4944: Active policy at Windows Firewall startup.
- 4945: Listed rule at Windows Firewall startup.
- 4946: Added rule to the exception list.
- 4947: Modified rule in the exception list.
- 4948: Deleted rule from the exception list.
- 4949: Restored default Windows Firewall settings.
- 4950: Changed Windows Firewall settings.
- 4951: Ignored rule due to unrecognized major version.
- 4952: Ignored rule parts due to unrecognized minor version.
- 4953: Ignored rule due to parsing issues.
- 4954: Applied new Group Policy settings.
- 4956: Changed active Windows Firewall profile.
- 4957: Unapplied rule.
- 4958: Rule ignored due to unconfigured items.

The recommended setting is to include both Success and Failure.

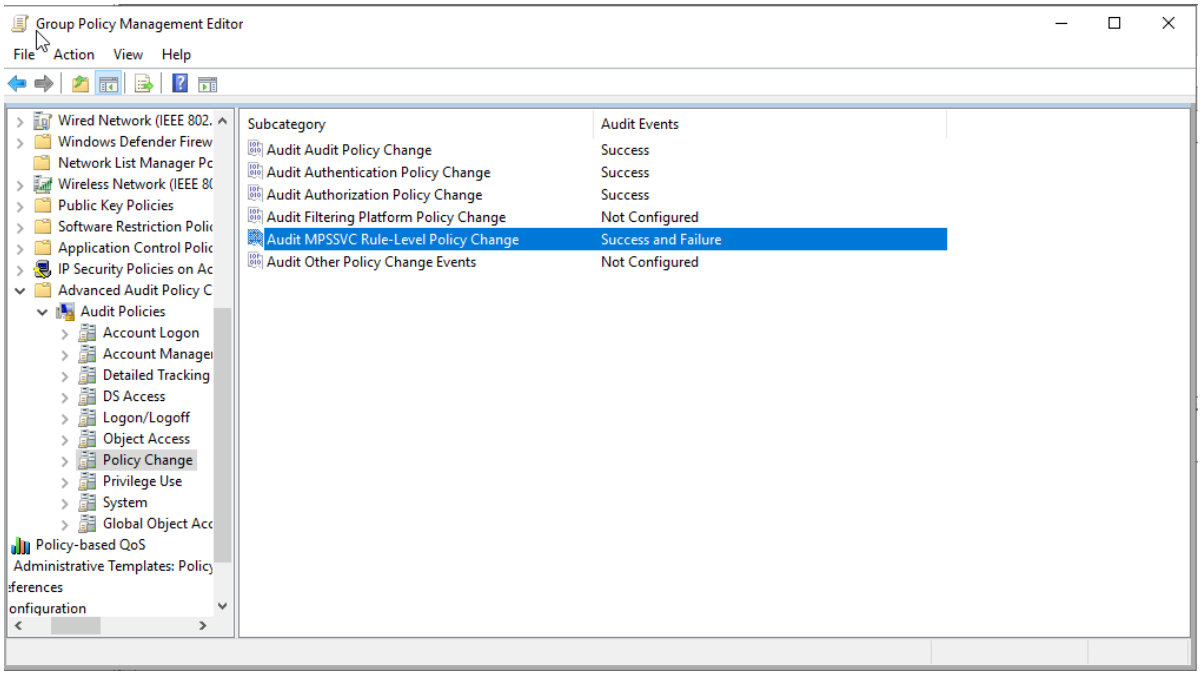


Image 155-Ensure 'Audit MPSSVC Rule-Level Policy Change' is set to 'Success and Failure'

6.7.5 Ensure 'Audit Other Policy Change Events' is set to include 'Failure'

This subcategory logs events related to various security policy changes and troubleshooting, including EFS Data Recovery Agent policy updates, Windows Filtering Platform filter changes, Security policy updates for local Group Policy settings, and Central Access Policy modifications. It also tracks detailed issues with Cryptographic Next Generation (CNG) operations. Events include:

• 5063: Attempted cryptographic provider operation.

• 5064: Attempted cryptographic context operation.

• 5065: Attempted modification of a cryptographic context.

• 5066: Attempted cryptographic function operation.

• 5067: Attempted modification of a cryptographic function.

• 5068: Attempted cryptographic function provider operation.

• 5069: Attempted cryptographic function property operation.

• 5070: Attempted modification of a cryptographic function property.

• 6145: Errors occurred processing security policy in group policy objects.

The recommended setting is to include Failure. This helps in detecting errors in Security settings applied through Group Policy and issues related to CNG functions.

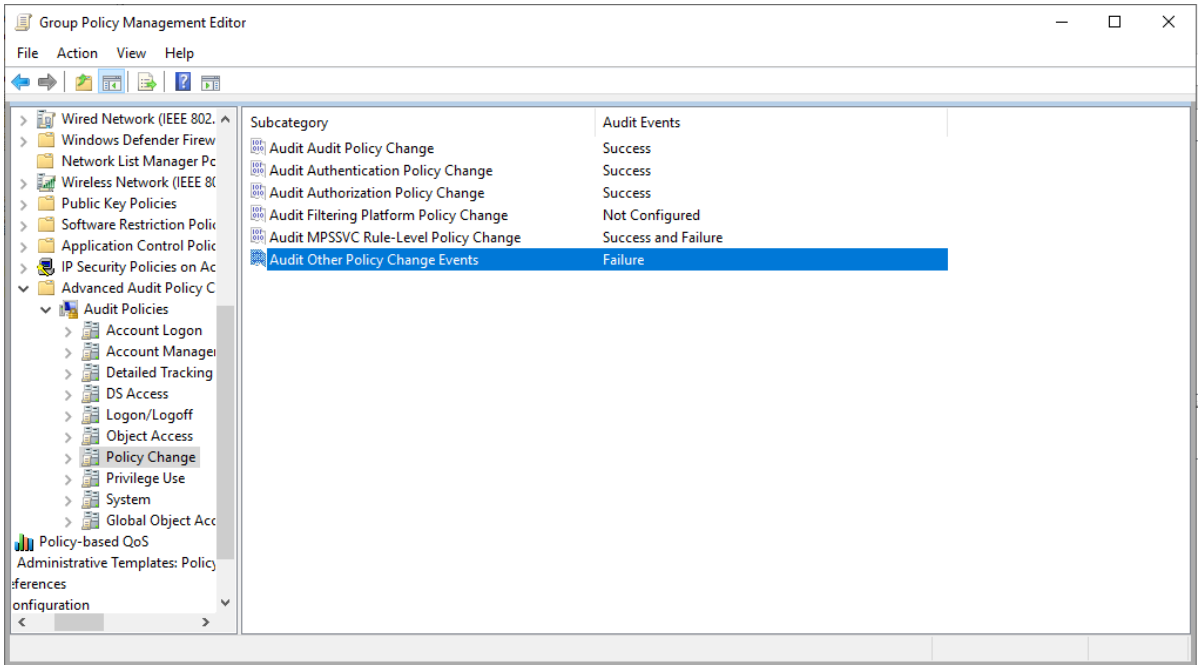


Image 156-Ensure 'Audit Other Policy Change Events' is set to include 'Failure'

6.8 Policy Change

The Policy Change Group Policy logs changes made to security policies, such as audit policies, user rights, and other critical system settings. Enabling this policy ensures that any modifications are recorded, helping administrators track who made the changes and when. This monitoring is essential for maintaining system security and compliance, and for identifying any unauthorized alterations to security configurations.

6.8.1 Ensure 'Audit Sensitive Privilege Use' is set to 'Success and Failure'

This subcategory tracks when a user account or service uses sensitive .

The recommended state is to include both Success and Failure. Auditing these events helps in investigating security incidents.

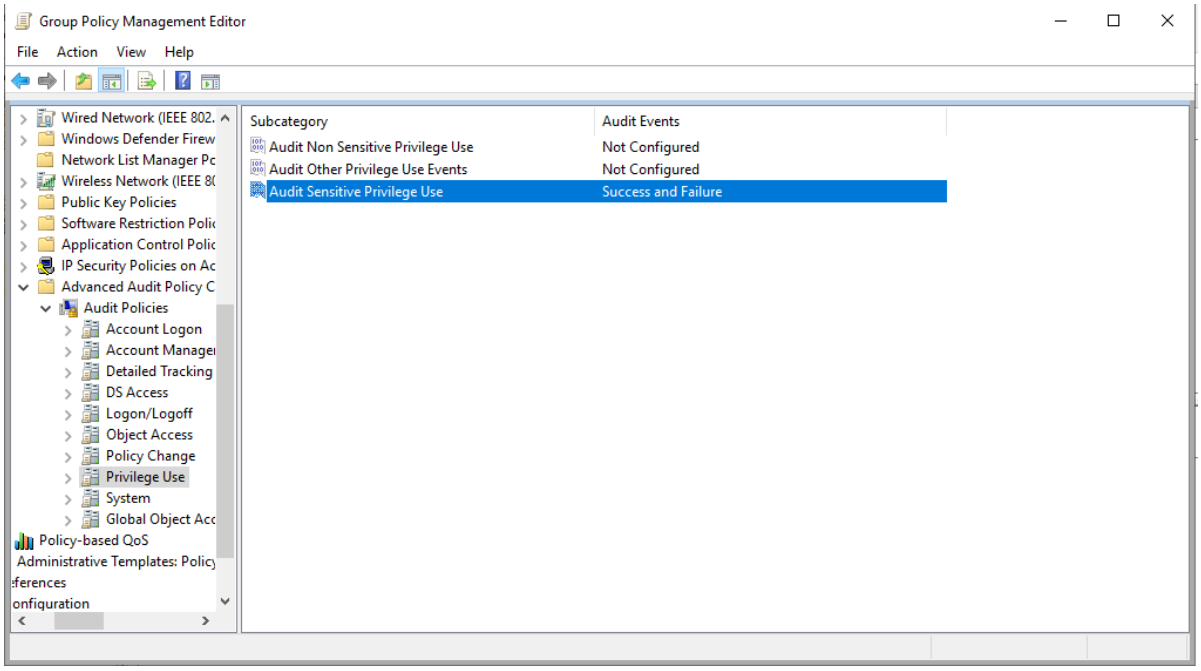


Image 157-Ensure 'Audit Sensitive Privilege Use' is set to 'Success and Failure'

6.9 System

The System Group Policy manages settings related to system events and configurations, such as startup and shutdown processes, system errors, and system time changes. Enabling this policy allows for detailed logging of system-related activities, which aids in troubleshooting and maintaining system stability. This ensures that all critical system events are tracked, providing valuable information for diagnosing issues and ensuring proper system operation.

6.9.1 Ensure 'Audit IPsec Driver' is set to 'Success and Failure'

This subcategory tracks activities related to the Internet Protocol security (IPsec) driver. The recommended setting is to include both Success and Failure events to aid in investigating security incidents.

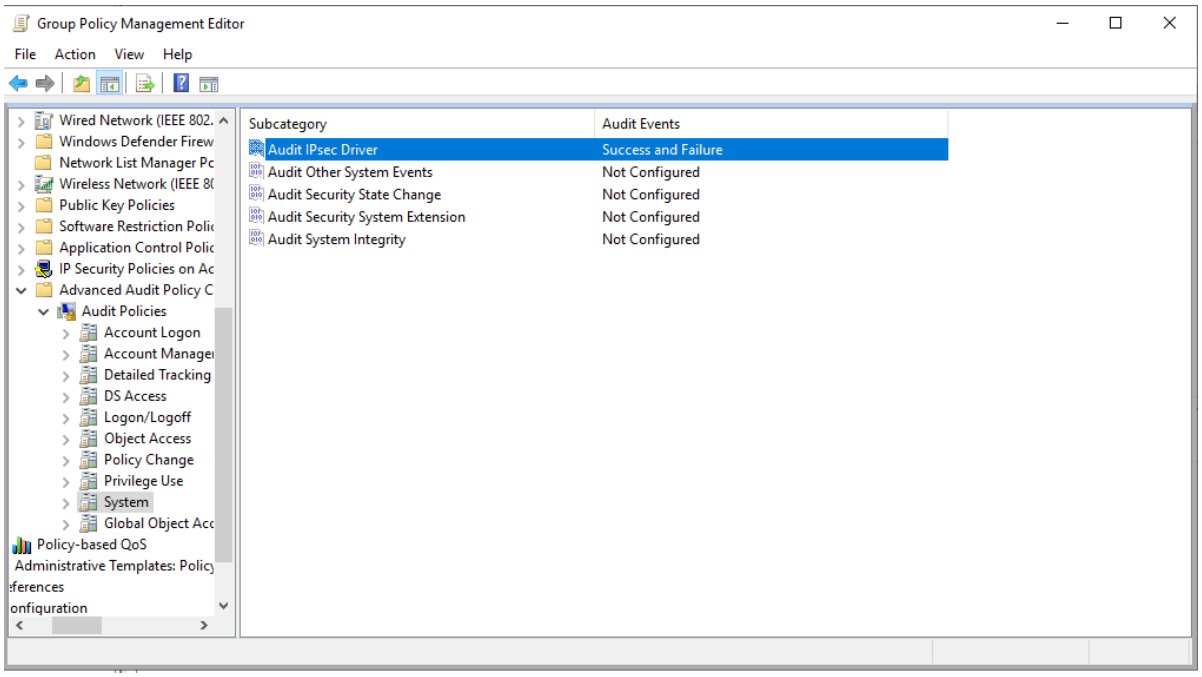


Image 158-Ensure 'Audit IPsec Driver' is set to 'Success and Failure'

6.9.2 Ensure 'Audit Other System Events' is set to 'Success and Failure'

This subcategory covers various system events related to the Windows Firewall and key operations, including:

- **5024**: Windows Firewall Service started successfully.
- **5025**: Windows Firewall Service stopped.
- **5027**: Windows Firewall Service couldn't retrieve the security policy from local storage but will continue with the current policy.
- **5028**: Windows Firewall Service couldn't parse the new security policy and will continue with the current one.
- **5029**: Windows Firewall Service failed to initialize the driver but will maintain the current policy.
- **5030**: Windows Firewall Service failed to start.
- **5032**: Windows Firewall couldn't notify the user about blocking an application from network connections.
- **5033**: Windows Firewall Driver started successfully.
- **5034**: Windows Firewall Driver stopped.
- **5035**: Windows Firewall Driver failed to start.
- **5037**: Windows Firewall Driver encountered a critical runtime error and is terminating.
- **5058**: Key file operation.
- **5059**: Key migration operation.

The recommended setting is to include both Success and Failure events. This helps in detecting issues with the Windows Firewall's performance.

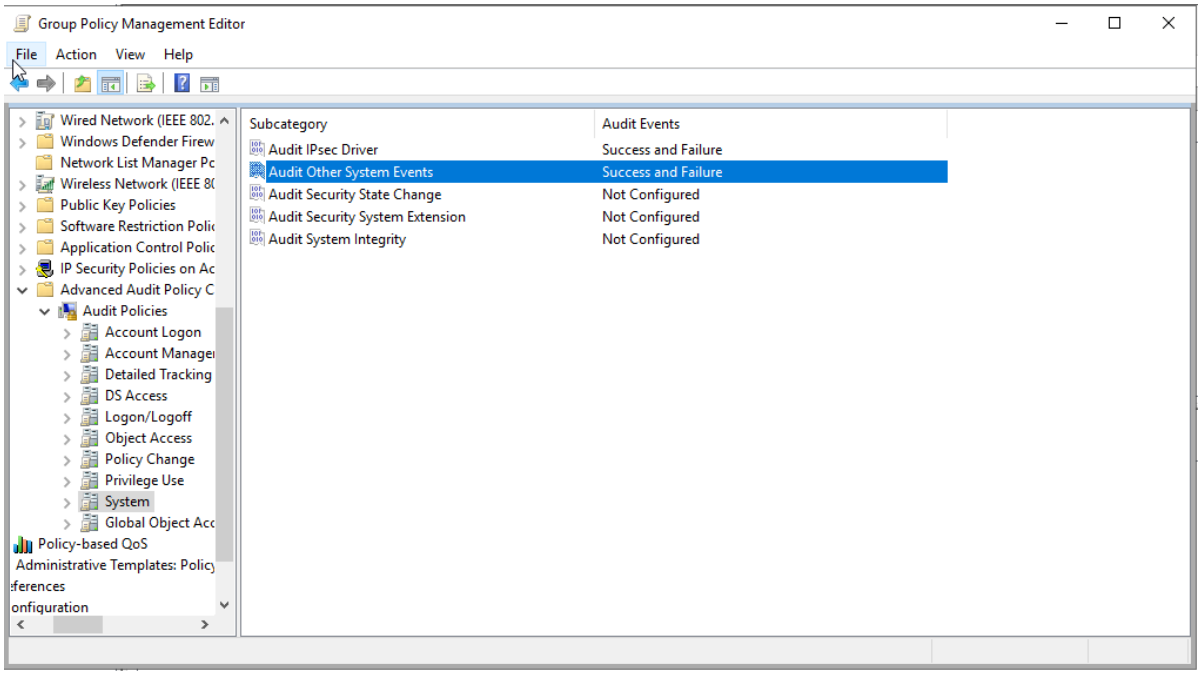


Image 159-Ensure 'Audit Other System Events' is set to 'Success and Failure'

6.9.3 Ensure 'Audit Security State Change' is set to include 'Success'

This subcategory tracks changes in the system's security state, such as when the security subsystem starts or stops. Key events include:

- **4608**: Windows startup.
- **4609**: Windows shutdown.
- **4616**: System time change.
- **4621**: System recovery from CrashOnAuditFail, allowing non-administrator logons and possibly missing some audit records.

It is recommended to include Success for this setting. Auditing these events can be helpful in investigating security incidents.

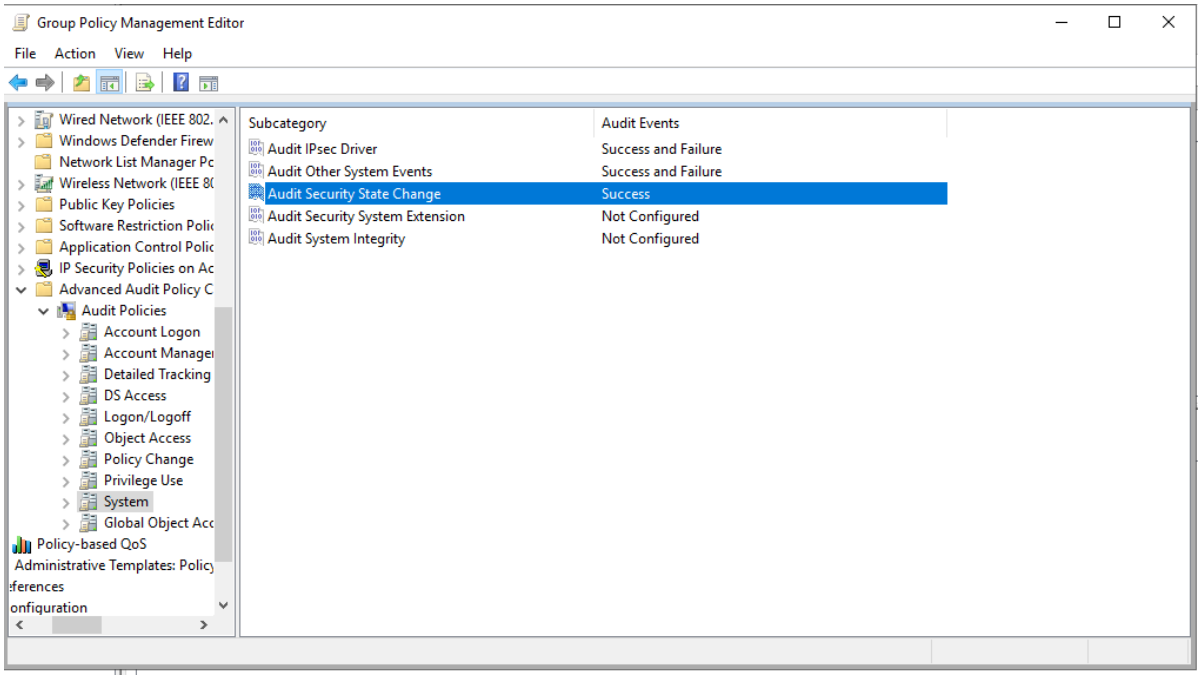


Image 160-Ensure 'Audit Security State Change' is set to include 'Success'

6.9.4 Ensure 'Audit Security System Extension' is set to include 'Success'

This subcategory monitors the loading of extension code, such as authentication packages, by the security subsystem. Key events include:

- **4610**: Authentication package loaded by the Local Security Authority.
- **4611**: Trusted logon process registered with the Local Security Authority.
- **4614**: Notification package loaded by the Security Account Manager.
- **4622**: Security package loaded by the Local Security Authority.
- **4697**: Service installed on the system.

It is recommended to set this to include Success. Auditing these events can be valuable for investigating security incidents.

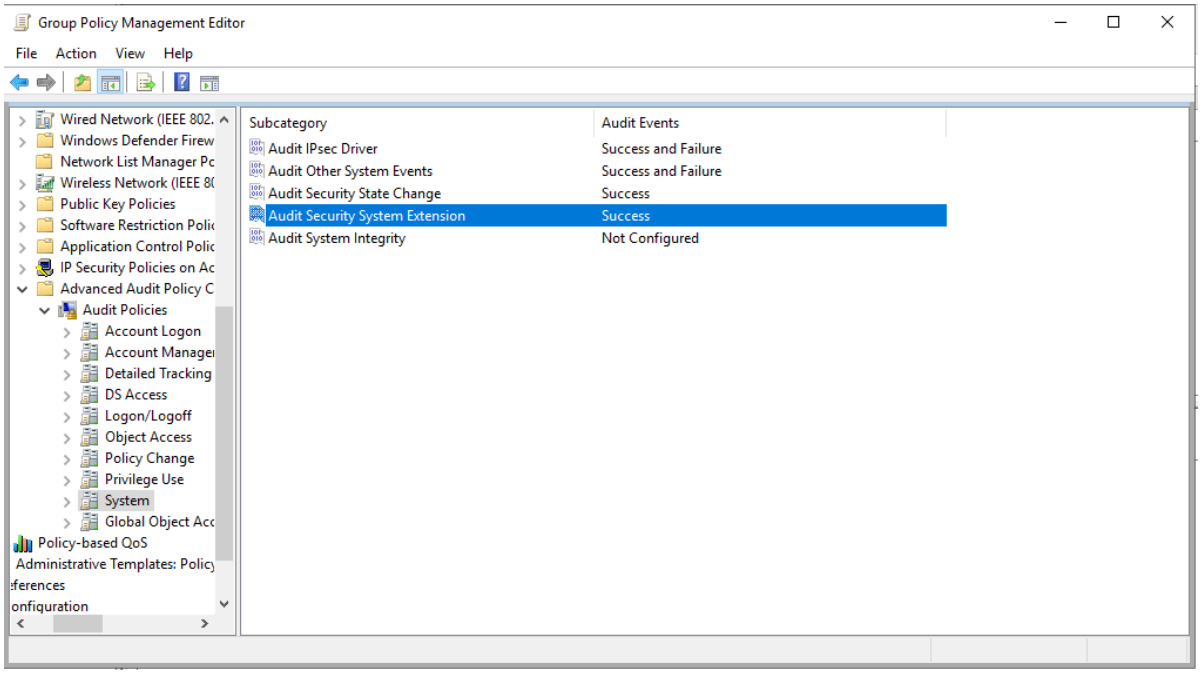


Image 161-Ensure 'Audit Security System Extension' is set to include 'Success'

6.9.5 Ensure 'Audit System Integrity' is set to 'Success and Failure'

This subcategory tracks breaches in the security subsystem's integrity. Notable events include:

- **4612**: Exhaustion of internal resources for queuing audit messages, resulting in lost audits.
- **4615**: Invalid use of LPC port.
- **4618**: Occurrence of a monitored security event pattern.
- **4816**: RPC detected an integrity issue while decrypting an incoming message.
- **5038**: Code integrity found an invalid image hash, possibly due to unauthorized modifications or disk errors.
- **5056**: Cryptographic self-test performed.
- **5057**: Failure in a cryptographic primitive operation.
- **5060**: Verification operation failed.
- **5061**: Cryptographic operation performed.
- **5062**: Kernel-mode cryptographic self-test conducted.

The recommended state for this setting is to include both Success and Failure. Auditing these events is important for investigating security incidents.

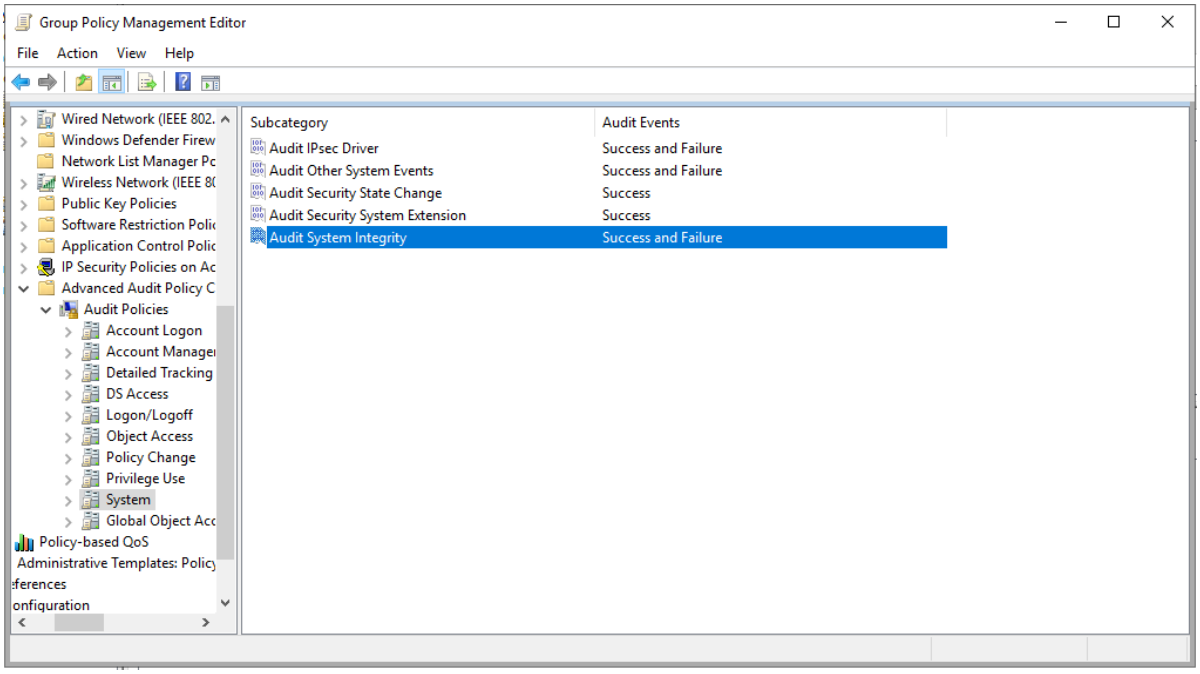


Image 162-Ensure 'Audit System Integrity' is set to 'Success and Failure'

7 Administrative Templates

Administrative Templates for Windows are a feature within Group Policy that allow administrators to manage registry-based policies. They provide a structured and simplified way to configure settings for both computer and user configurations. By using predefined templates, administrators can enforce specific configurations across multiple machines, ensuring consistency and compliance with organizational policies. These templates cover a wide range of settings, from system security to user interface customizations, making them a crucial tool for centralized management in a Windows environment.

7.1 Control Panel

The Control Panel Group Policy manages access to and functionality within the Windows Control Panel. It allows administrators to control which Control Panel applets and settings are available to users, enhancing security and preventing unauthorized changes to system configurations. By configuring this policy, administrators can streamline user access to necessary settings while restricting access to sensitive or potentially disruptive system controls.

7.1.1 Personalization

7.1.1.1 Ensure 'Prevent enabling lock screen camera' is set to 'Enabled'

This setting disables the lock screen camera toggle in PC Settings, preventing the camera from being activated on the lock screen. The recommended state is: Enabled. Disabling the lock screen camera enhances the security provided by the lock screen by restricting camera access.

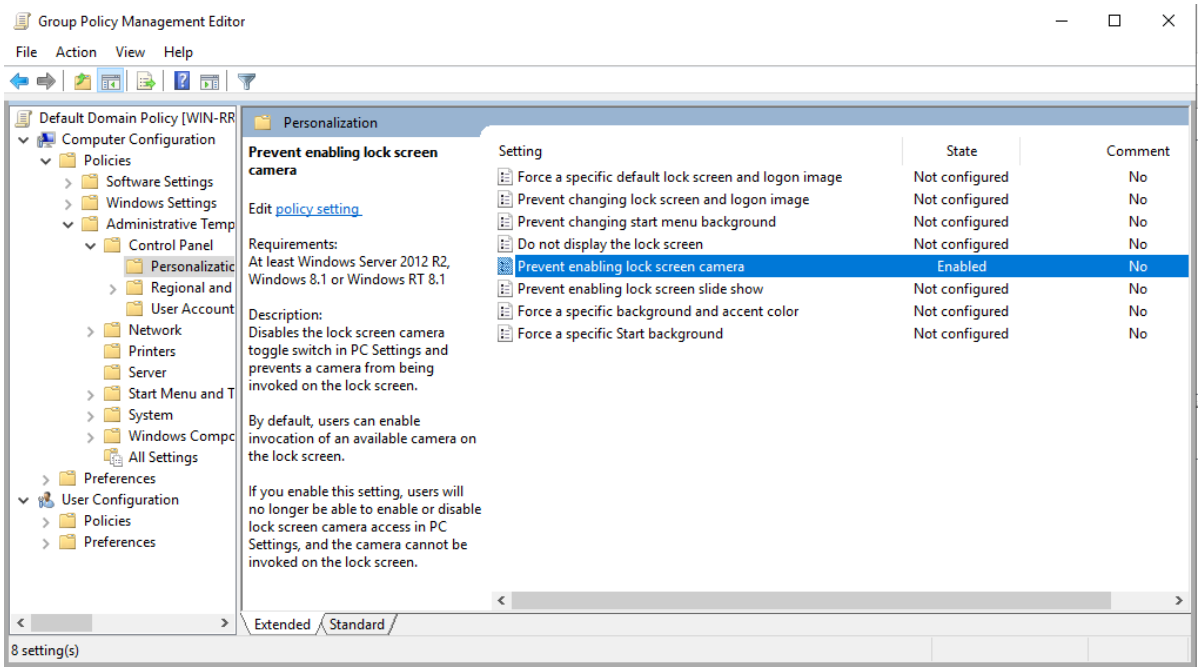


Image 163-Ensure 'Prevent enabling lock screen camera' is set to 'Enabled'

7.1.1.2 Ensure 'Prevent enabling lock screen slide show' is set to 'Enabled'

This setting disables the lock screen slide show in PC Settings, preventing a slide show from playing on the lock screen. The recommended state is: Enabled. Disabling the lock screen slide show enhances security by protecting the contents displayed during the slide show.

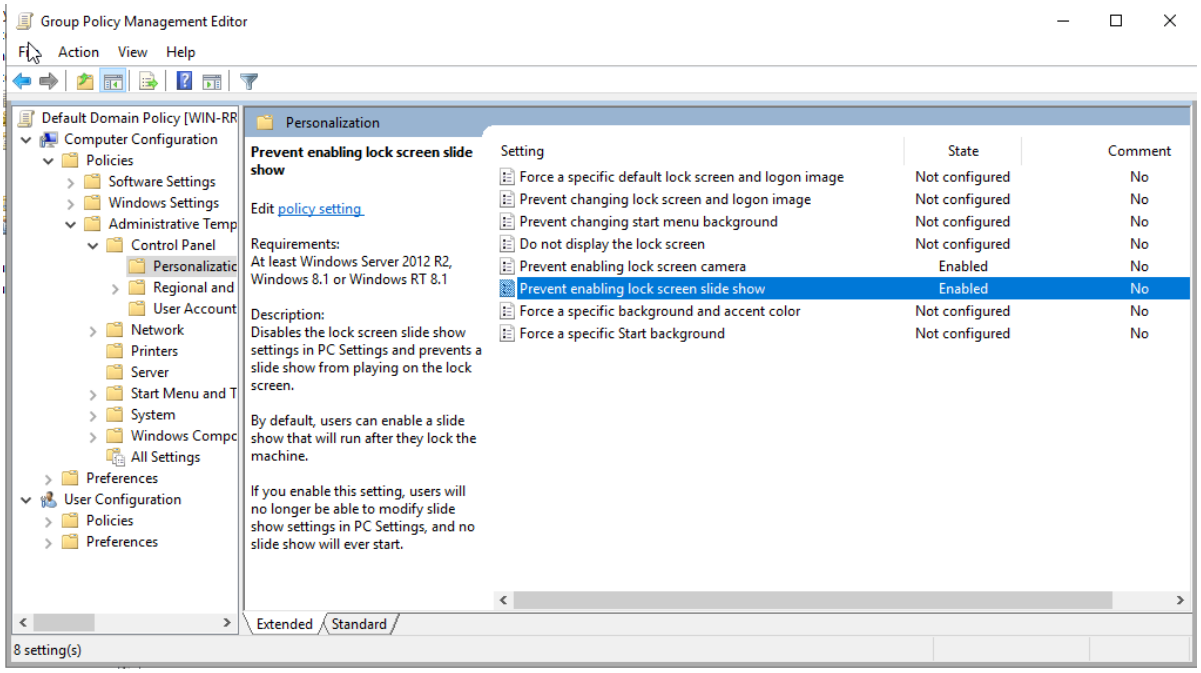


Image 164-Ensure 'Prevent enabling lock screen slide show' is set to 'Enabled'

7.1.2 Regional and Language Options

7.1.2.1 Ensure 'Allow users to enable online speech recognition services' is set to 'Disabled'

This policy enables automatic learning for input personalization, including speech, inking, and typing, by collecting speech and handwriting patterns, typing history, contacts, and recent calendar information. This data is necessary for Cortana and may be stored on the user's OneDrive or uploaded to Microsoft for speech personalization. The recommended state for this setting is: Disabled. Enabling this setting could result in sensitive information being stored in the cloud or sent to Microsoft.

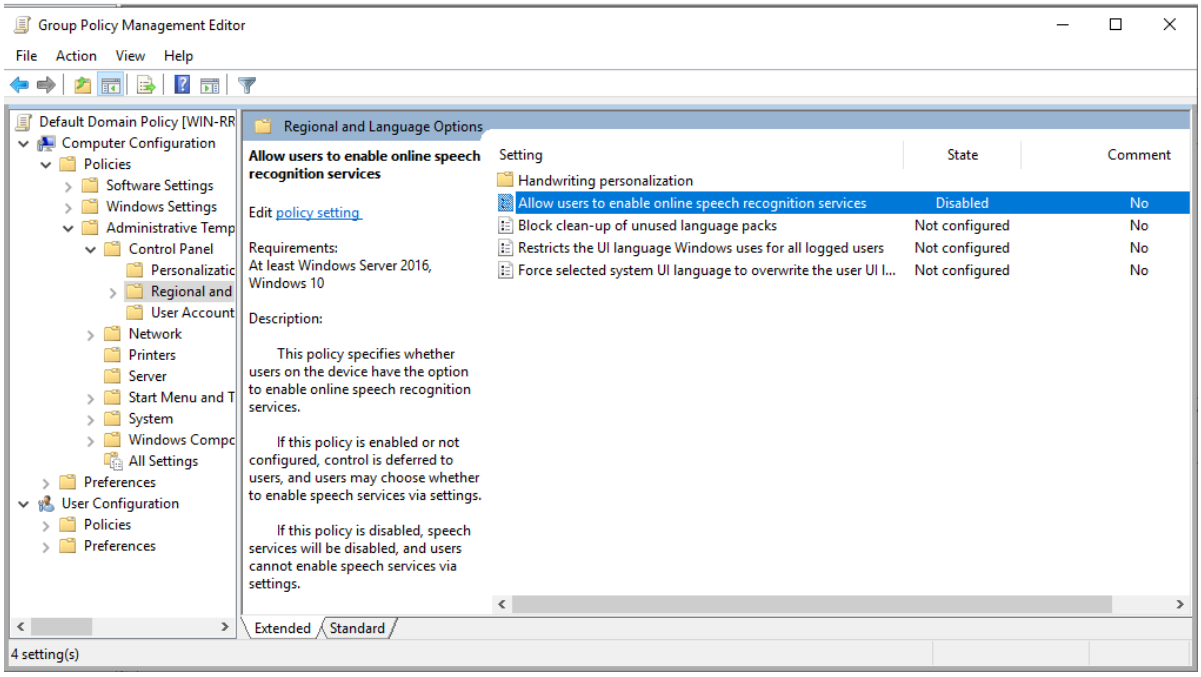


Image 165-Ensure 'Allow users to enable online speech recognition services' is set to 'Disabled'

7.1.3 Ensure 'Allow Online Tips' is set to 'Disabled'

This policy setting controls the retrieval of online tips and help for the Settings app. The recommended state for this setting is: Disabled. Data should not be sent to any third-party due to privacy concerns, as it could contain sensitive information.

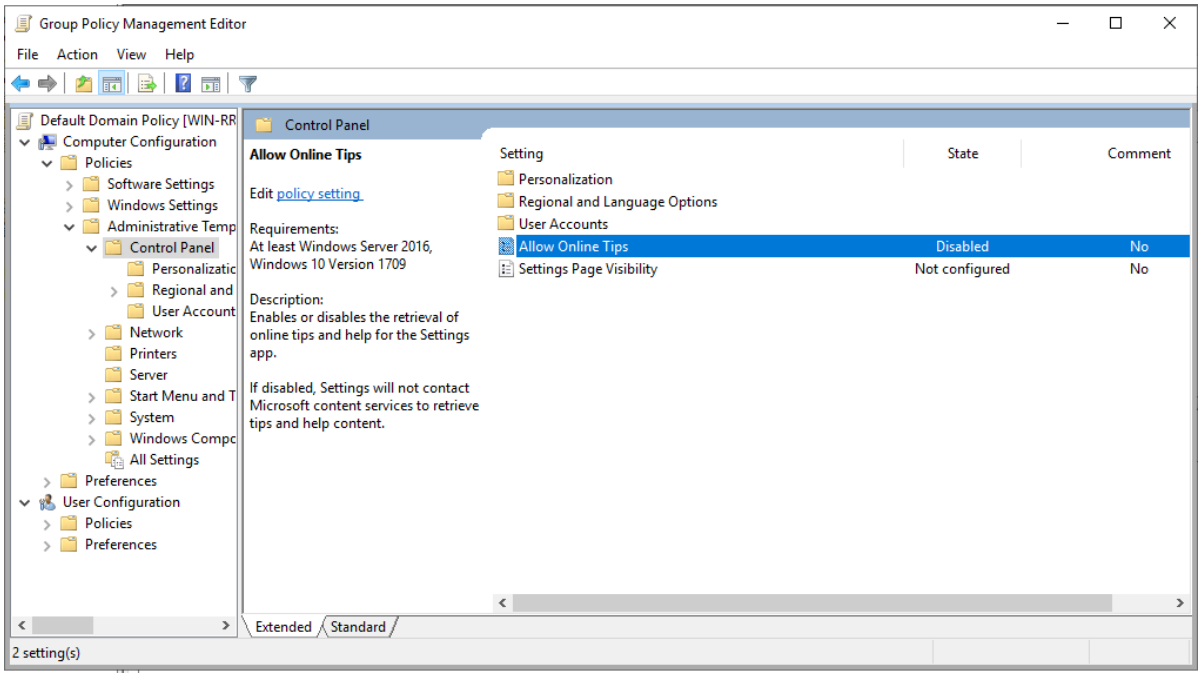


Image 166-Ensure 'Allow Online Tips' is set to 'Disabled'

7.2 MS Security Guide

The MS Security Guide Group Policy settings provide a framework for applying Microsoft's security recommendations to Windows environments. These settings help ensure that security best practices are followed, such as enforcing password policies, controlling user rights, and managing audit settings. By implementing the MS Security Guide policies, organizations can strengthen their security posture, reduce vulnerabilities, and maintain compliance with industry standards.

7.2.1 Ensure 'Configure SMB v1 client driver' is set to 'Enabled: Disable driver (recommended)'

This setting configures the start type for the SMBv1 client driver service (MRxSmb10) and should be disabled. The recommended state for this setting is: Enabled: Disable driver (recommended). Never configure this setting as Disabled, as it will delete the underlying registry entry and cause serious problems. Microsoft has recommended disabling SMBv1 since September 2016 due to its vulnerability to attacks compared to newer designs like SMBv2 and SMBv3.

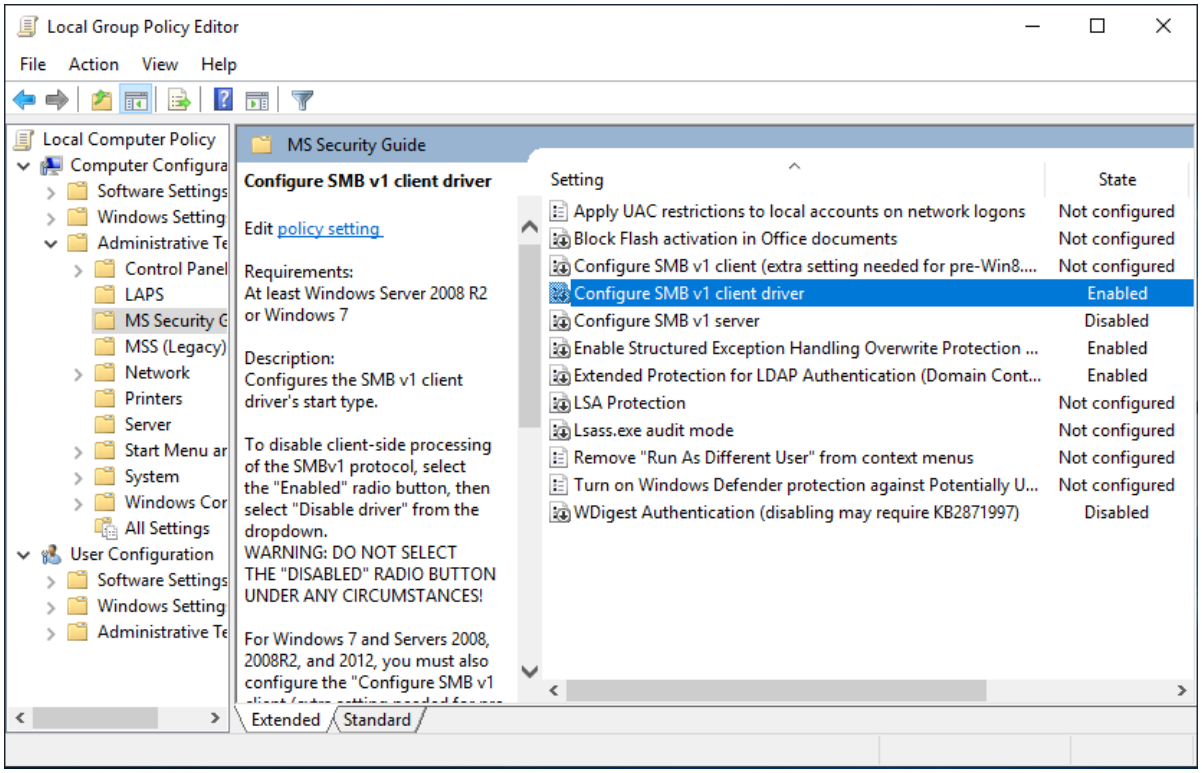


Image 167-Ensure 'Configure SMB v1 client driver' is set to 'Enabled: Disable driver (recommended)'

7.2.2 Ensure 'Configure SMB v1 server' is set to 'Disabled'

This setting configures the server-side processing of the SMBv1 protocol. The recommended state for this setting is: Disabled. Microsoft has advised disabling SMBv1 since September 2016 due to its increased vulnerability to attacks compared to the newer SMBv2 and SMBv3 protocols.

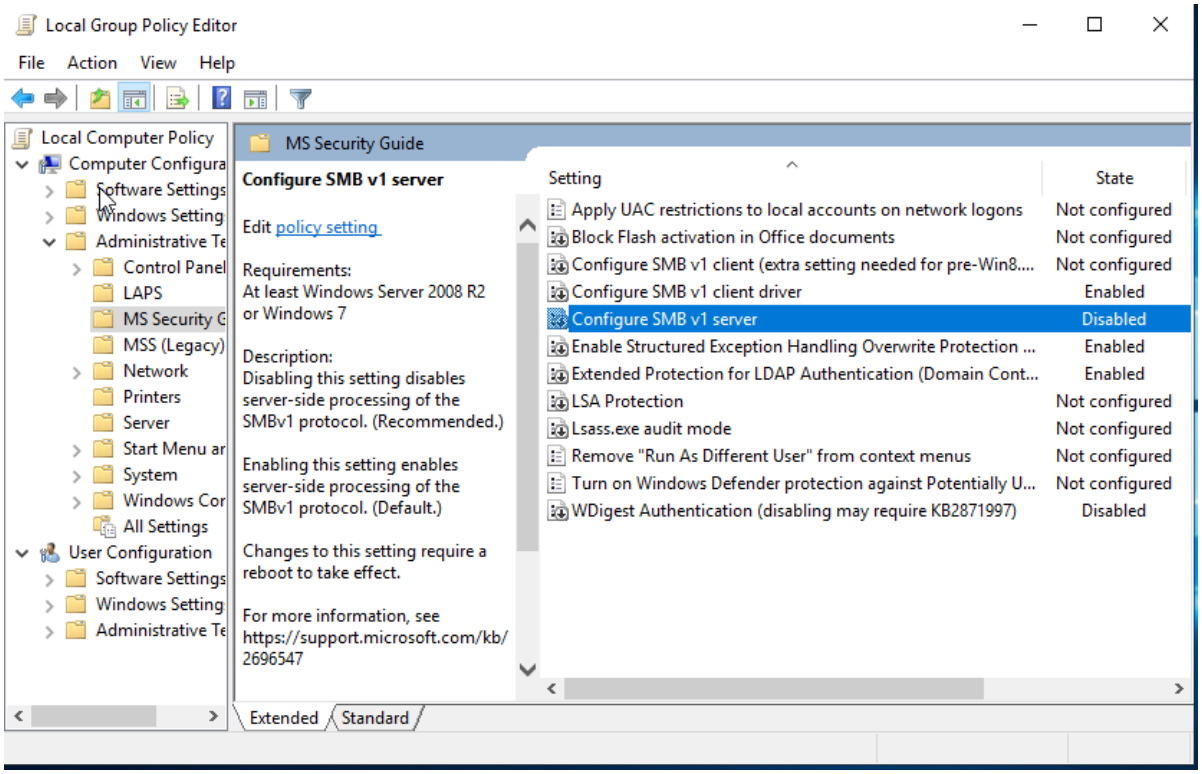


Image 168-Ensure 'Configure SMB v1 server' is set to 'Disabled'

7.2.3 Ensure 'Enable Structured Exception Handling Overwrite Protection (SEHOP)' is set to 'Enabled'

Windows includes support for Structured Exception Handling Overwrite Protection (SEHOP), which is recommended to be enabled to enhance the computer's security. This feature blocks exploits that use the SEH overwrite technique, offering run-time protection for applications even if they haven't been compiled with the latest improvements, such as the /SAFESEH option. The recommended state for this setting is: Enabled.

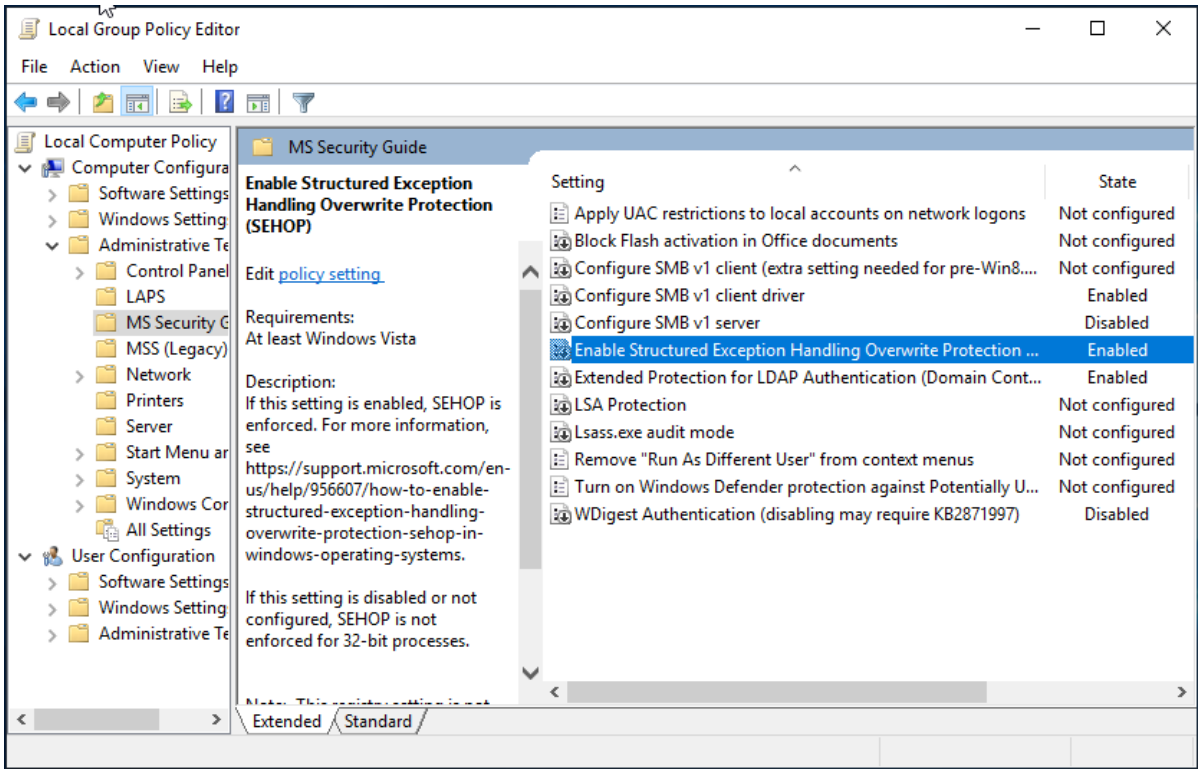


Image 169-Ensure 'Enable Structured Exception Handling Overwrite Protection (SEHOP)' is set to 'Enabled'

7.2.4 Ensure 'LSA Protection' is set to 'Enabled'

This policy setting determines whether the Local Security Authority Server Service (LSASS) process operates in a protected mode. LSASS, part of the Local Security Authority (LSA), handles user authentication for both local and remote sign-ins and enforces local security policies. The recommended state for this setting is: Enabled. Note that this applies to Windows Server 2012 R2 and newer versions, excluding Windows Server 2022 and later. Enabling this setting enhances security by preventing unauthorized processes from accessing LSASS memory and performing code injection, thereby protecting the credentials managed by LSASS.

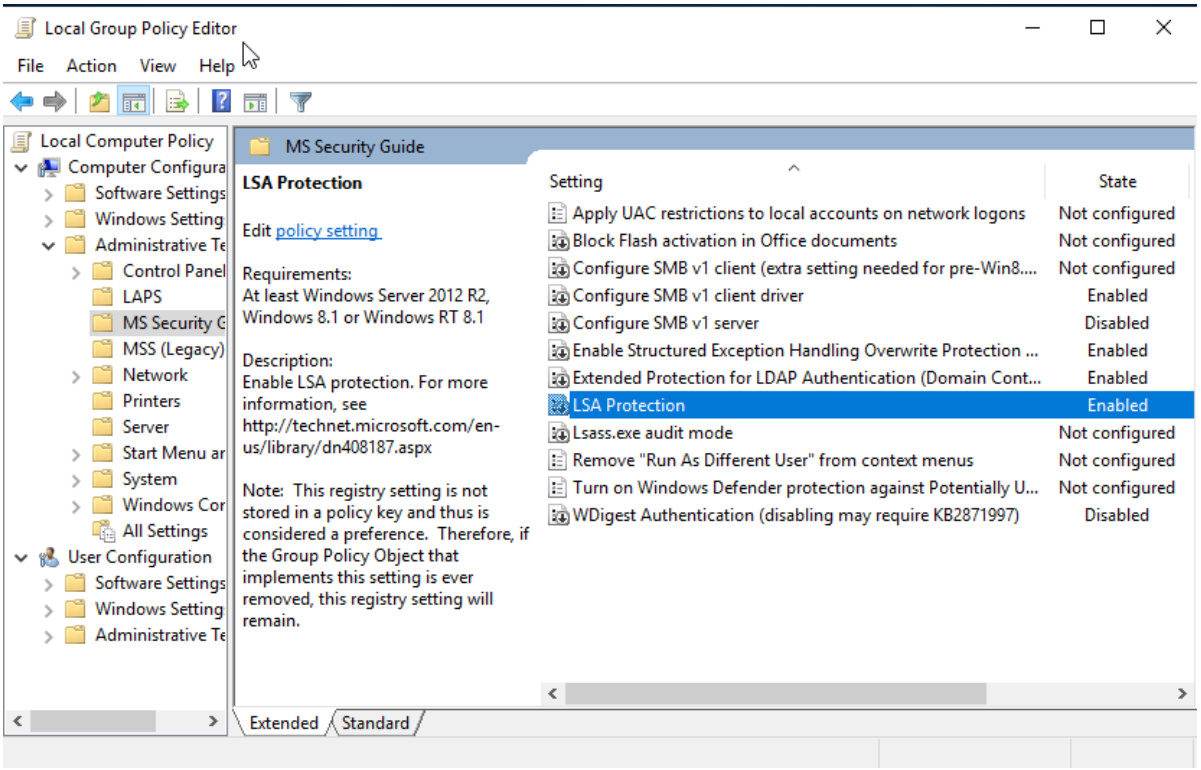


Image 170-Ensure 'LSA Protection' is set to 'Enabled'

7.2.5 Ensure 'WDigest Authentication' is set to 'Disabled'

When WDigest authentication is enabled, Lsass.exe retains a plaintext copy of the user's password in memory, making it vulnerable to theft. By default, WDigest authentication is disabled in Windows 8.1 and Windows Server 2012 R2, but it is enabled in earlier versions. For more details on local accounts and credential theft, refer to the "Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques" documents and Microsoft Knowledge Base article 2871997. The recommended state for this setting is: Disabled. Preventing plaintext storage of credentials in memory reduces the risk of credential theft.

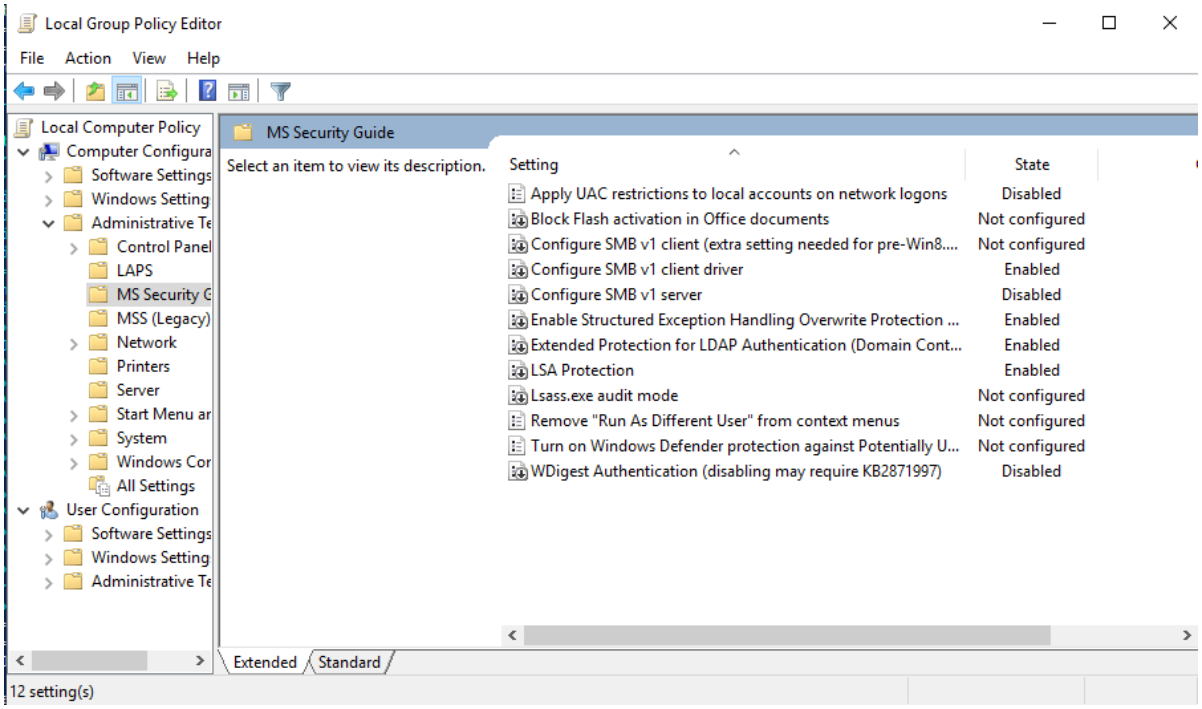


Image 171-Ensure 'WDigest Authentication' is set to 'Disabled'

7.3 MSS (Legacy)

The MSS (Legacy) Group Policy settings refer to older Microsoft Security Settings that were used in previous versions of Windows operating systems. These settings offer guidance on security configurations such as password policies, account lockout policies, and audit settings. While they are still relevant for maintaining security in legacy systems, it is recommended to transition to the latest security settings provided by newer versions of Windows for improved protection and support.

7.3.1 Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled'

This setting is independent of the Welcome screen feature in Windows XP and Vista. If a computer is configured for automatic logon, anyone with physical access can access everything on the computer and any connected networks. Enabling automatic logon stores the password in plaintext in the registry, which is remotely readable by the Authenticated Users group. For more information, see Microsoft Knowledge Base article 324737. The recommended state for this setting is: Disabled. This prevents unauthorized access and safeguards the plaintext password in the registry.

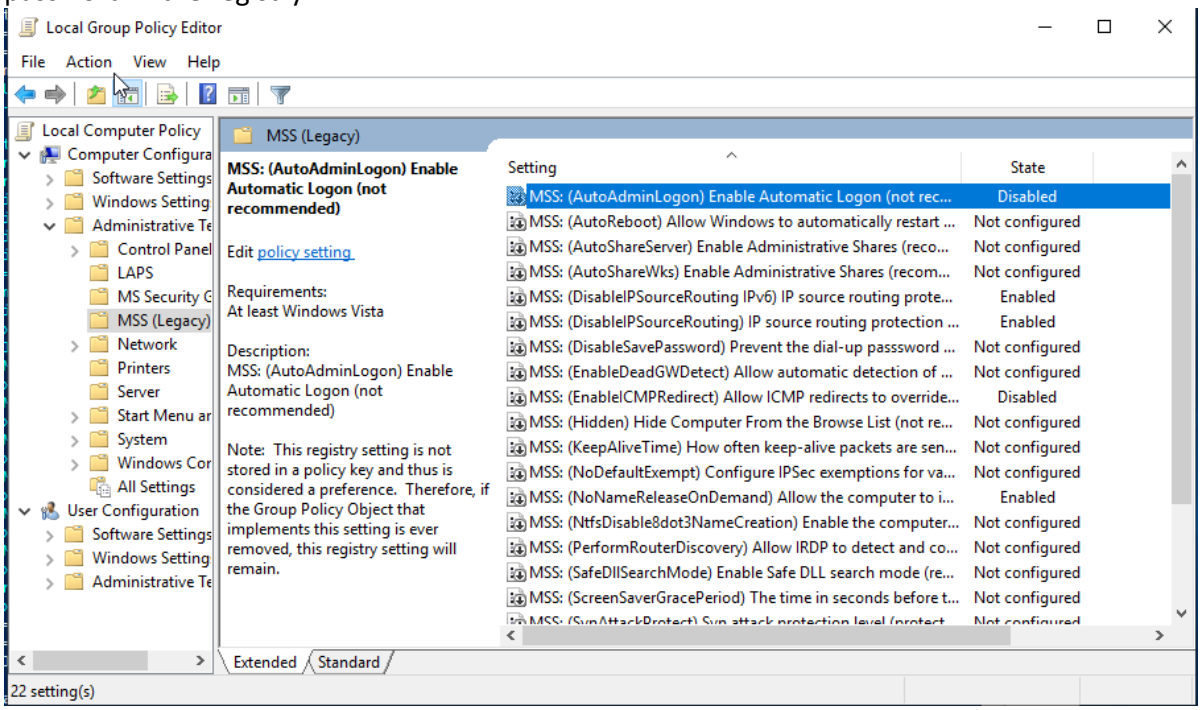


Image 172-Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled'

7.3.2 Ensure 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled'

IP source routing lets the sender specify the route a datagram takes through the network. The recommended state for this setting is: Enabled: Highest protection, source routing is completely disabled. Disabling source routing prevents attackers from using it to hide their identity and location.

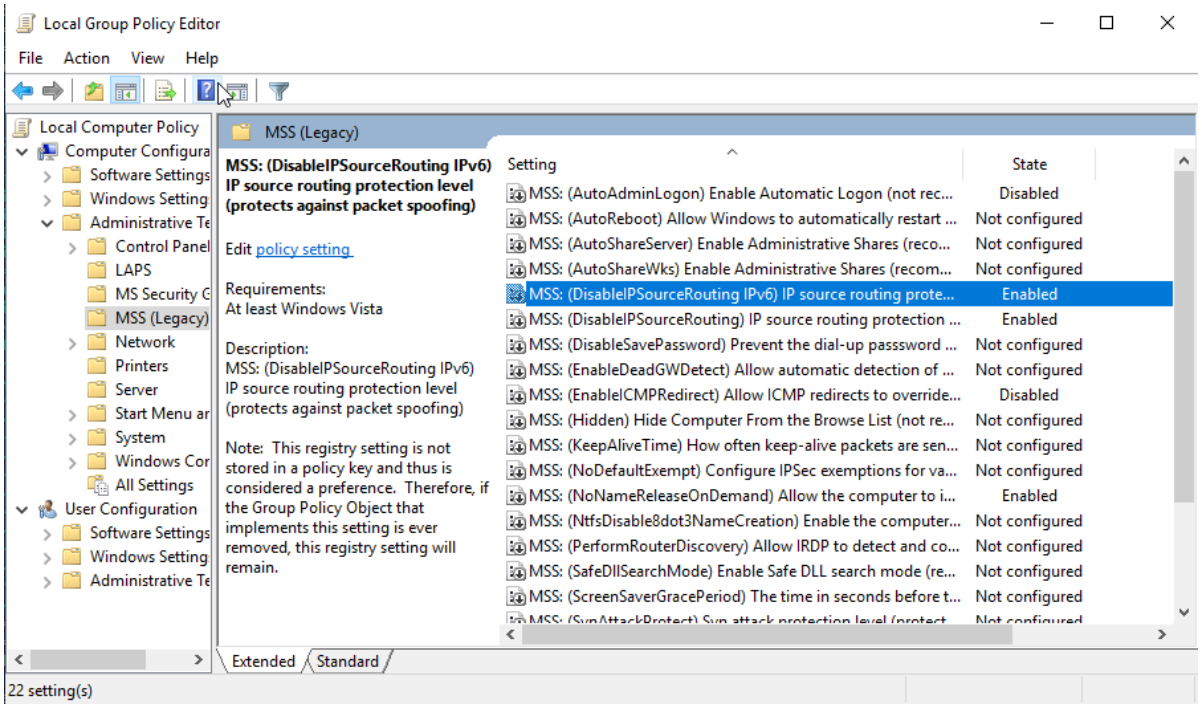


Image 173-Ensure 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled'

7.3.3 Ensure 'MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled'

IP source routing lets the sender specify the path a datagram takes through the network. For enterprise environments, it is recommended to set this to Not Defined, and for high-security environments, to Highest Protection, which completely disables source routing. The recommended state for this setting is: Enabled: Highest protection, source routing is completely disabled. Disabling source routing prevents attackers from using it to hide their identity and location.

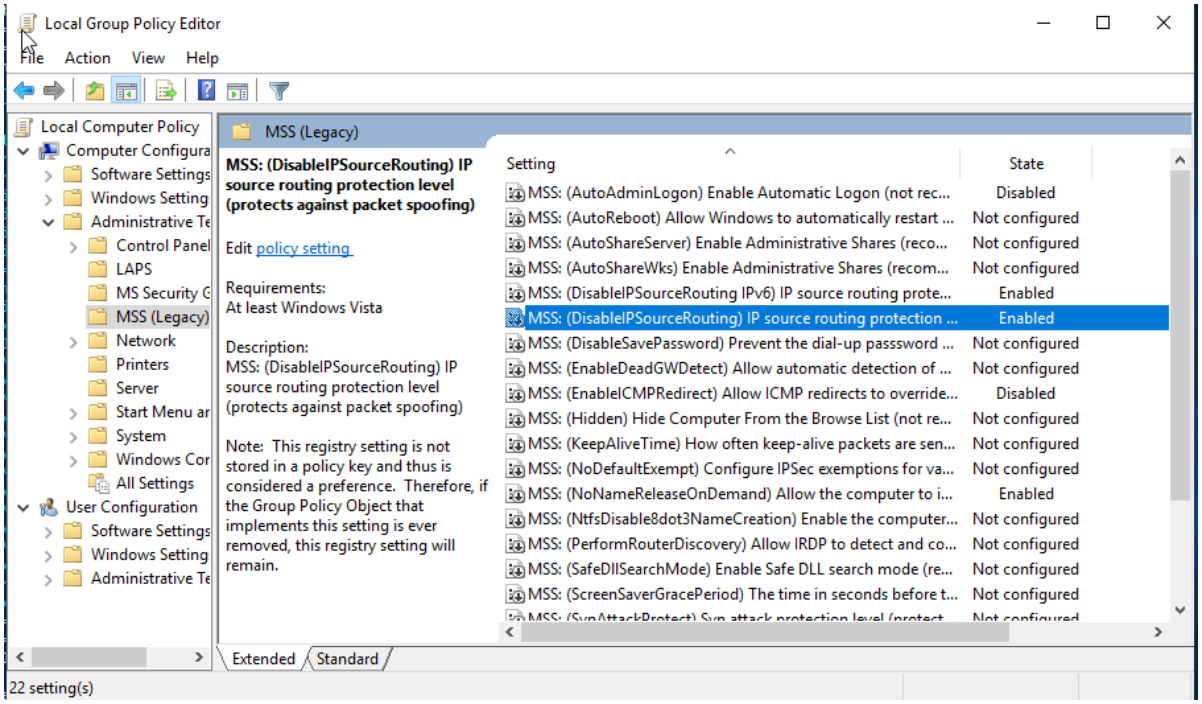


Image 174-Ensure 'MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled'

7.3.4 Ensure 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' is set to 'Disabled'

ICMP redirects cause the IPv4 stack to create host routes that override OSPF-generated routes. The recommended state for this setting is: Disabled. This prevents network issues due to the 10-minute time-out period of ICMP redirect-plumbed routes, ensuring proper traffic routing and reducing the system's vulnerability to network participation attacks.

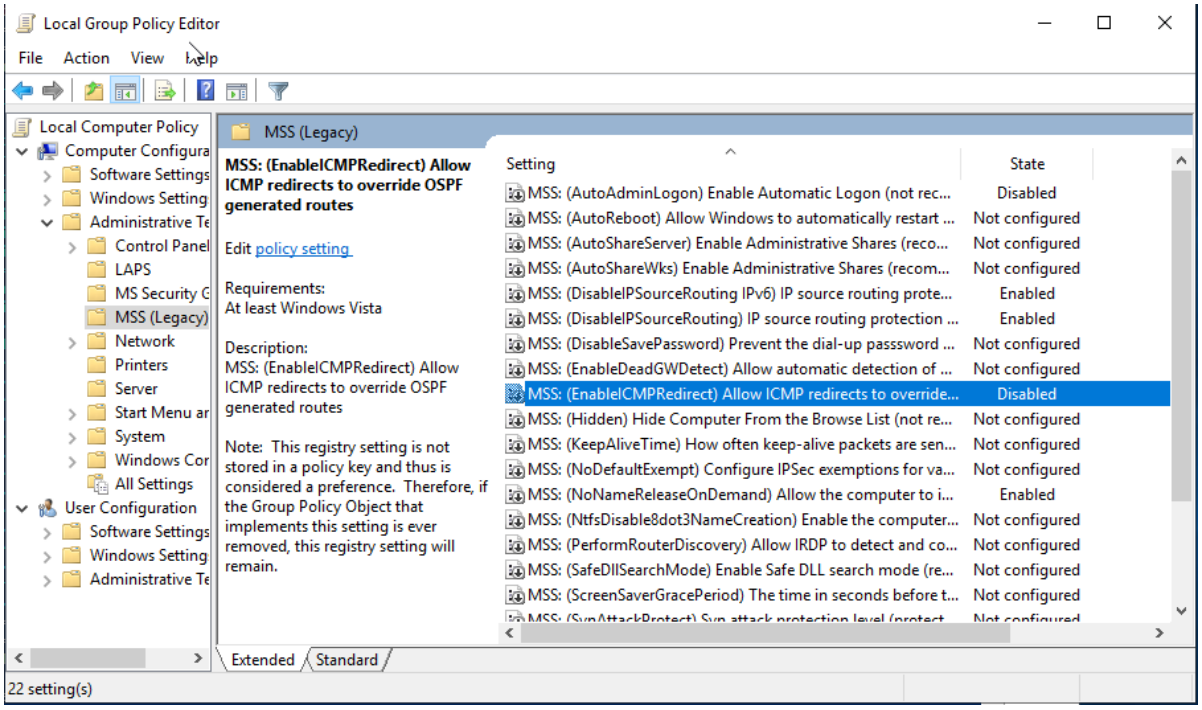


Image 175-Ensure 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' is set to 'Disabled'

7.3.5 Ensure 'MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds' is set to 'Enabled: 300,000 or 5 minutes (recommended)'

This setting determines the frequency of TCP keep-alive packets sent to verify if an idle connection is still active, expecting an acknowledgment from the remote computer if it is reachable. The recommended state for this setting is: Enabled, with a value of 300,000 milliseconds or 5 minutes. This helps prevent an attacker from causing a DoS condition by establishing numerous connections to network applications.

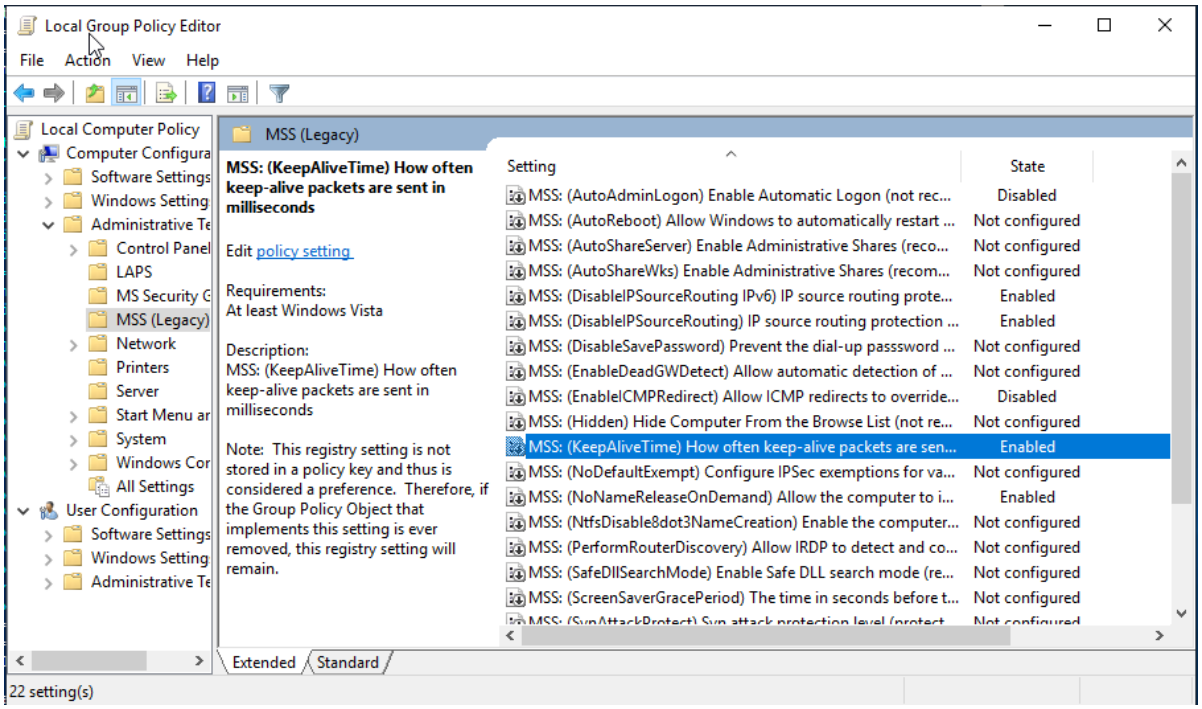


Image 176-Ensure 'MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds' is set to 'Enabled: 300,000 or 5 minutes (recommended)'

7.3.6 Ensure 'MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers' is set to 'Enabled'

NetBIOS over TCP/IP is a network protocol that allows for the easy resolution of NetBIOS names on Windows systems to their IP addresses. This setting determines if the computer releases its NetBIOS name upon receiving a name-release request. The recommended state for this setting is: Enabled.

This protocol lacks authentication, making it vulnerable to spoofing, where a transmission appears to come from a different user. An attacker could exploit this by sending a name-conflict datagram, causing the target computer to relinquish its name and not respond to queries, leading to intermittent connectivity issues, or preventing the use of Network Neighborhood, domain logons, and other NetBIOS name resolution features. Testing in a non-production environment is recommended before making this change in a production environment.

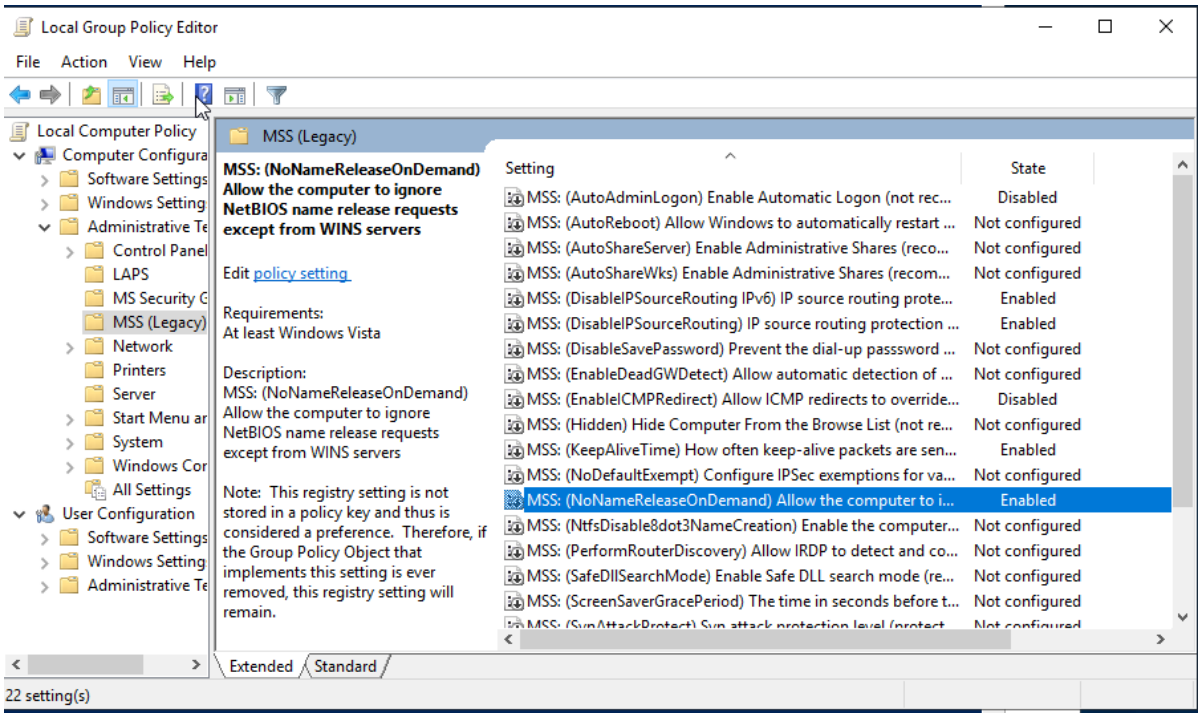


Image 177-Ensure 'MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers' is set to 'Enabled'

7.3.7 Ensure 'MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)' is set to 'Disabled'

This setting enables or disables the Internet Router Discovery Protocol (IRDP), allowing the system to automatically detect and configure default gateway addresses per interface, as described in RFC 1256. The recommended state for this setting is: Disabled.

An attacker on the same network segment could exploit IRDP by configuring a computer to impersonate a router, causing other computers with IRDP enabled to route their traffic through the compromised machine.

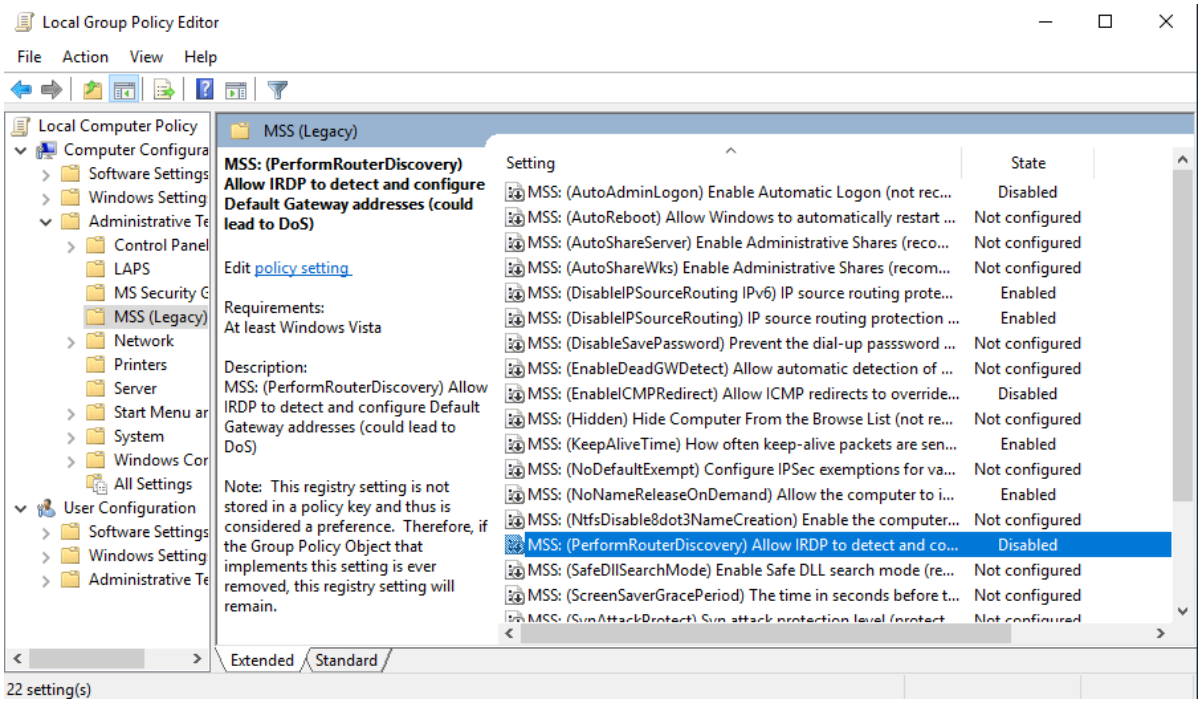


Image 178-Ensure 'MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)' is set to 'Disabled'

7.3.8 Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' is set to 'Enabled'

The DLL search order can be configured in two ways: either by searching folders specified in the system path first and then the current working folder, or by searching the current working folder first and then the system path. When enabled, the system searches the system path first (registry value set to 1). When disabled, it searches the current working folder first (registry value set to 0). Enabling this setting ensures that applications search for DLLs in the system path first, which may prevent performance or stability issues for applications that require unique DLL versions. The recommended state for this setting is: Enabled.

This helps prevent hostile code from loading its own versions of system DLLs, potentially reducing the damage such code can cause.

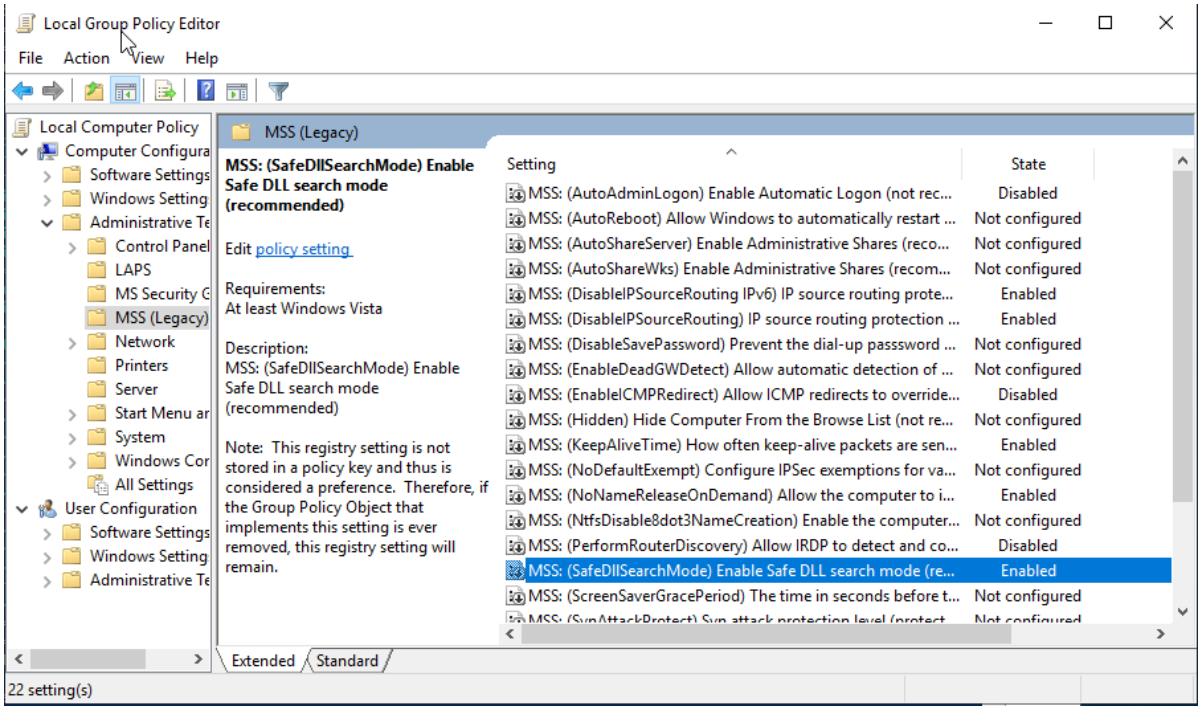


Image 179-Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' is set to 'Enabled'

7.3.9 Ensure 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)' is set to 'Enabled: 5 or fewer seconds'

Windows provides a grace period between when the screen saver activates and when the console locks automatically. The recommended state for this setting is: Enabled, with a grace period of 5 seconds or less. This minimizes the time window in which someone could access the console before it locks, reducing the risk of unauthorized access. The grace period can be adjusted via a registry entry.

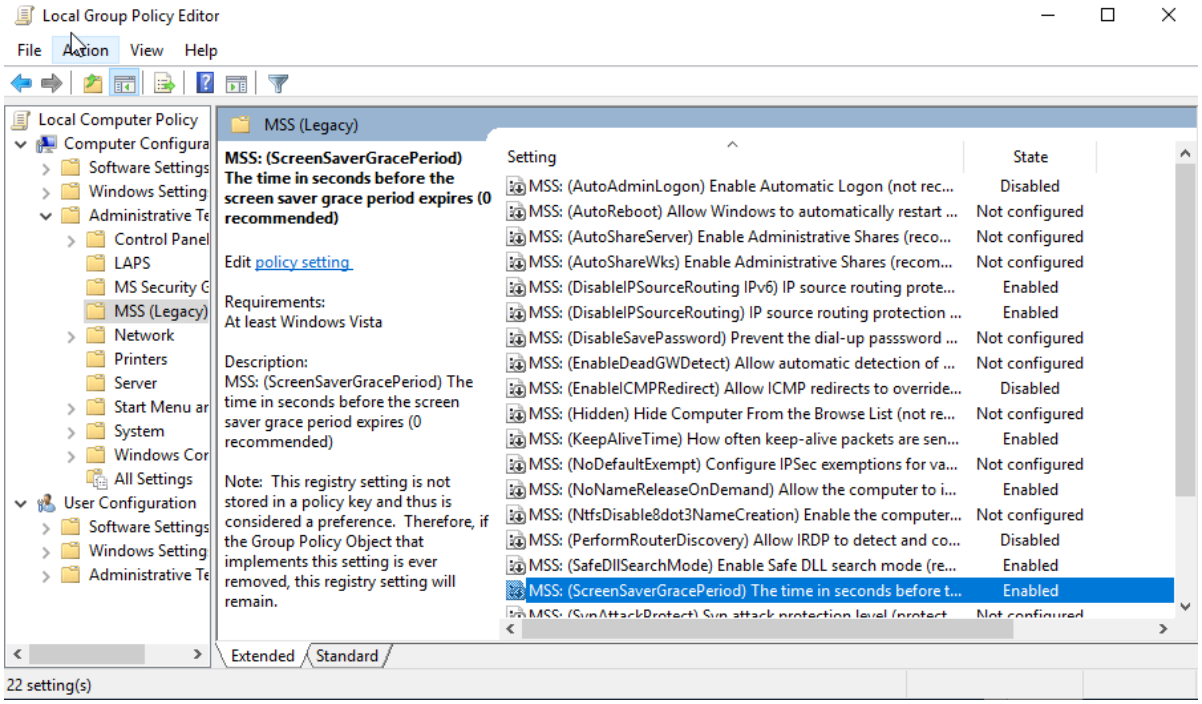


Image 180-Ensure 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)' is set to 'Enabled: 5 or fewer seconds'

7.3.10 Ensure 'MSS: (TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted' is set to 'Enabled: 3'

This setting regulates the number of retransmissions for a TCP data segment (excluding connect segments) before the connection is terminated. Each retransmission doubles the time-out period, which resets when responses resume, with the base time-out determined dynamically by the connection's round-trip time. The recommended configuration is: Enabled, with 3 retransmissions. This helps prevent a scenario where a malicious user could deplete a target computer's resources by not acknowledging received data.

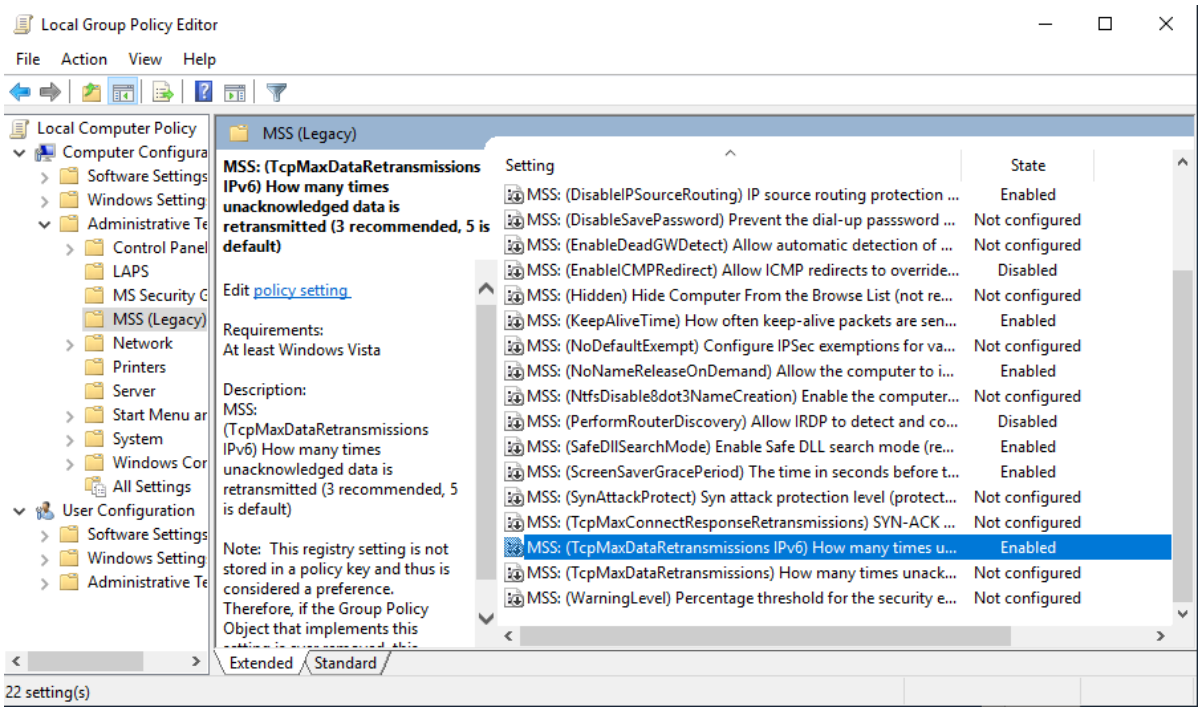


Image 181-Ensure 'MSS: (TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted' is set to 'Enabled: 3'

7.3.11 Ensure 'MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted' is set to 'Enabled: 3'

This setting manages how many times TCP will retransmit a single data segment (excluding connect segments) before terminating the connection. The time-out period doubles with each retransmission and resets when responses are received, with the base time-out value dynamically based on the connection's round-trip time. It is recommended to configure this setting to: Enabled, with a value of 3. This prevents a situation where a malicious user could overload a target computer's resources by not acknowledging received data.

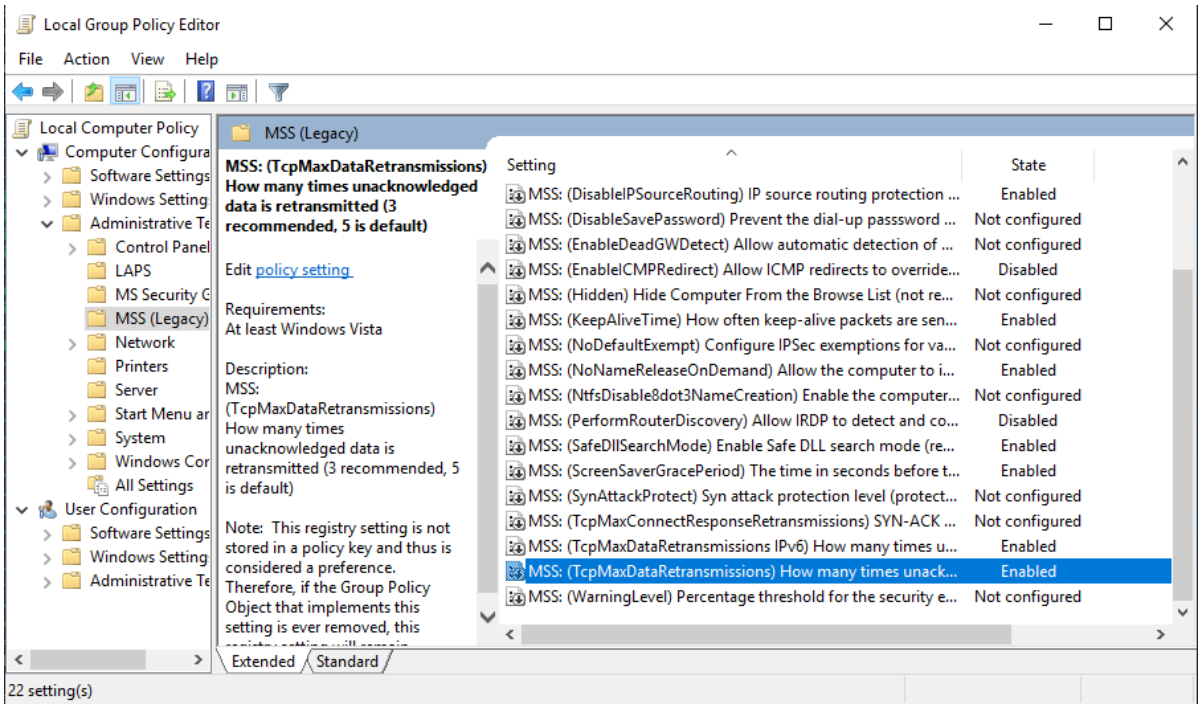


Image 182-Ensure 'MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted' is set to 'Enabled: 3'

7.3.12 Ensure 'MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning' is set to 'Enabled: 90% or less'

This setting allows for the generation of a security audit in the Security event log when the log approaches a user-defined capacity threshold. It is recommended to set this to: Enabled, with a threshold of 90% or less. Note that if the log settings are configured to either overwrite events as needed or overwrite events older than a certain number of days, this event will not be triggered. Monitoring the log's capacity is crucial; if it reaches 90% and the system is not set to overwrite older events, new entries will not be recorded. If the log fills up and the system is configured to shut down when it cannot log new events, the computer will shut down and become unavailable for network services.

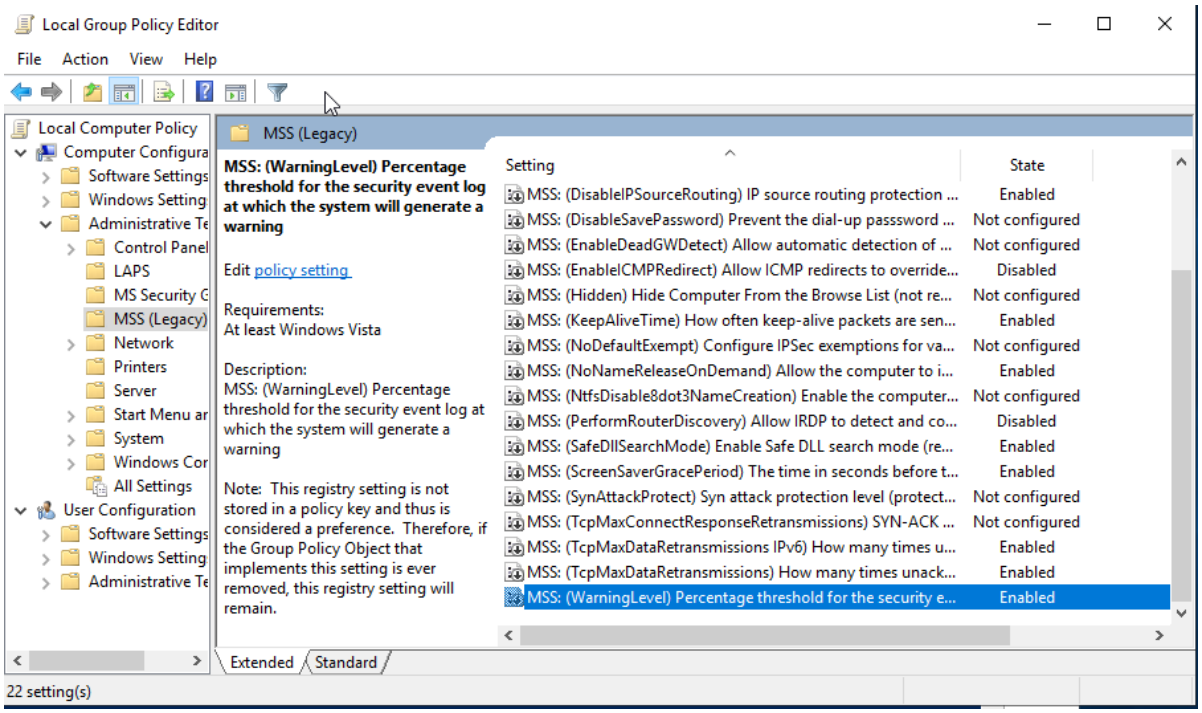


Image 183-Ensure 'MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning' is set to 'Enabled: 90% or less'

7.4 Network

The Network Group Policy settings manage various aspects of network connectivity and security within a Windows environment. These settings control configurations related to network access, firewall rules, VPNs, and network sharing. Properly configuring network policies helps ensure secure and efficient network operations, protect against unauthorized access, and manage network resources effectively across the organization.

7.4.1 DNS Client

7.4.1.1 Ensure 'Turn off multicast name resolution' is set to 'Enabled'

LLMNR is a secondary name resolution protocol that uses multicast to send queries over a local network link within a single subnet. It allows client computers on the same subnet to resolve names without needing a DNS server or client configuration, providing an alternative when conventional DNS resolution fails. The recommended setting for LLMNR is: Enabled. This is because attackers can exploit LLMNR (UDP/5355) or NBT-NS (UDP/137) broadcasts to intercept and respond to queries, misleading the host into believing it has found the requested system.

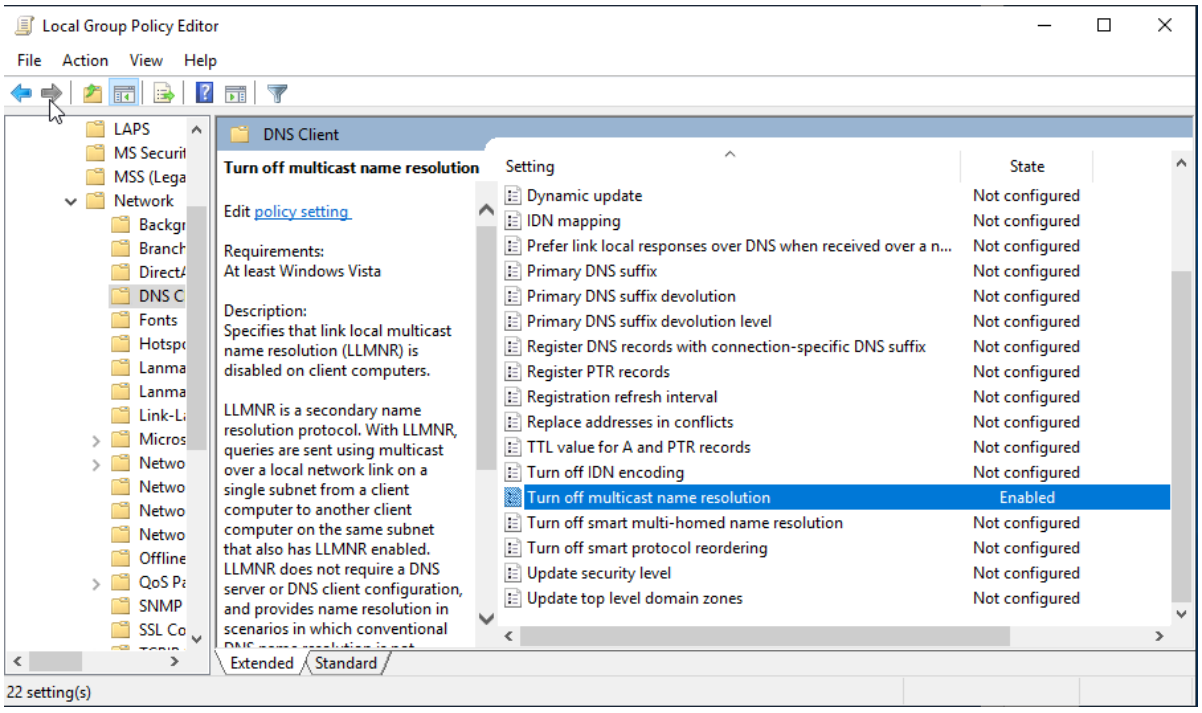


Image 184-Ensure 'Turn off multicast name resolution' is set to 'Enabled'

7.4.2 Fonts

7.4.2.1 Ensure 'Enable Font Providers' is set to 'Disabled'

This policy setting controls whether Windows can download fonts and font catalog data from an online provider. It is recommended to set this policy to: Disabled. This ensures that the IT department in a managed enterprise environment oversees and approves all system configuration changes to maintain proper testing and control.

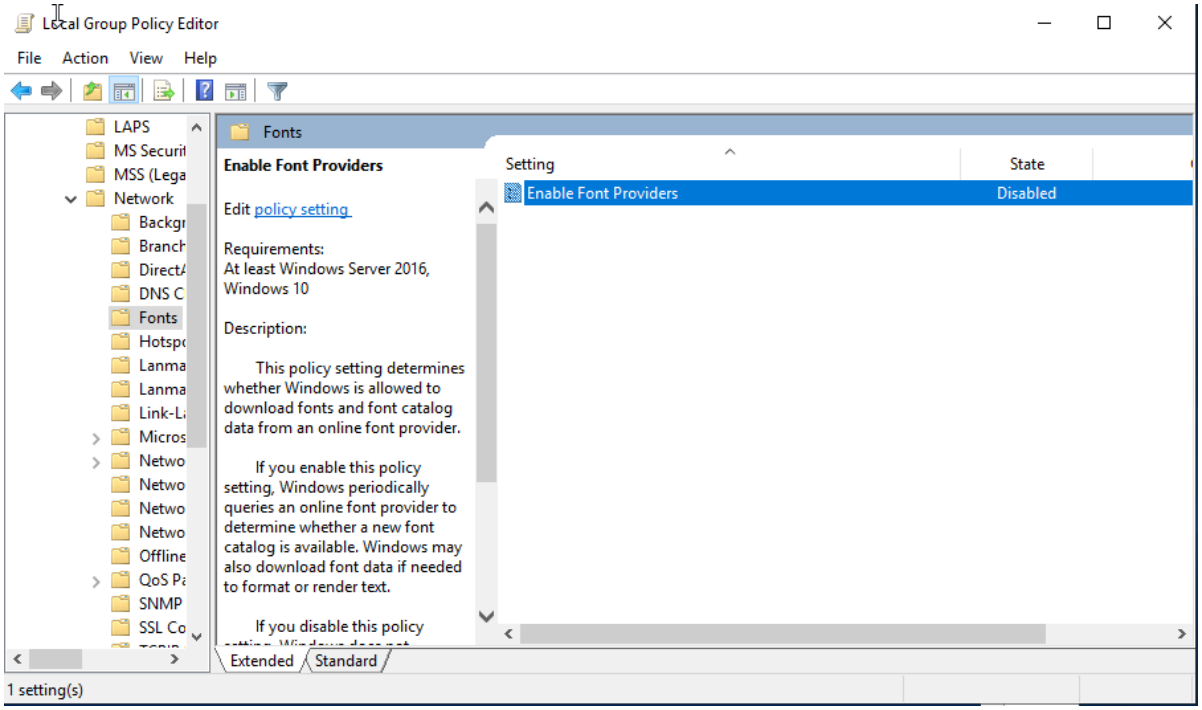


Image 185-Ensure 'Enable Font Providers' is set to 'Disabled'

7.4.3 Lanman Workstation

7.4.3.1 Ensure 'Enable insecure guest logons' is set to 'Disabled'

This policy setting controls whether the SMB client permits insecure guest logons to an SMB server. It is recommended to set this policy to: Disabled. Insecure guest logons enable file servers to provide unauthenticated access to shared folders.

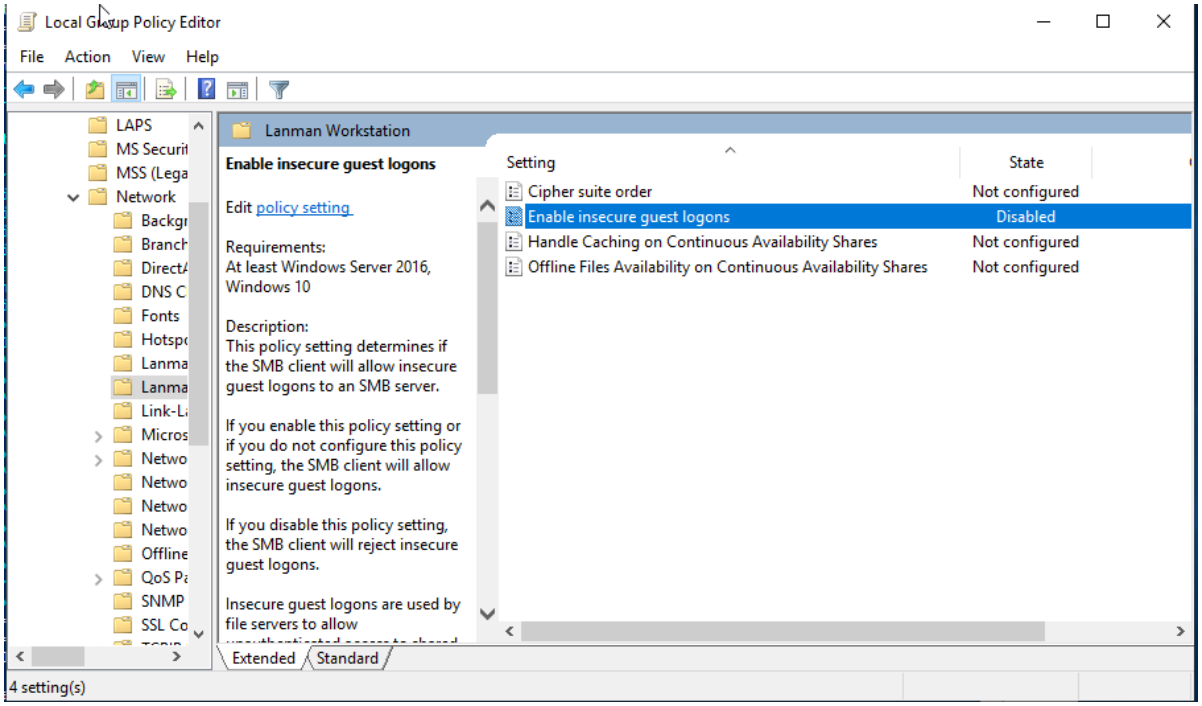


Image 186-Ensure 'Enable insecure guest logons' is set to 'Disabled'

7.4.4 Link-Layer Topology Discovery

7.4.4.1 Ensure 'Turn on Mapper I/O (LLTDIO) driver' is set to 'Disabled'

This policy setting modifies the operational behavior of the Mapper I/O network protocol driver. LLTDIO enables a computer to map the network topology it is connected to and to request Quality-of-Service features like bandwidth estimation and network health analysis. The recommended state for this setting is: Disabled. Disabling it helps protect against unauthorized network discovery and connections by preventing responses to network traffic related to topology discovery.

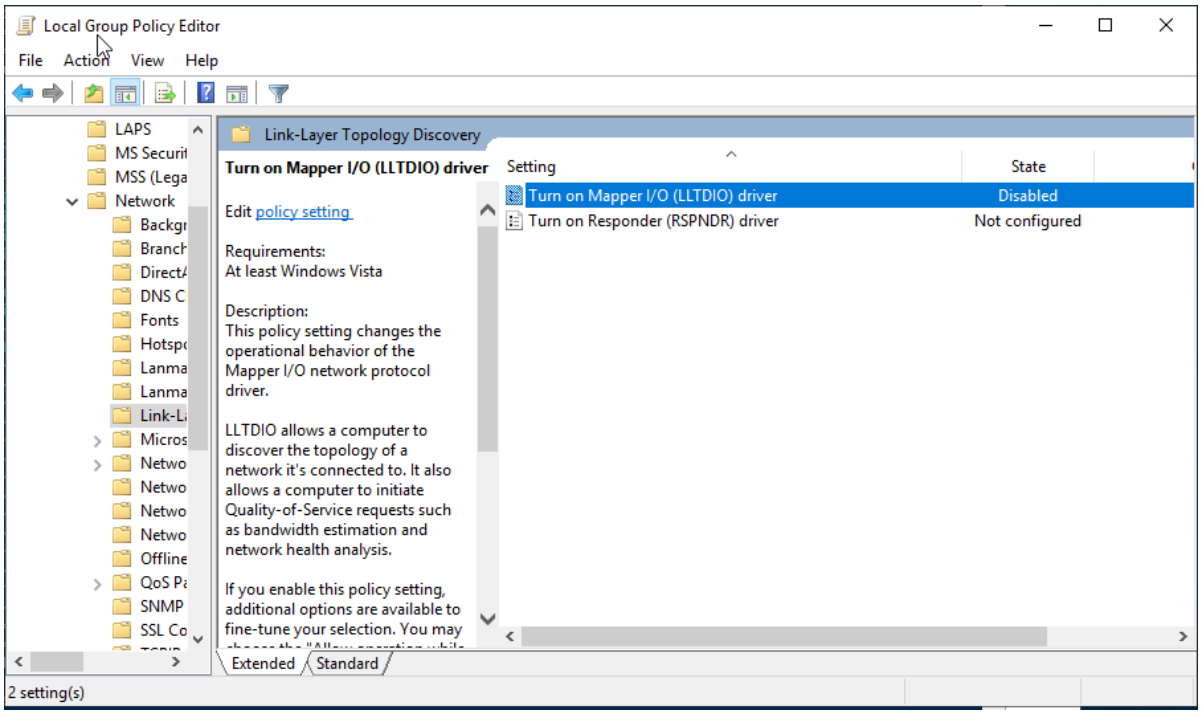


Image 187-Ensure 'Turn on Mapper I/O (LLTDIO) driver' is set to 'Disabled'

7.4.4.2 Ensure 'Turn on Responder (RSPNDR) driver' is set to 'Disabled'

This policy setting adjusts the operation of the Responder network protocol driver. The Responder enables a computer to engage in Link Layer Topology Discovery requests, making it detectable and locatable on the network, and allows participation in Quality-of-Service functions like bandwidth estimation and network health analysis. The recommended state for this setting is: Disabled. Disabling it helps protect against unauthorized network discovery and connections by preventing responses to network traffic related to topology discovery.

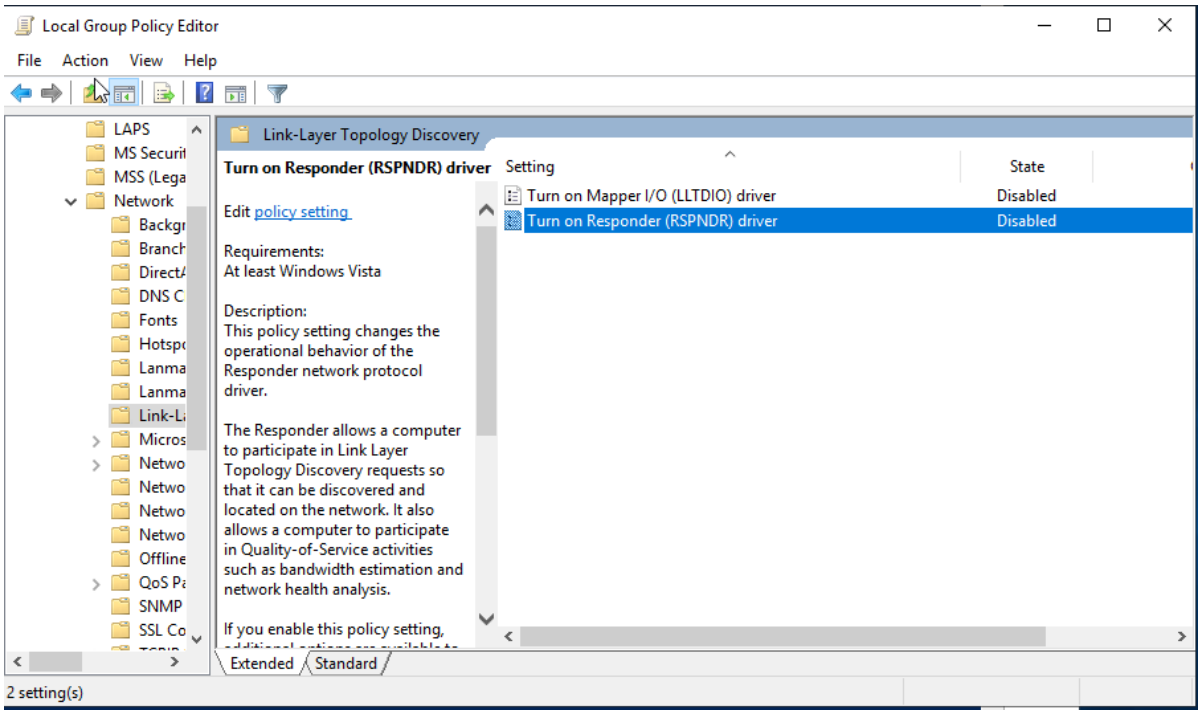


Image 188-Ensure 'Turn on Responder (RSPNDR) driver' is set to 'Disabled'

7.4.5 Microsoft Peer-to-Peer Networking Services

7.4.5.1 Ensure 'Turn off Microsoft Peer-to-Peer Networking Services' is set to 'Enabled'

The Peer Name Resolution Protocol (PNRP) facilitates the distributed resolution of names to IPv6 addresses and port numbers within cloud environments, where a cloud consists of peer computers communicating within the same IPv6 scope. Peer-to-Peer protocols support various applications, including real-time communication, collaboration, content distribution, and distributed processing. The recommended state for this setting is: Enabled. Enabling this setting improves security and minimizes the risk associated with peer-to-peer networking.

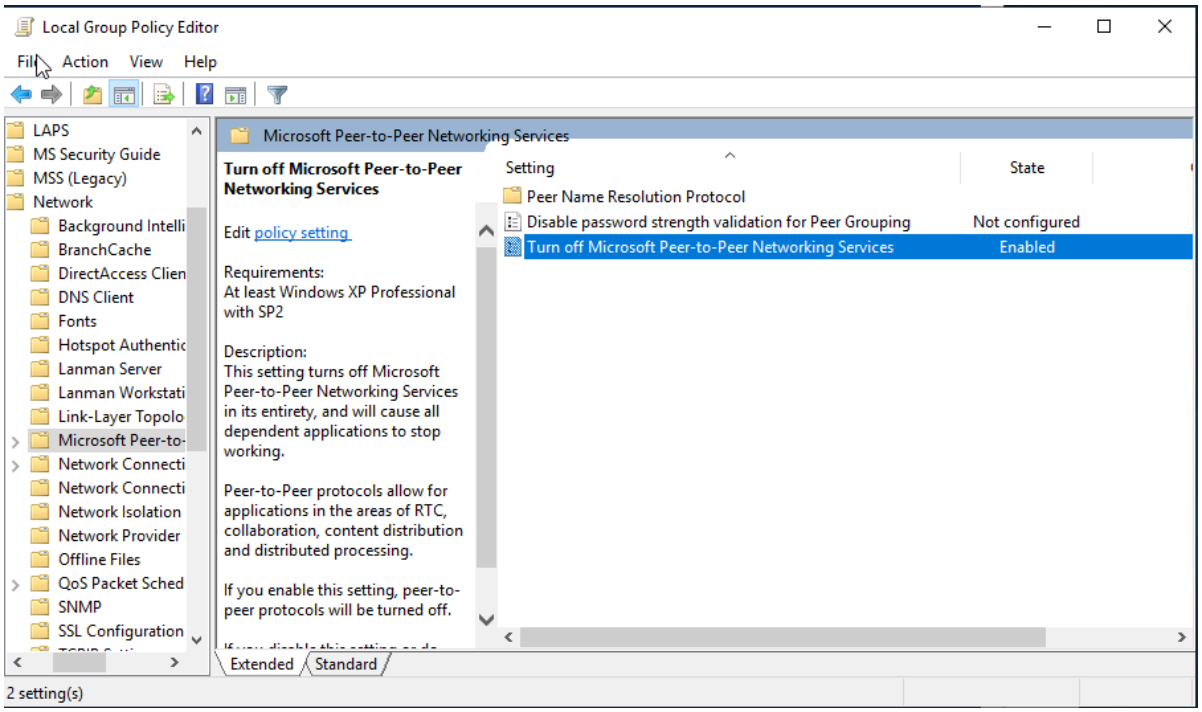


Image 189-Ensure 'Turn off Microsoft Peer-to-Peer Networking Services' is set to 'Enabled'

7.4.6 Network Connections

7.4.6.1 Ensure 'Prohibit installation and configuration of Network Bridge on your DNS domain network' is set to 'Enabled'

This setting allows you to manage a user's ability to install and configure a Network Bridge. The recommended state for this setting is: Enabled. Enabling this setting permits users to create a Layer 2 Media Access Control (MAC) bridge, which can connect multiple physical network segments and enable data sharing between different networks. In a controlled enterprise environment where network traffic should be restricted to authorized paths, allowing users to set up a Network Bridge could increase the risk and expand the attack surface from the bridged networks.

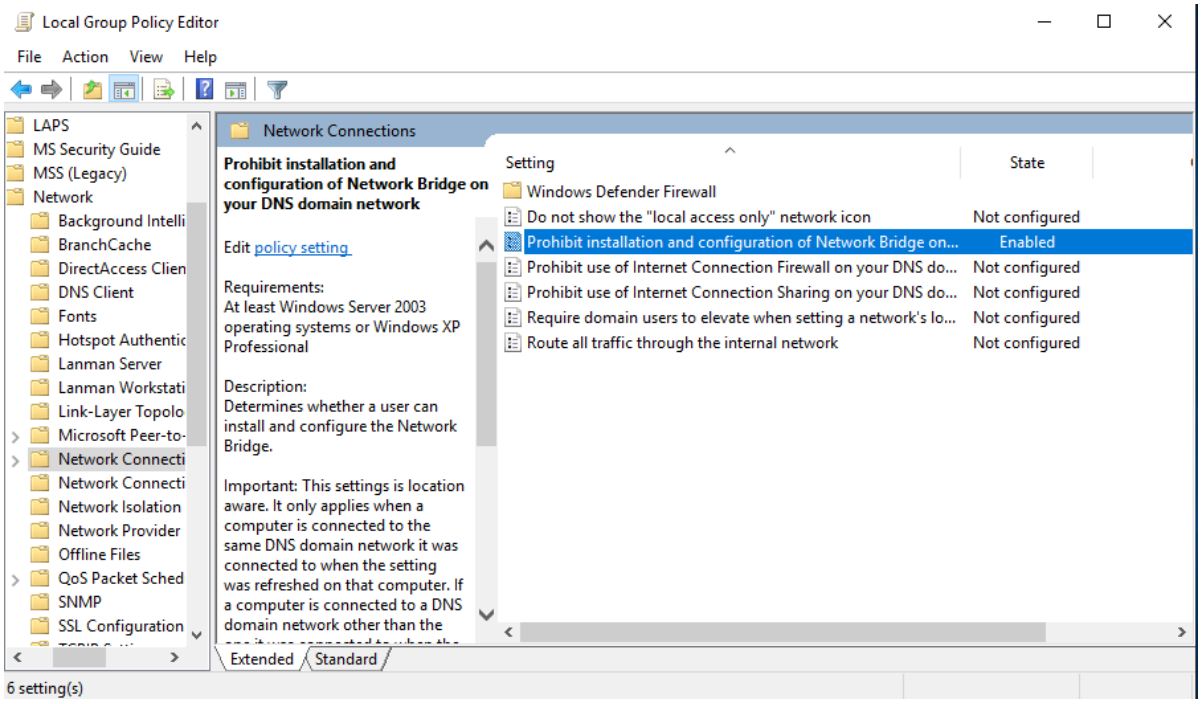


Image 190-Ensure 'Prohibit installation and configuration of Network Bridge on your DNS domain network' is set to 'Enabled'

7.4.6.2 Ensure 'Prohibit use of Internet Connection Sharing on your DNS domain network' is set to 'Enabled'

Originally used for Internet Connection Sharing (ICS) in Windows 2000, XP, and Server 2003, this setting now applies to the Mobile Hotspot feature in Windows 10 and Server 2016. The recommended state for this setting is: Enabled. This configuration ensures that non-administrators cannot activate the Mobile Hotspot feature, thereby preventing them from sharing their internet connection with nearby mobile devices.

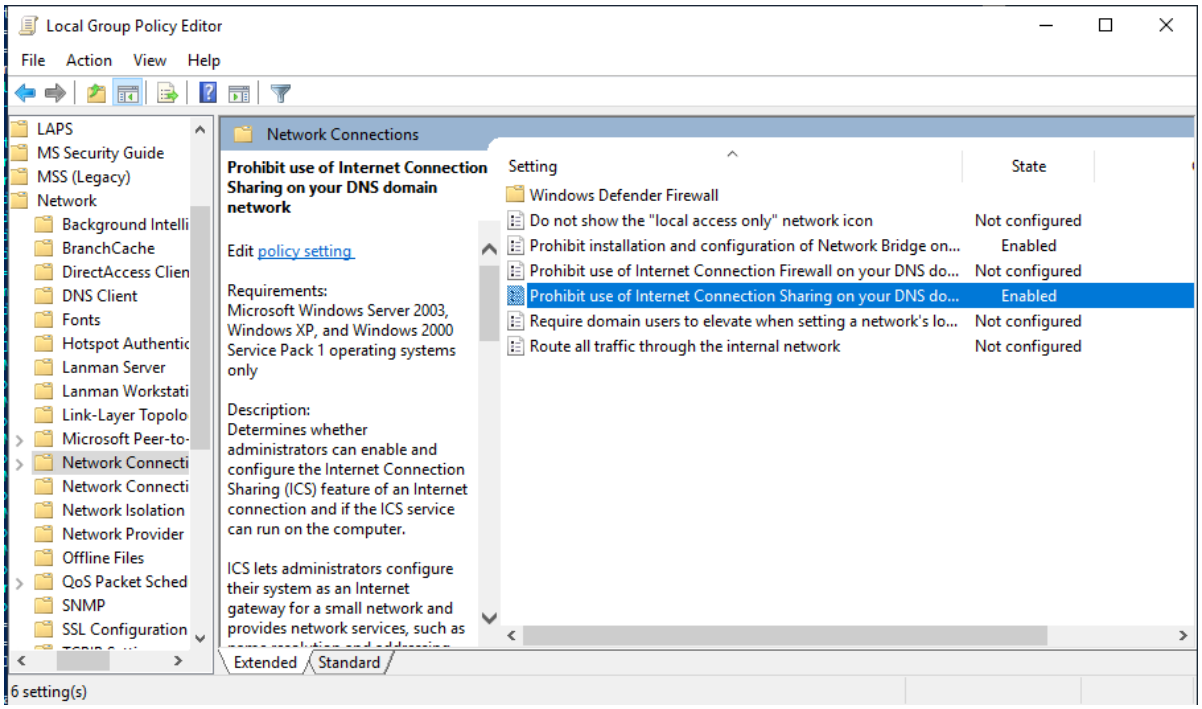


Image 191-Ensure 'Prohibit use of Internet Connection Sharing on your DNS domain network' is set to 'Enabled'

7.4.7 Network Provider

7.4.7.1 Ensure 'Hardened UNC Paths' is set to 'Enabled, with "Require Mutual Authentication" and "Require Integrity" set for all NETLOGON and SYSVOL shares'

This policy setting ensures secure access to UNC paths. The recommended state is: Enabled, with "Require Mutual Authentication" and "Require Integrity" enforced for all NETLOGON and SYSVOL shares. If the environment only includes Windows 8.0/Server 2012 (non-R2) or newer systems, the "Require Privacy" setting can optionally be enabled for SMB encryption, though this will block access for older OS versions and should be used cautiously. This setting mitigates a security risk in Group Policy addressed by the MS15-011 / MSKB 3000483 update, requiring specific Group Policy settings on domain computers running Windows Vista/Server 2008 (non-R2) or newer.

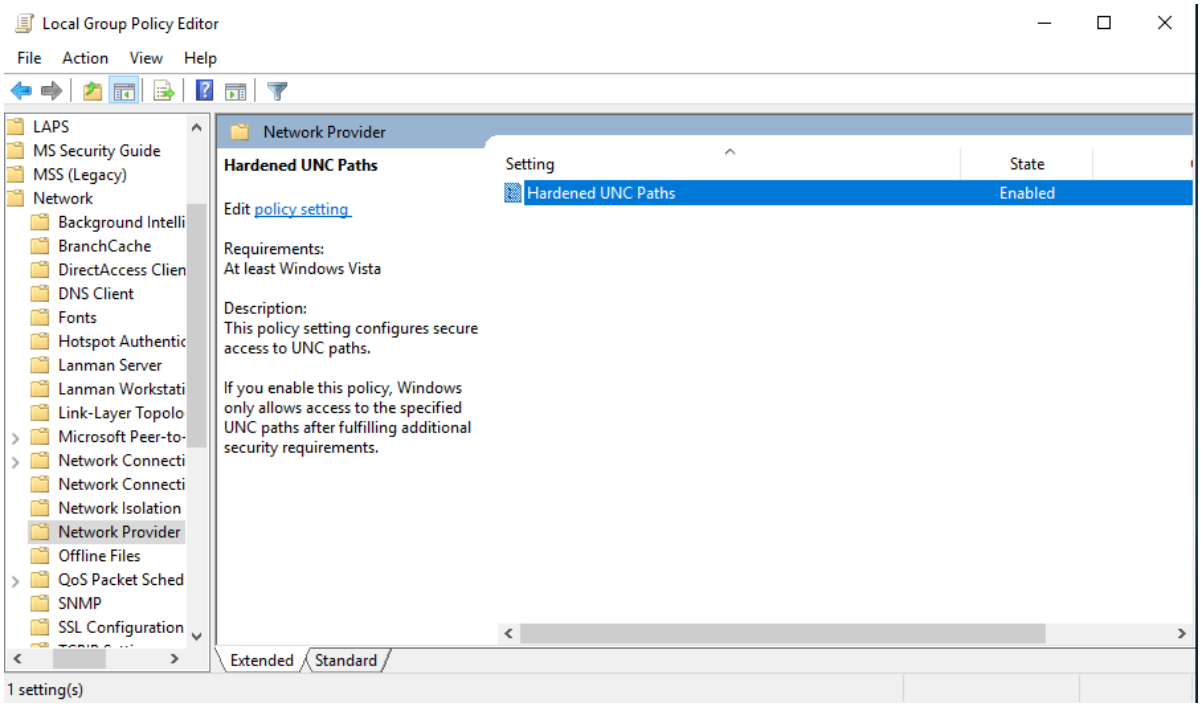


Image 192-Ensure 'Hardened UNC Paths' is set to 'Enabled, with "Require Mutual Authentication" and "Require Integrity" set for all NETLOGON and SYSVOL shares'

7.4.8 Windows Connect Now

7.4.8.1 Ensure 'Configuration of wireless settings using Windows Connect Now' is set to 'Disabled'

This policy setting controls the configuration of wireless settings using Windows Connect Now (WCN), which allows the discovery and setup of devices over Ethernet, Wi-Fi, and USB. The recommended state is Disabled to enhance security and minimize risks associated with user-configured wireless settings.

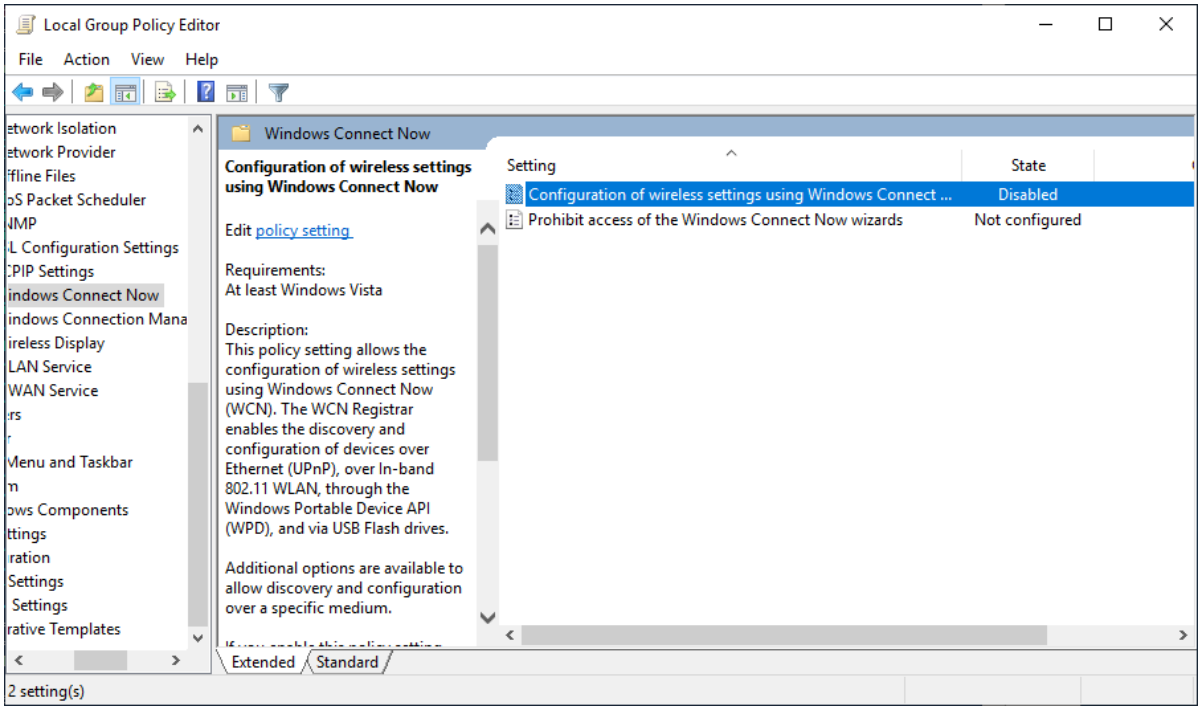


Image 193-Ensure 'Configuration of wireless settings using Windows Connect Now' is set to 'Disabled'

7.4.8.2 Ensure 'Prohibit access of the Windows Connect Now wizards' is set to 'Enabled'

This policy setting restricts access to Windows Connect Now (WCN) wizards. The recommended state is Enabled to reduce risk and minimize the attack surface by preventing standard users from accessing the WCN wizard.

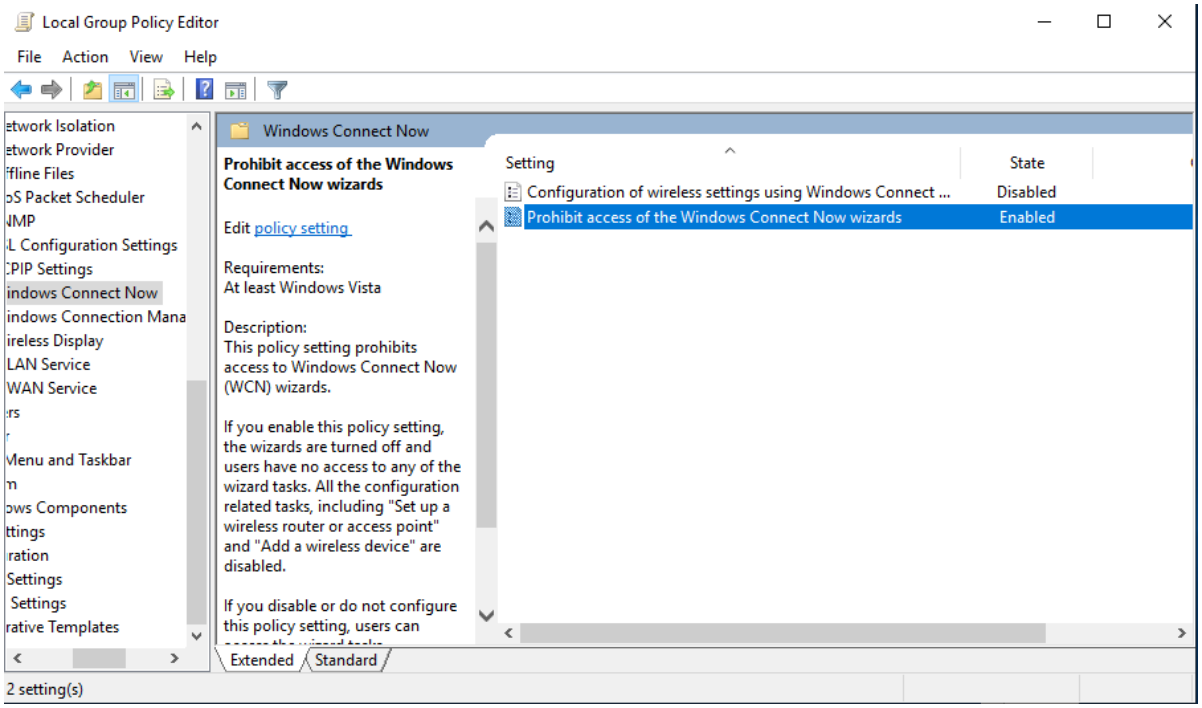


Image 194-Ensure 'Prohibit access of the Windows Connect Now wizards' is set to 'Enabled'

7.4.9 Windows Connection Manager

7.4.9.1 Ensure 'Minimize the number of simultaneous connections to the Internet or a Windows Domain' is set to 'Enabled: 3 = Prevent Wi-Fi when on Ethernet'

This policy setting restricts computers from establishing multiple simultaneous connections to the Internet or a Windows domain. The recommended state is Enabled with the setting "Prevent Wi-Fi when on Ethernet" to reduce the risk of unintentional bridging between internal and external networks, protecting sensitive internal data.

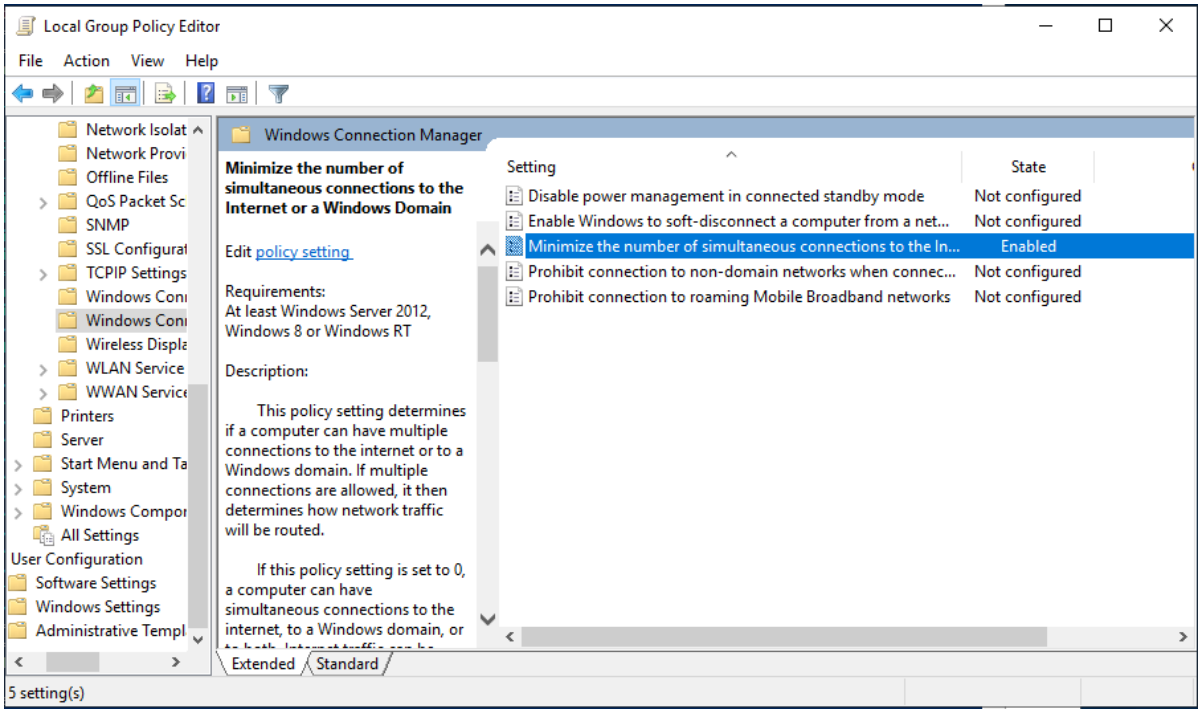


Image 195-Ensure 'Minimize the number of simultaneous connections to the Internet or a Windows Domain' is set to 'Enabled: 3 = Prevent Wi-Fi when on Ethernet'

7.5 Printers

The Printers Group Policy settings control the management and configuration of printers within a Windows environment. These settings can govern printer deployment, access permissions, and printer driver installations. By properly configuring printer policies, administrators can ensure secure and efficient printer usage, manage printer resources, and control who can add or modify printers within the network.

7.5.1 Ensure 'Allow Print Spooler to accept client connections' is set to 'Disabled'

This policy setting determines whether the Print Spooler service will accept client connections. The recommended state is Disabled to mitigate remote attacks like the PrintNightmare vulnerability (CVE-2021-34527) and other remote Print Spooler attacks. Note that the Print Spooler service must be restarted for changes to take effect, and an exception to this recommendation is necessary for print servers to function properly, as disabling client connections will prevent users from printing to the server.

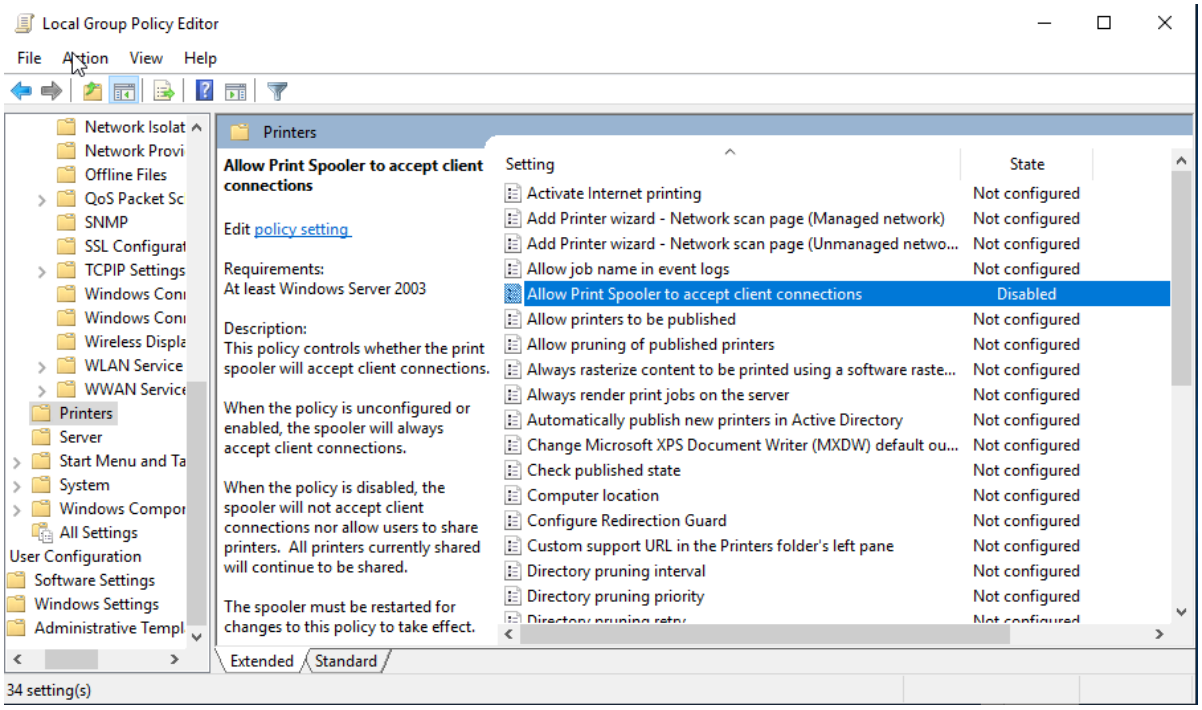


Image 196-Ensure 'Allow Print Spooler to accept client connections' is set to 'Disabled'

7.5.2 Ensure 'Configure Redirection Guard' is set to 'Enabled: Redirection Guard Enabled'

This policy setting controls whether Redirection Guard is enabled for the print spooler, preventing file redirections within the spooler. The recommended state is Enabled, which stops non-administrators from redirecting files within the print spooler process.

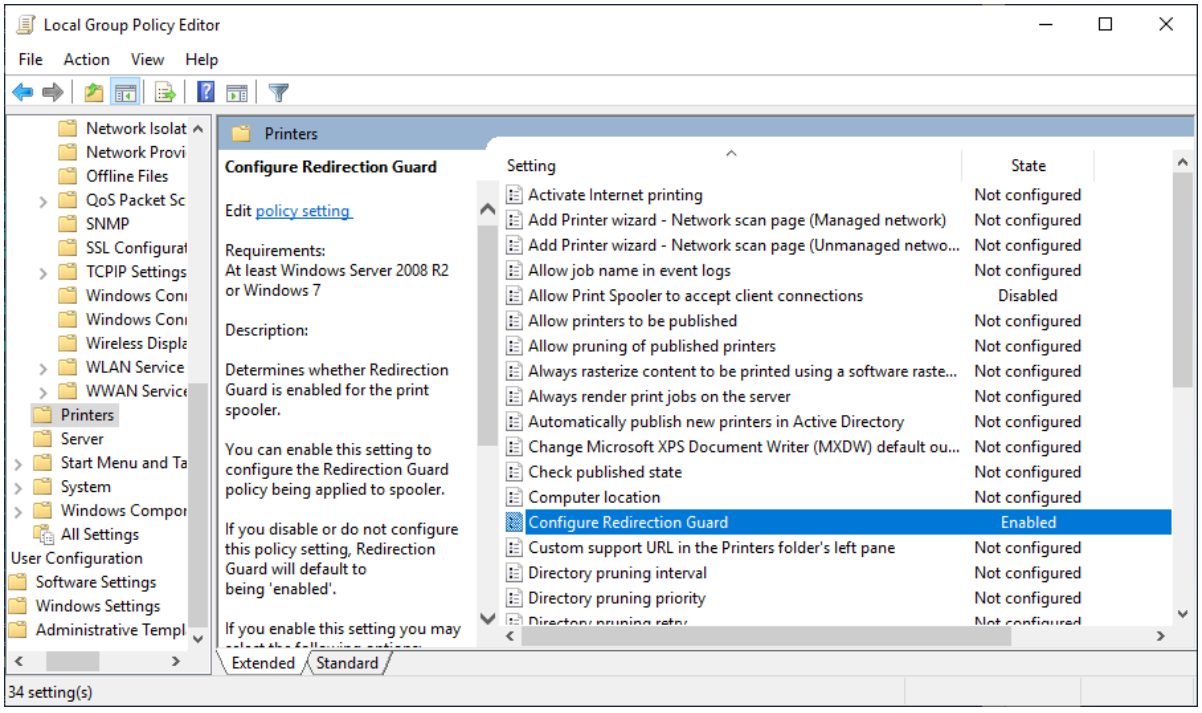


Image 197-Ensure 'Configure Redirection Guard' is set to 'Enabled: Redirection Guard Enabled'

7.5.3 Ensure 'Point and Print Restrictions: When installing drivers for a new connection' is set to 'Enabled: Show warning and elevation prompt'

This policy setting controls whether computers display a warning and a security elevation prompt when users create a new printer connection using Point and Print. The recommended state is Enabled: Show warning and elevation prompt. Following a Microsoft update on August 10, 2021, Administrator privileges are now required for Point and Print driver installations and updates, as documented in KB5005652. This change overrides existing Point and Print Group Policy settings and ensures that only Administrators can install printer drivers from a print server, helping to mitigate the PrintNightmare vulnerability (CVE-2021-34527) and other Print Spooler attacks.

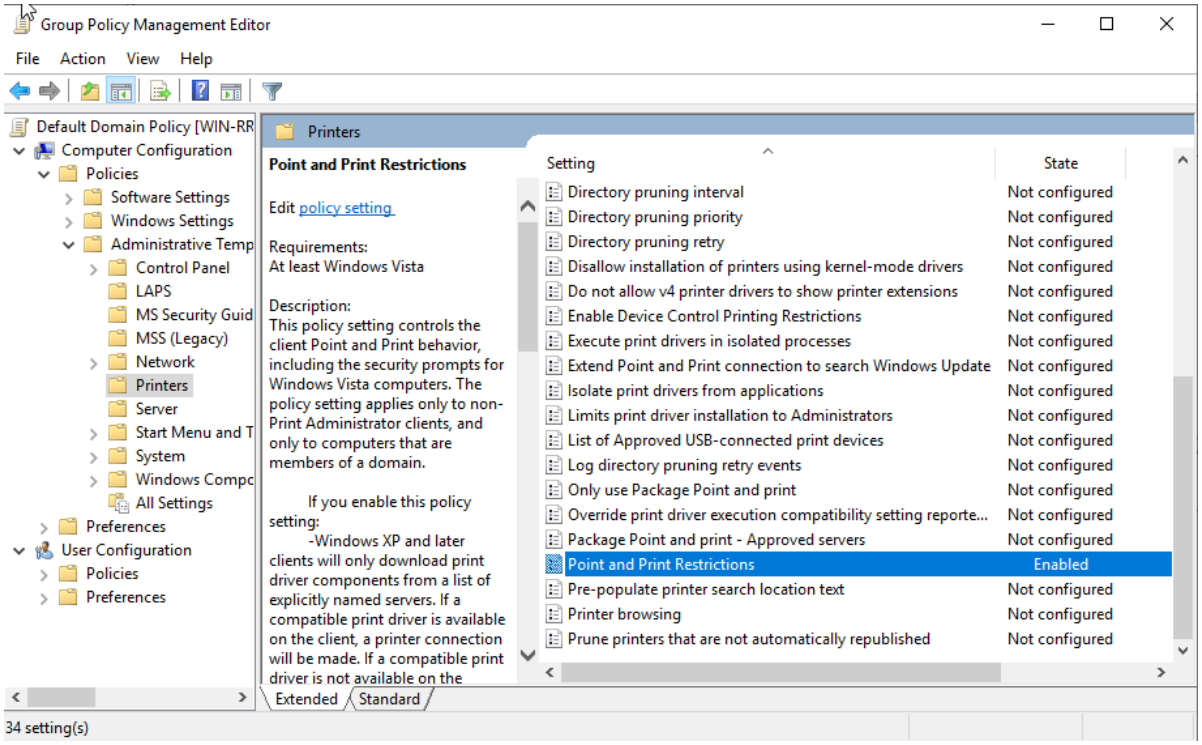


Image 198-Ensure 'Point and Print Restrictions: When installing drivers for a new connection' is set to 'Enabled: Show warning and elevation prompt'

7.5.4 Ensure 'Point and Print Restrictions: When updating drivers for an existing connection' is set to 'Enabled: Show warning and elevation prompt'

This policy setting determines whether computers will display a warning and a security elevation prompt when users update drivers for an existing connection using Point and Print. The recommended state is Enabled: Show warning and elevation prompt. Following an August 10, 2021, update by Microsoft, Administrator privileges are now required for Point and Print driver installations and updates, as outlined in KB5005652. This update overrides all previous Point and Print Group Policy settings, ensuring only Administrators can install printer drivers from a print server. This helps mitigate the PrintNightmare vulnerability (CVE-2021-34527) and other Print Spooler attacks. Although the default behavior now requires Administrator privileges, it is crucial to configure this setting as a precaution in case the default behavior changes.

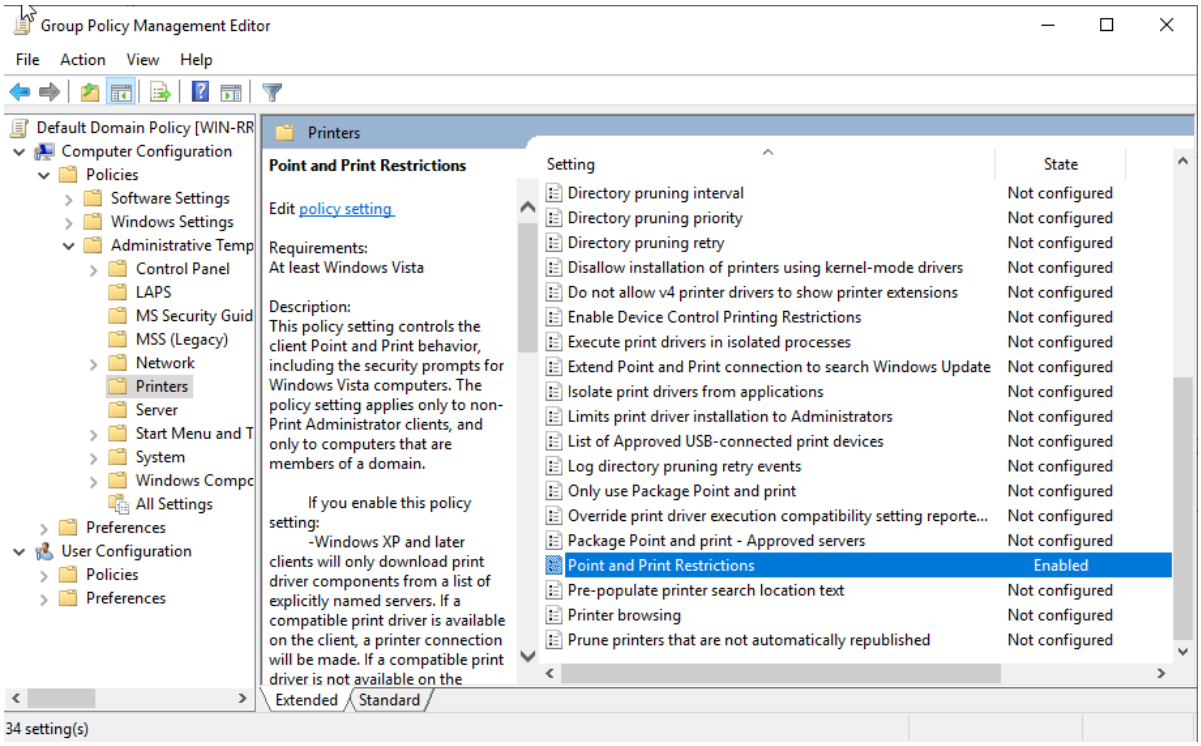


Image 199-Ensure 'Point and Print Restrictions: When updating drivers for an existing connection' is set to 'Enabled: Show warning and elevation prompt'

7.6 Start Menu and Taskbar

The Start Menu and Taskbar Group Policy settings manage the configuration and behavior of the Start Menu and Taskbar in Windows. These policies can control which icons are displayed, how the Start Menu is organized, and what features are available on the Taskbar. By adjusting these settings, administrators can customize the user interface for efficiency, enforce organizational branding, and manage access to applications and features, ensuring a consistent and controlled user experience across the network.

7.6.1 Notifications

7.6.1.1 Ensure 'Turn off notifications network usage' is set to 'Enabled'

This policy setting disables applications from using the network to send notifications for updating tiles, badges, toast, or raw notifications by turning off the connection between Windows and the Windows Push Notification Service (WNS). It also prevents applications from polling services to update tiles. The recommended state for this setting is: Enabled. In high-security environments, external systems, particularly those outside the organization, should be prevented from influencing secure workstations, making it important to block third-party notifications and updates from the cloud or Internet.

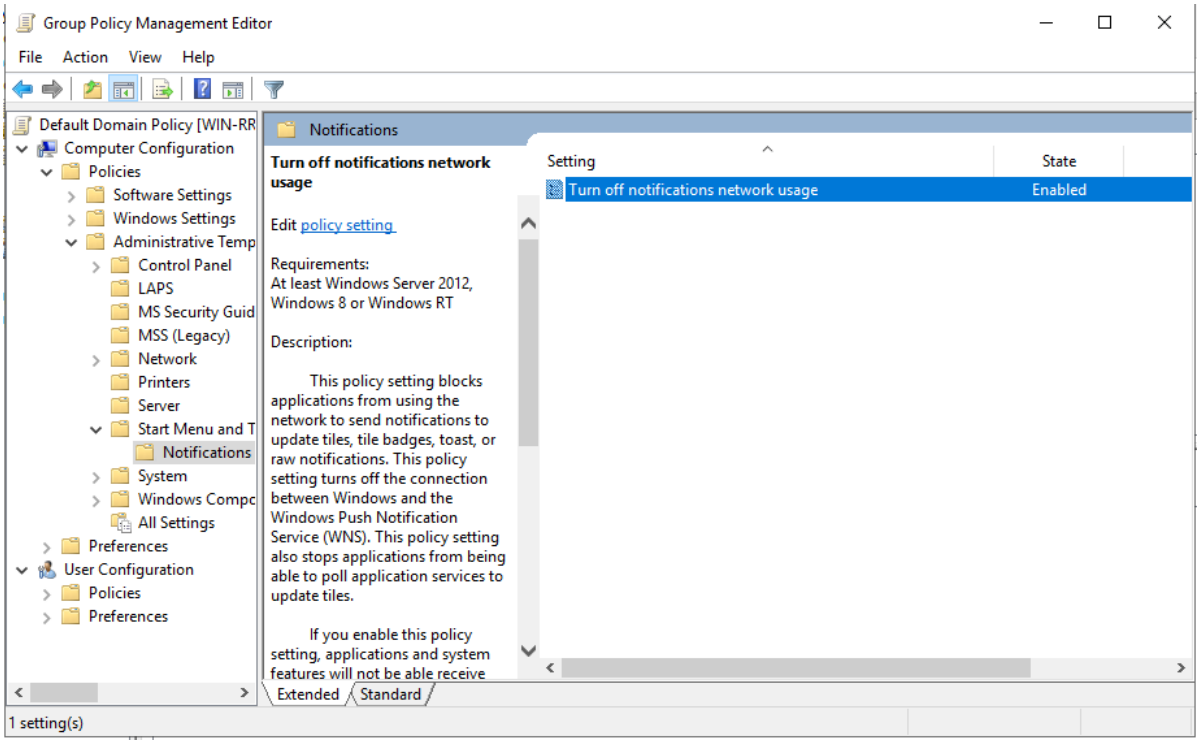


Image 200-Ensure 'Turn off notifications network usage' is set to 'Enabled'

7.7 System

The System Group Policy Section in Windows allows administrators to configure core system settings across multiple computers. It manages startup, shutdown procedures, security options, and system performance. By enforcing policies like automatic updates and security settings, it ensures consistency and compliance within a network.

7.7.1 Audit Process Creation

7.7.1.1 Ensure 'Include command line in process creation events' is set to 'Enabled'

This policy setting controls whether the process creation command line text is logged in security audit events when a new process is created. The recommended state is Enabled. Initially unsupported in older server OSes, Microsoft added this feature to Windows Server 2008 R2 and Windows Server 2012 (non-R2) through update KB3004375 in February 2015. Capturing command line information in event logs is crucial for forensic investigations during attack incidents.

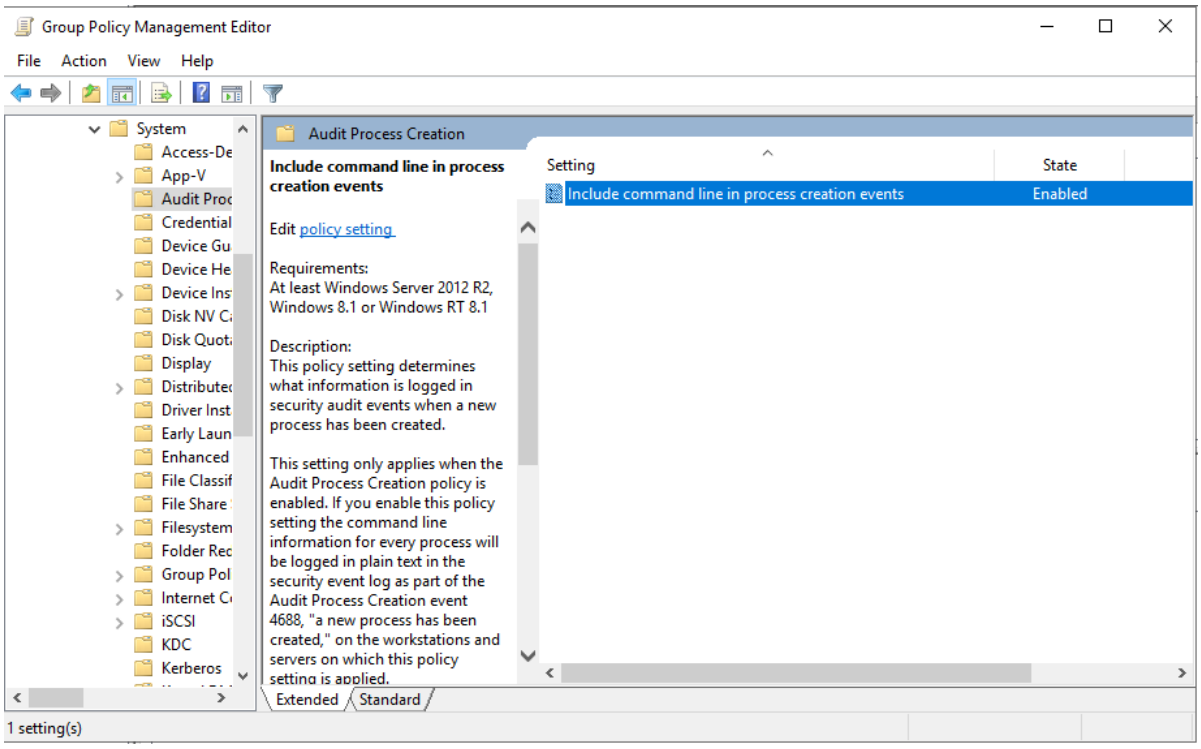


Image 201-Ensure 'Include command line in process creation events' is set to 'Enabled'

7.7.2 Credentials Delegation

7.7.2.1 Ensure 'Encryption Oracle Remediation' is set to 'Enabled: Force Updated Clients'

This policy setting addresses vulnerabilities in the CredSSP protocol, used by applications like Remote Desktop Connection, which are susceptible to an encryption oracle attack. It controls compatibility with vulnerable clients and servers and allows setting the desired protection level. The recommended state is Enabled: Force Updated Clients. This configuration is crucial to mitigate the CredSSP encryption oracle vulnerability, as detailed in CVE-2018-0886, affecting all Windows Server versions from Server 2008 onward, provided they have been patched through May 2018 or later.

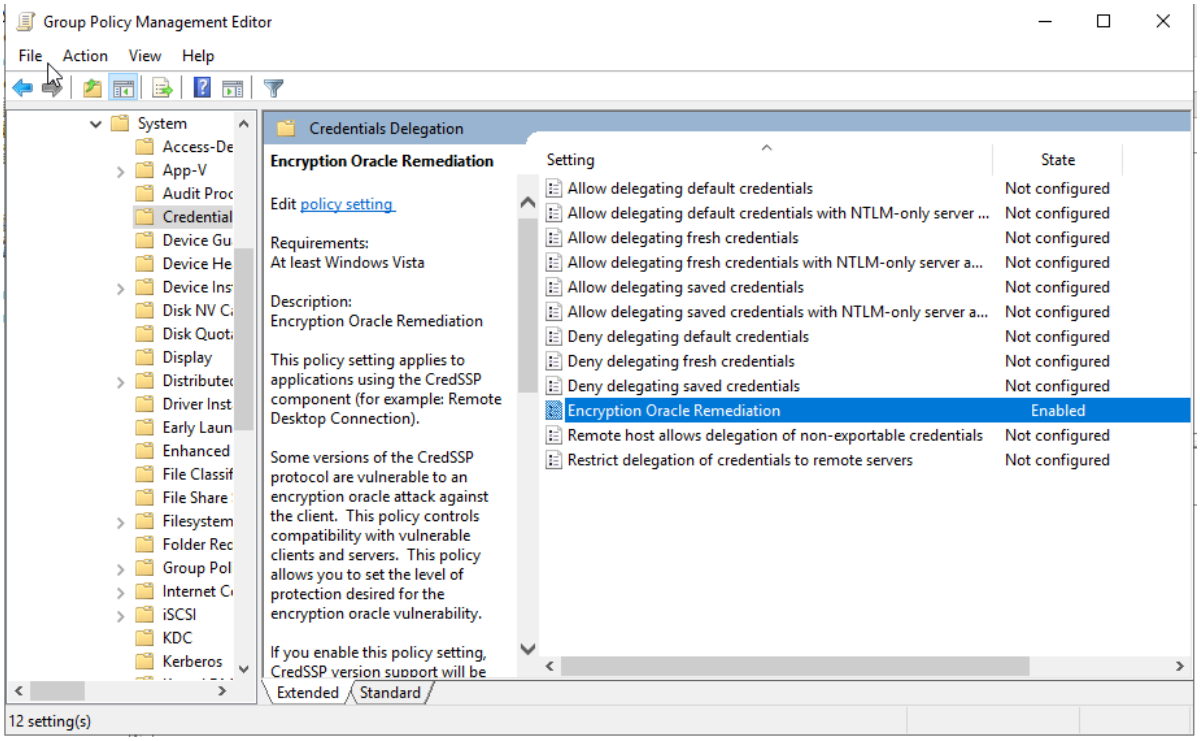


Image 202-Ensure 'Encryption Oracle Remediation' is set to 'Enabled: Force Updated Clients'

7.7.2.2 Ensure 'Remote host allows delegation of nonexportable credentials' is set to 'Enabled'

This policy setting prevents the delegation of non-exportable credentials to a remote host, reducing the risk of credential theft by attackers on the remote system. Enabling features like Restricted Admin Mode and Windows Defender Remote Credential Guard can provide protection by preventing reusable credentials from being stored on potentially compromised remote devices. The recommended state for this setting is Enabled. These features work together to mitigate the risk of credential theft during Remote Desktop sessions by redirecting Kerberos requests back to the initiating device.

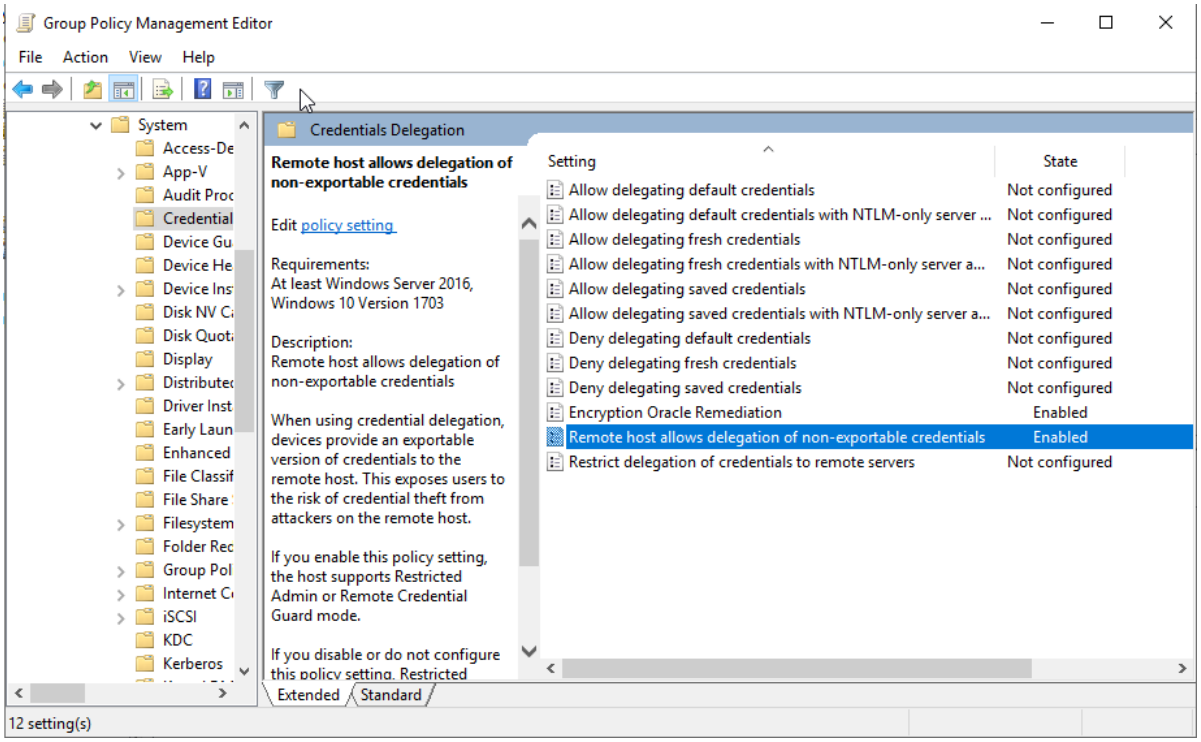


Image 203-Ensure 'Remote host allows delegation of non exportable credentials' is set to 'Enabled'

7.7.3 Device Guard

7.7.3.1 Ensure 'Remote host allows delegation of nonexportable credentials' is set to 'Enabled'

This policy setting determines whether Virtualization Based Security (VBS) is enabled, which uses the Windows Hypervisor to enhance security services. The recommended state is Enabled. VBS requires a 64-bit Windows version with Secure Boot and UEFI BIOS, and if used in a virtual machine, hardware-assisted CPU virtualization (Intel VT-x or AMD-V) must be enabled. VBS enhances security by isolating sensitive data, such as Kerberos, NTLM, and Credential Manager secrets, in a protected environment that isn't accessible to the rest of the operating system, improving protection against attacks.

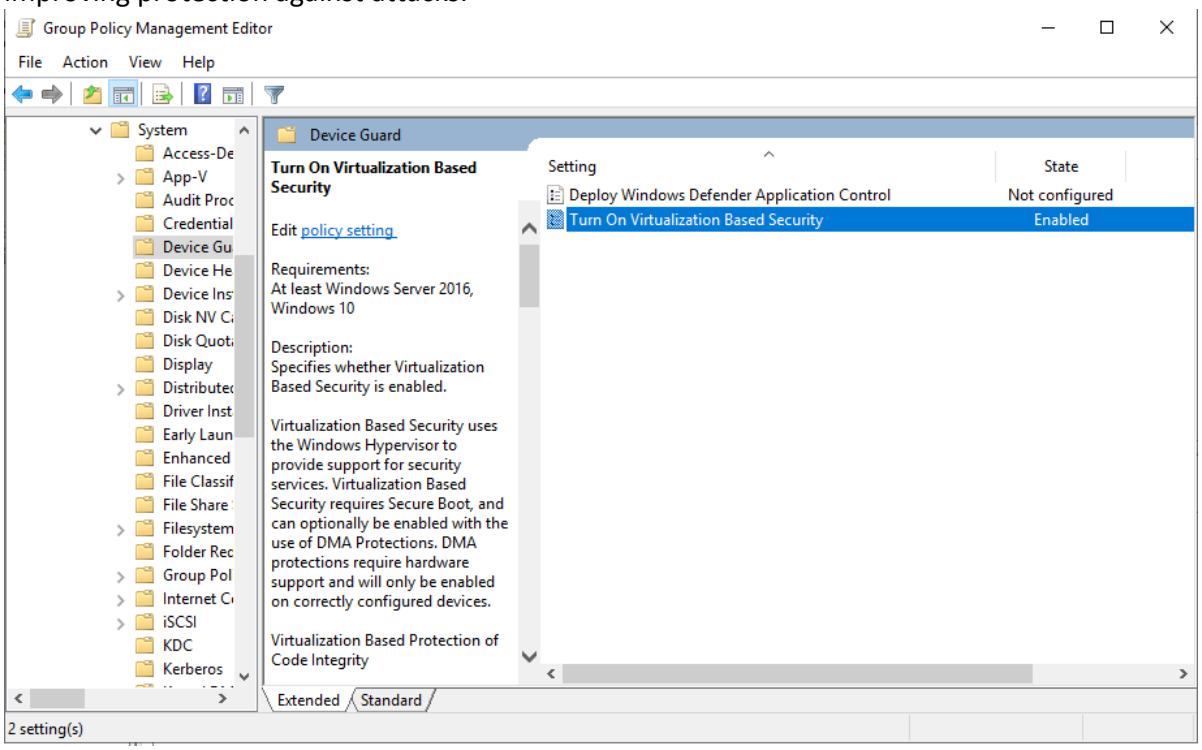


Image 204-Ensure 'Remote host allows delegation of non exportable credentials' is set to 'Enabled'

7.7.4 Device Installation

7.7.4.1 Ensure 'Prevent device metadata retrieval from the Internet' is set to 'Enabled'

This policy setting prevents Windows from retrieving device metadata from the Internet. The recommended state is Enabled. While it doesn't block the installation of basic hardware drivers, it does stop third-party utility software from automatically installing under the SYSTEM account. This is important because software installation should be managed by an authorized administrator to avoid unauthorized access through potential backdoors or software vulnerabilities.

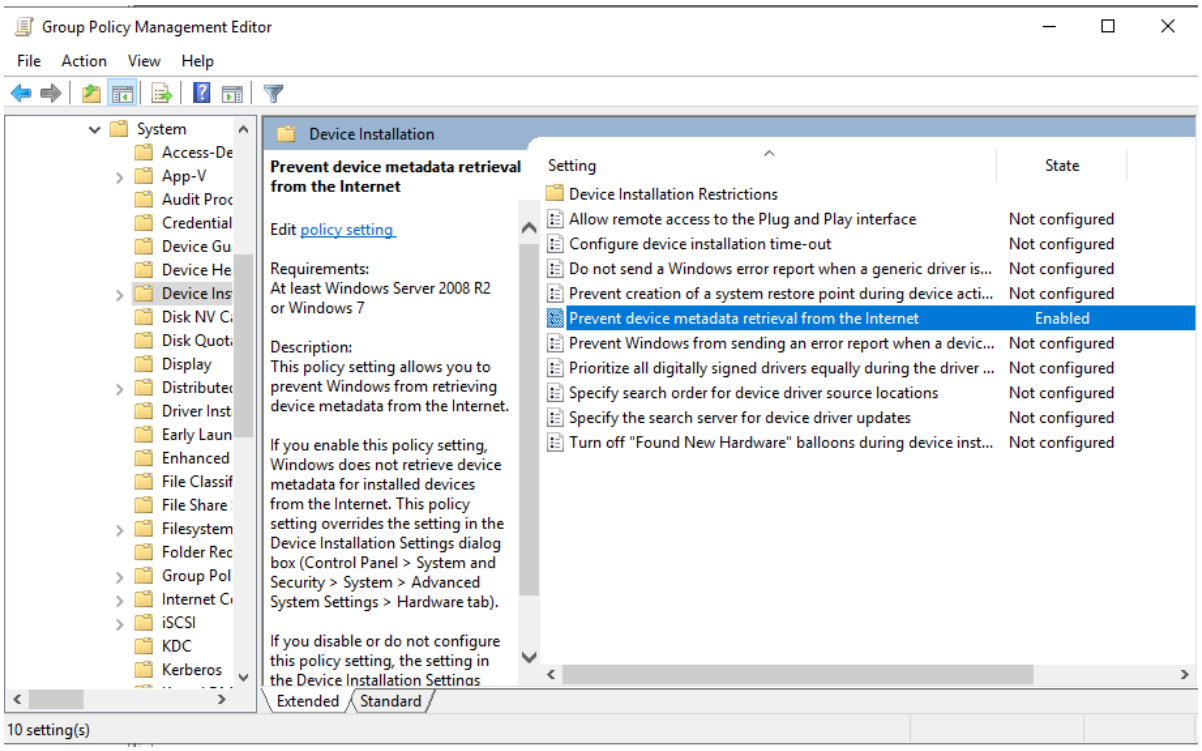


Image 205-Ensure 'Prevent device metadata retrieval from the Internet' is set to 'Enabled'

7.7.5 Early Launch Antimalware

7.7.5.1 Ensure 'Boot-Start Driver Initialization Policy' is set to 'Enabled: Good, unknown and bad but critical'

This policy setting allows you to control which boot-start drivers are initialized based on classifications determined by an Early Launch Antimalware (ELAM) boot-start driver. The classifications include Good (signed and untampered), Bad (identified as malware), Bad but required for boot (malware necessary for booting), and Unknown (unclassified by the malware detection application). If enabled, you can select which drivers to initialize on the next boot. If the malware detection application lacks an ELAM driver or if it's disabled, this setting won't affect boot-start drivers. The recommended state is Enabled: Good, Unknown, and Bad but critical drivers. This setting helps mitigate the impact of malware on your system.

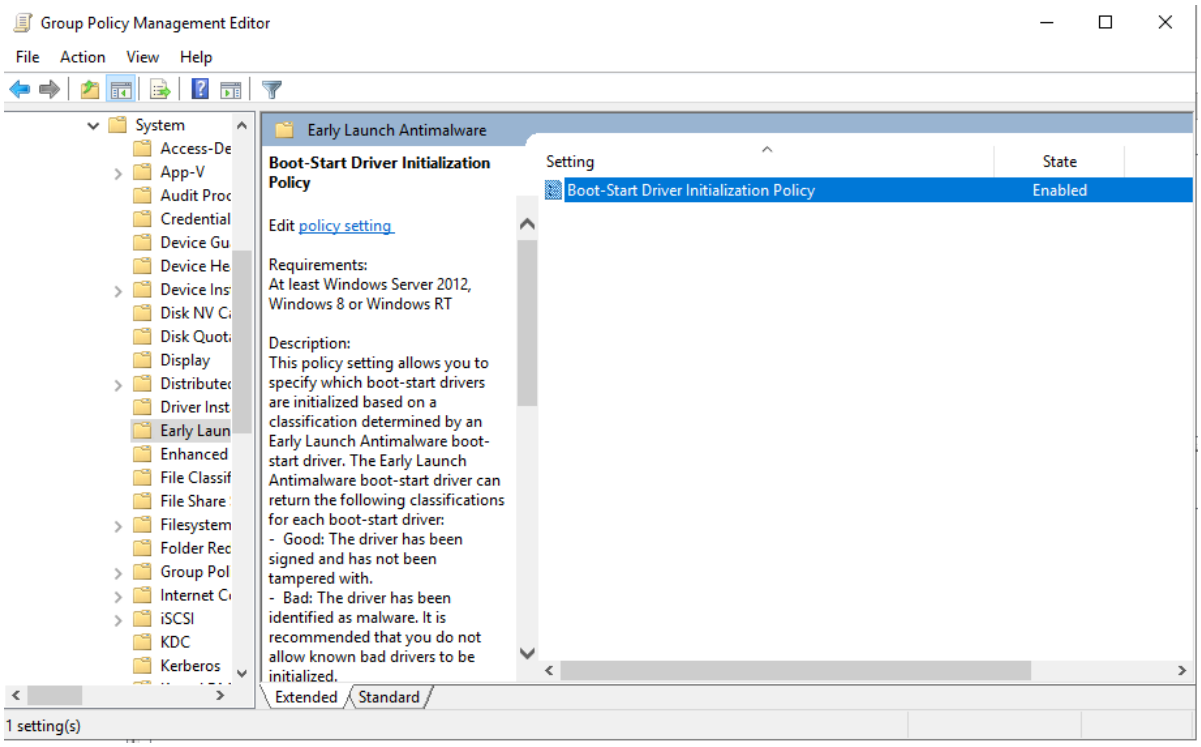


Image 206-Ensure 'Boot-Start Driver Initialization Policy' is set to 'Enabled: Good, unknown and bad but critical'

7.7.6 Group Policy

7.7.6.1 Ensure 'Continue experiences on this device' is set to 'Disabled'

This policy setting controls whether a Windows device can participate in cross-device experiences, where apps and messages are shared across devices. The recommended state is Disabled, as in an enterprise environment, only trusted systems should communicate within the network, and external system access should be restricted.

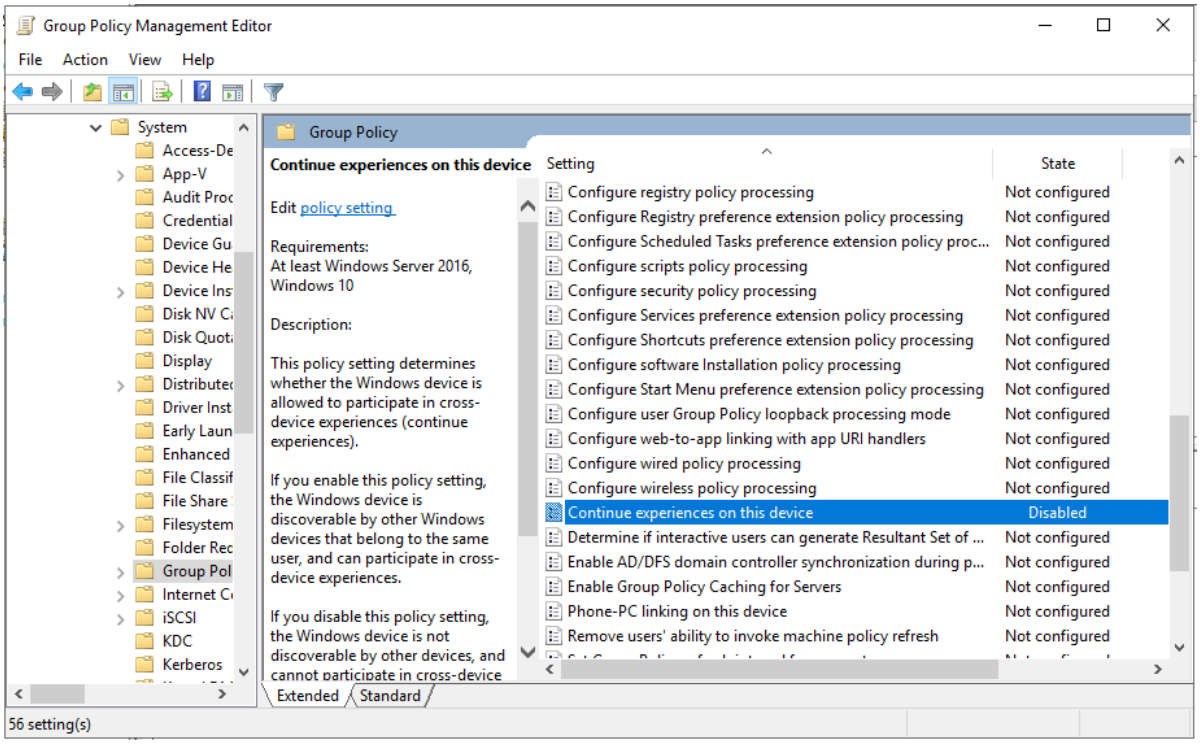


Image 207-Ensure 'Continue experiences on this device' is set to 'Disabled'

7.7.7 Internet Communication Management

7.7.7.1 Internet Communication settings

7.7.7.1.1 Ensure 'Turn off downloading of print drivers over HTTP' is set to 'Enabled'

This policy setting determines if the computer is allowed to download print driver packages via HTTP. This option is necessary for setting up HTTP printing when the required printer drivers are not included with the standard operating system installation. The recommended state for this setting is Enabled. This is advised to ensure that users can download necessary drivers, though it is crucial to be cautious as such drivers might contain malicious code.

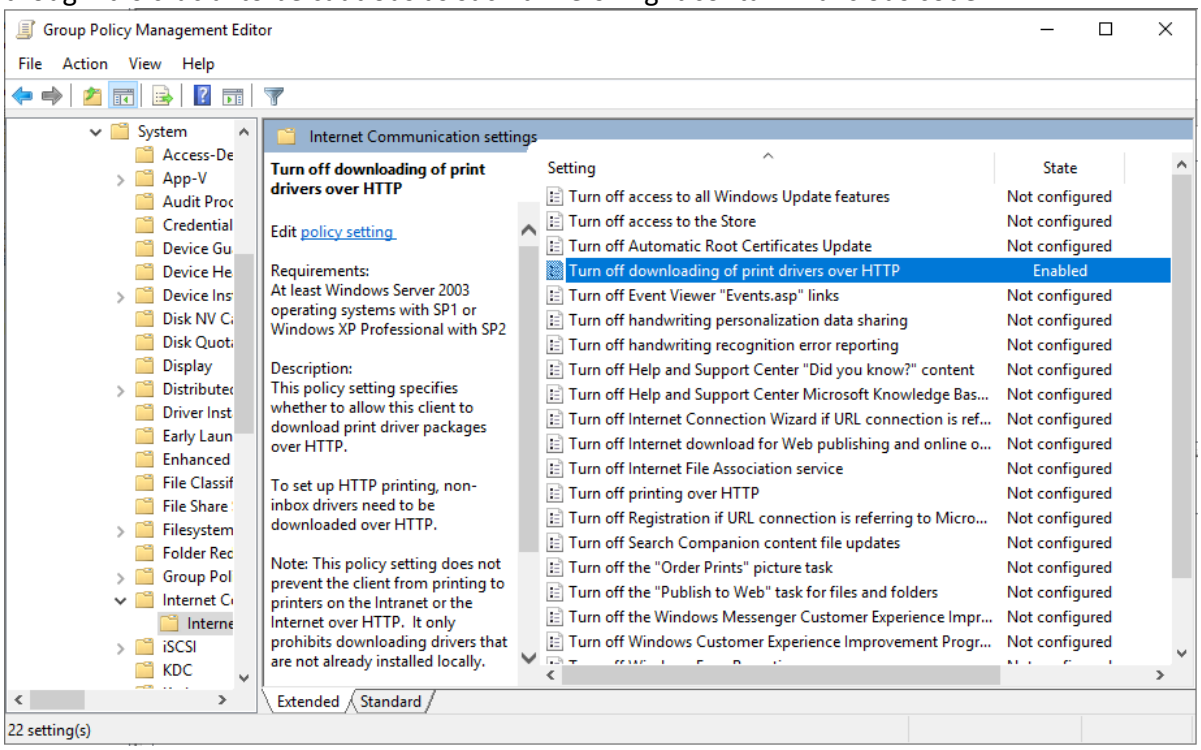


Image 208-Ensure 'Turn off downloading of print drivers over HTTP' is set to 'Enabled'

7.7.7.1.2 Ensure 'Turn off handwriting personalization data sharing' is set to 'Enabled'

This setting disables data sharing from the handwriting recognition personalization tool. This tool allows Tablet PC users to improve handwriting recognition by providing writing samples, which can be shared with Microsoft to enhance future versions of Windows. These samples are transmitted securely. The recommended state for this setting is Enabled. This is to ensure that personally identifiable information (PII), such as handwriting or signatures, is not automatically uploaded without explicit user consent, which is crucial in many environments.

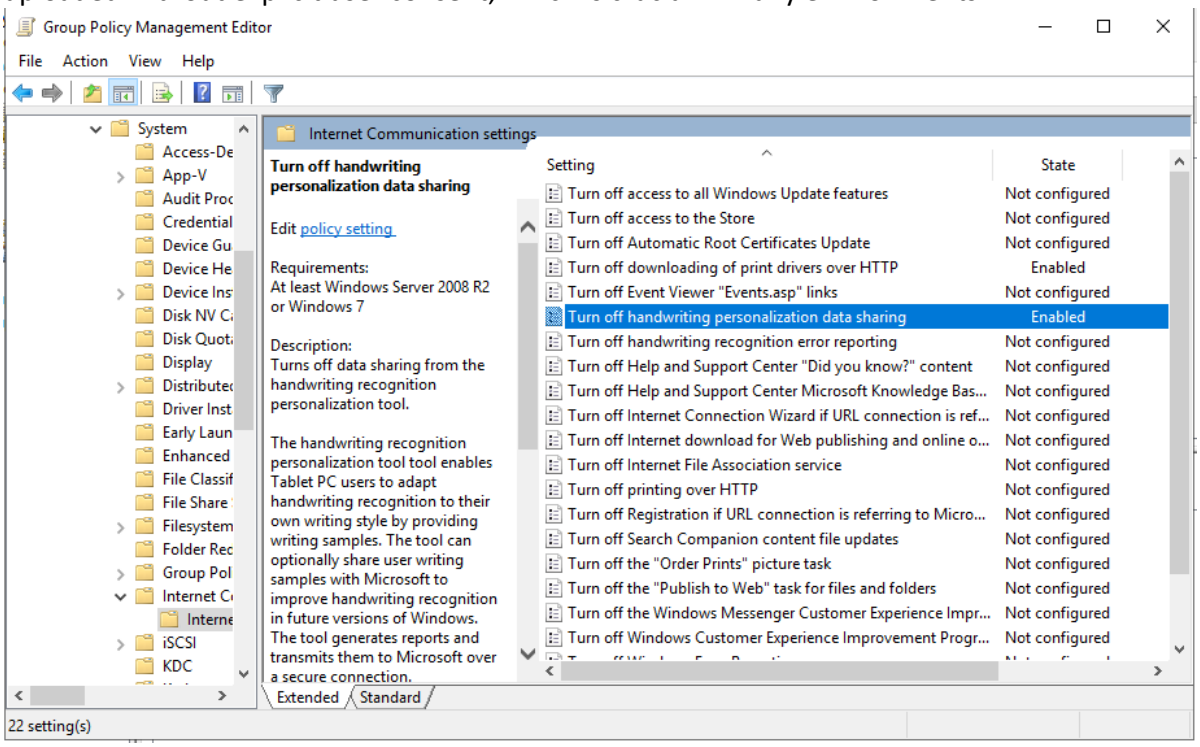


Image 209-Ensure 'Turn off handwriting personalization data sharing' is set to 'Enabled'

7.7.7.1.3 Ensure 'Turn off handwriting recognition error reporting' is set to 'Enabled'

This setting disables the handwriting recognition error reporting tool. This tool allows users to report errors encountered in the Tablet PC Input Panel, generating error reports that are securely sent to Microsoft. These reports are used by Microsoft to enhance handwriting recognition in future Windows versions. The recommended state for this setting is Enabled. This is to prevent the automatic upload of personally identifiable information (PII), such as handwriting or signatures, without explicit user consent, which is necessary in many environments.

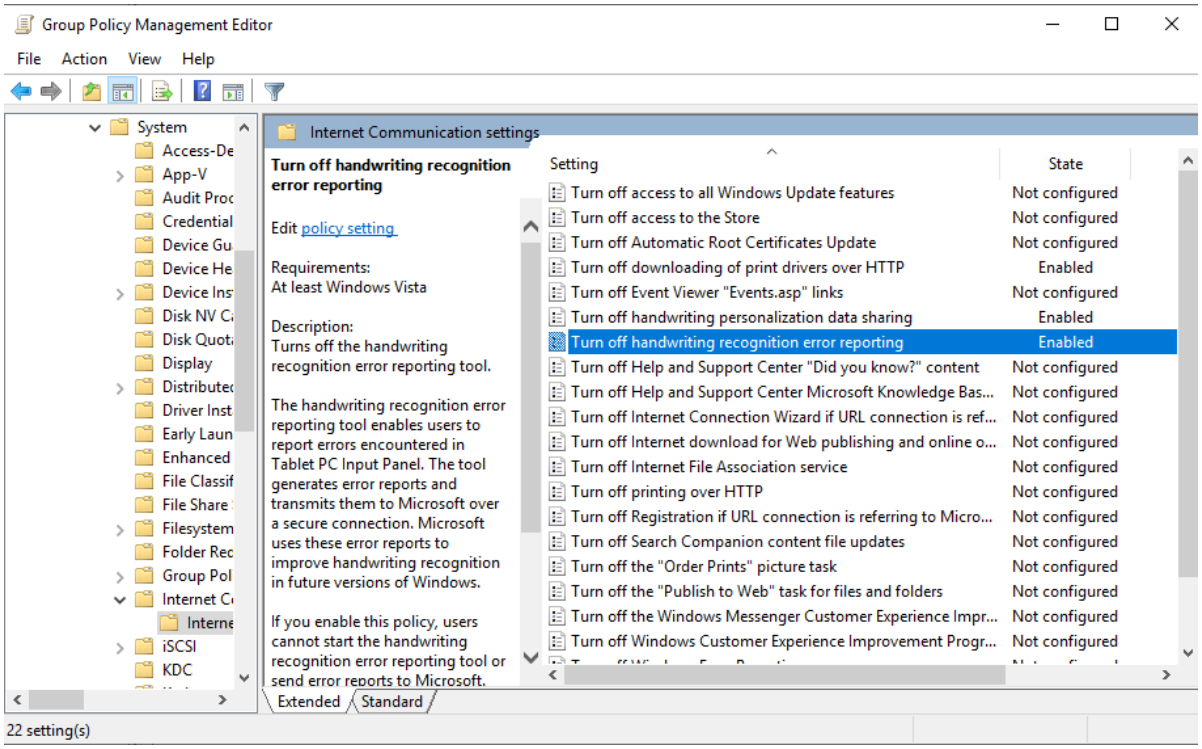


Image 210-Ensure 'Turn off handwriting recognition error reporting' is set to 'Enabled'

7.7.7.1.4 Ensure 'Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com' is set to 'Enabled'

This policy setting determines if the Internet Connection Wizard is permitted to connect to Microsoft to download a list of Internet Service Providers (ISPs). The recommended state for this setting is Enabled. This configuration helps mitigate the risk of users inadvertently exposing sensitive data in a managed enterprise environment.

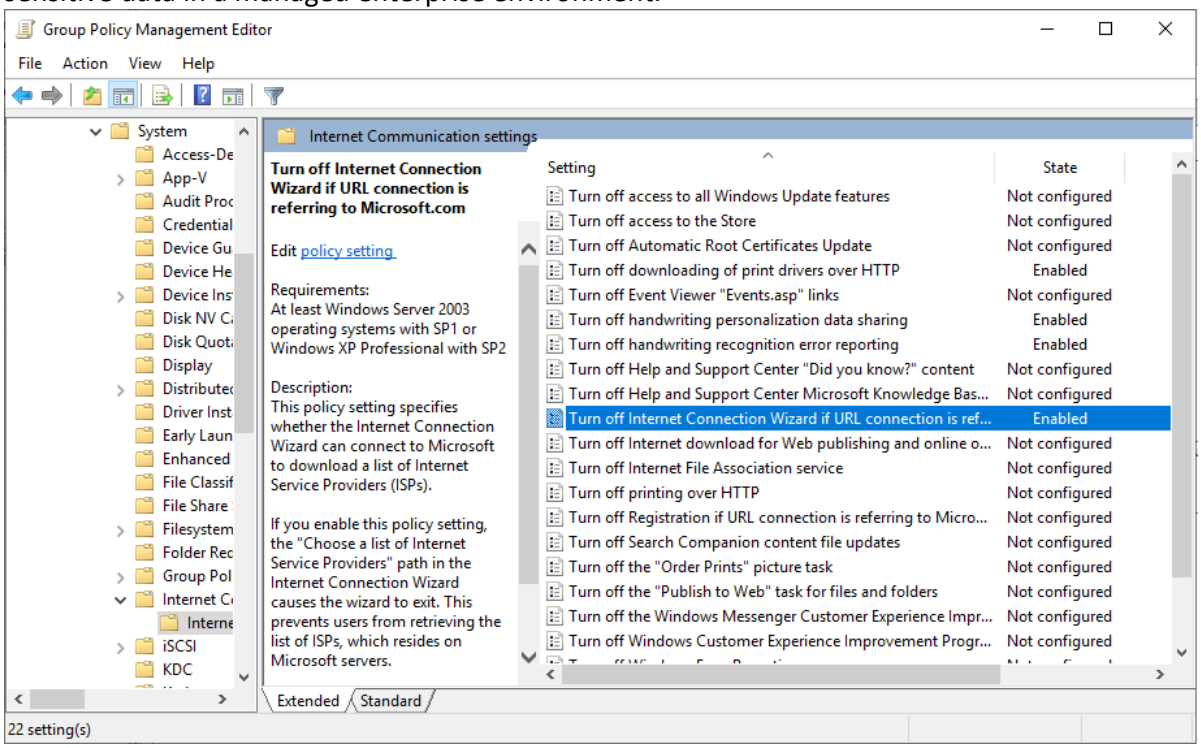


Image 211-Ensure 'Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com' is set to 'Enabled'

7.7.7.1.5 Ensure 'Turn off Internet download for Web publishing and online ordering wizards' is set to 'Enabled'

This policy setting regulates whether Windows will download a list of providers for the Web publishing and online ordering wizards. The recommended state for this setting is Enabled. This precaution minimizes the risk of users inadvertently downloading malicious content through this feature, even though the risk is generally low.

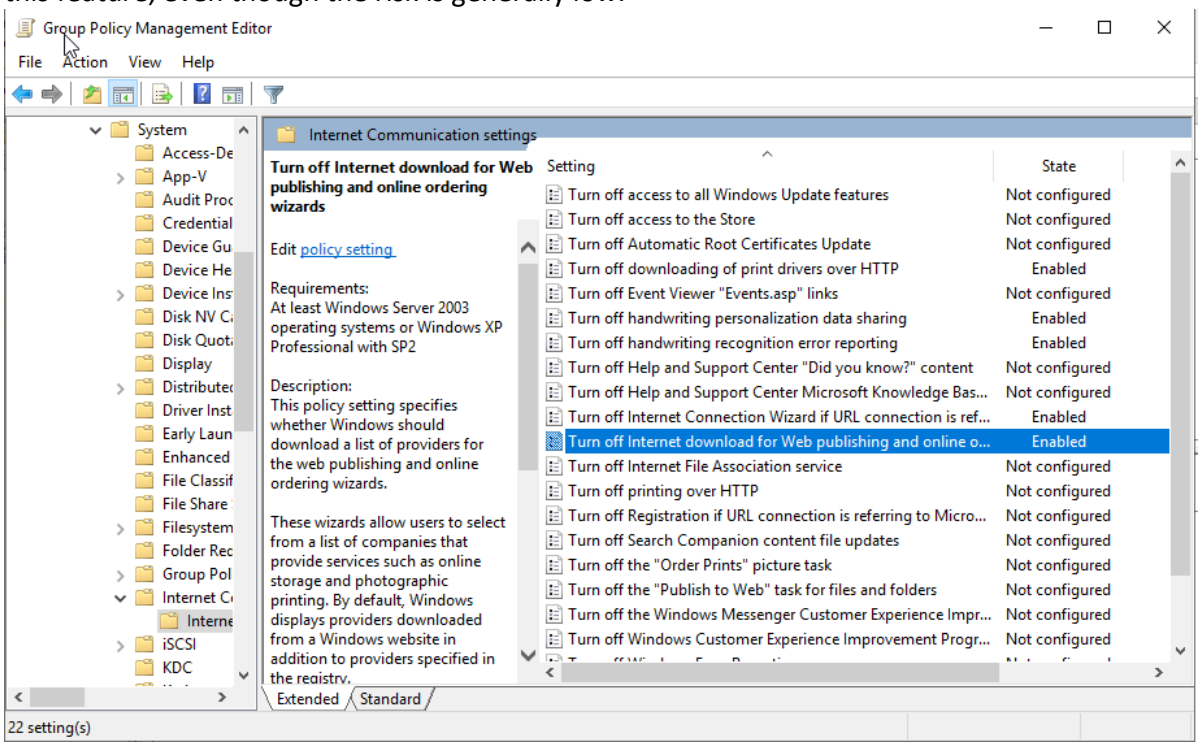


Image 212-Ensure 'Turn off Internet download for Web publishing and online ordering wizards' is set to 'Enabled'

7.7.7.1.6 Ensure 'Turn off printing over HTTP' is set to 'Enabled'

This policy setting permits the disabling of a client computer's ability to print over HTTP, which enables printing to printers both on the intranet and the Internet. The recommended state for this setting is Enabled. Note that this control impacts printing over both HTTP and HTTPS. The rationale is that information transmitted via HTTP is not secure and can be intercepted by malicious users, making this capability unsuitable for use in enterprise-managed environments.

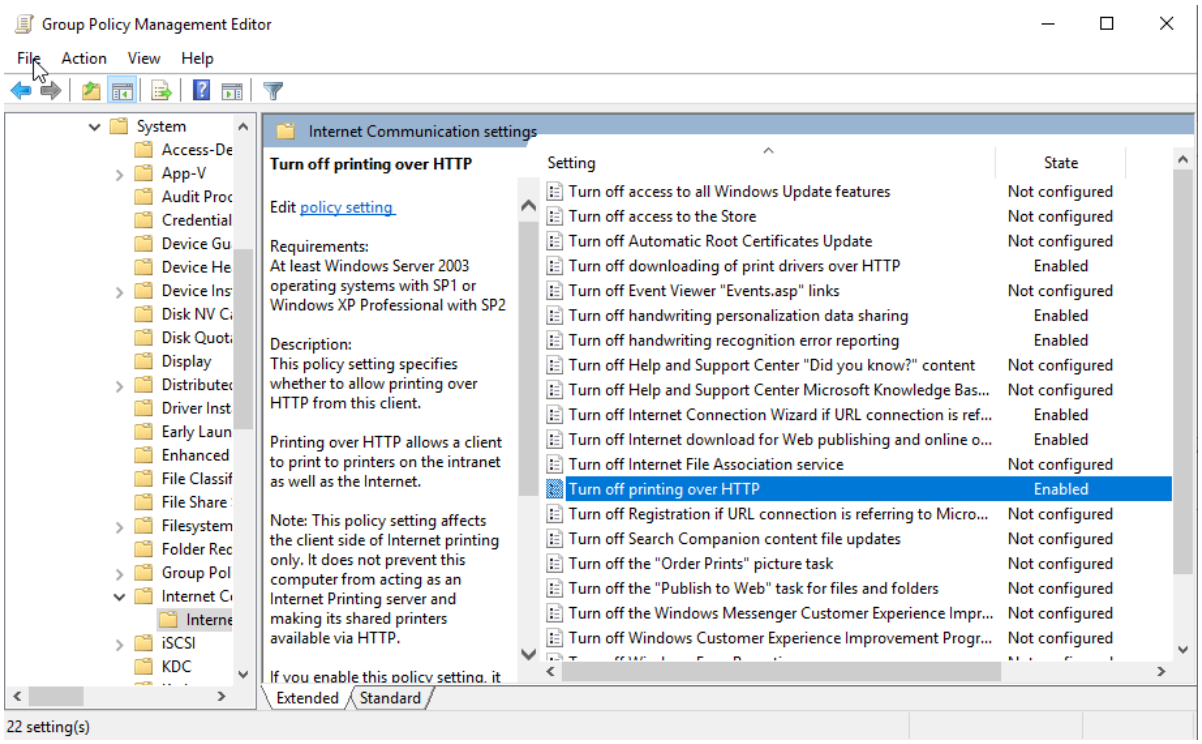


Image 213-Ensure 'Turn off printing over HTTP' is set to 'Enabled'

7.7.7.1.7 Ensure 'Turn off Registration if URL connection is referring to Microsoft.com' is set to 'Enabled'

This policy setting determines whether the Windows Registration Wizard connects to Microsoft.com for online registration. The recommended state for this setting is Enabled. The rationale is that in an enterprise-managed environment, users should not independently register their copies of Windows or provide their own personally identifiable information (PII).

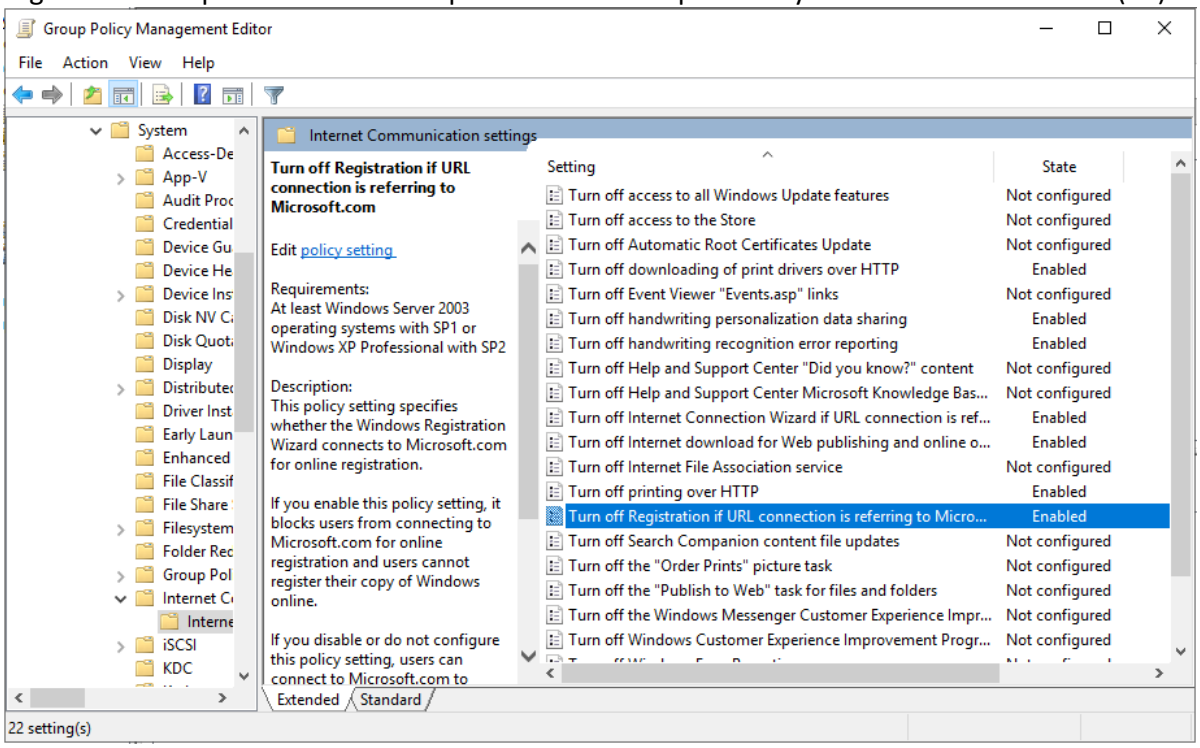


Image 214-Ensure 'Turn off Registration if URL connection is referring to Microsoft.com' is set to 'Enabled'

7.7.7.1.8 Ensure 'Turn off Search Companion content file updates' is set to 'Enabled'

This policy setting determines whether Search Companion is allowed to automatically download content updates during local and Internet searches. The recommended state for this setting is Enabled. The rationale is that although there is a slight risk of users unintentionally disclosing sensitive information based on their search topics, this risk remains minimal. Even with this setting enabled, users must still submit their search queries to the search engine to perform searches.

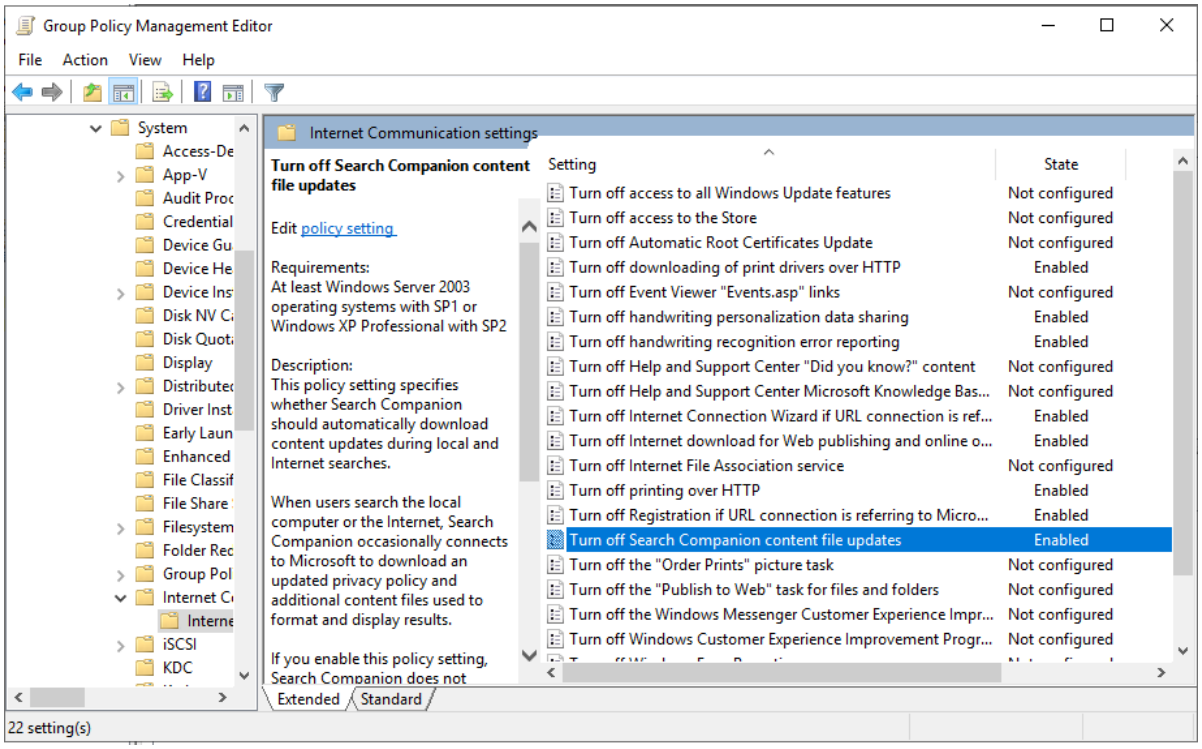


Image 215-Ensure 'Turn off Search Companion content file updates' is set to 'Enabled'

7.7.7.1.9 Ensure 'Turn off the "Order Prints" picture task' is set to 'Enabled'

This policy setting controls whether the "Order Prints Online" task appears in Picture Tasks within Windows folders. The Order Prints Online Wizard enables users to access a list of providers and place print orders online. The recommended state for this setting is Enabled. The rationale is that in an enterprise-managed environment, enabling this setting helps reduce the risk of users inadvertently exposing sensitive data.

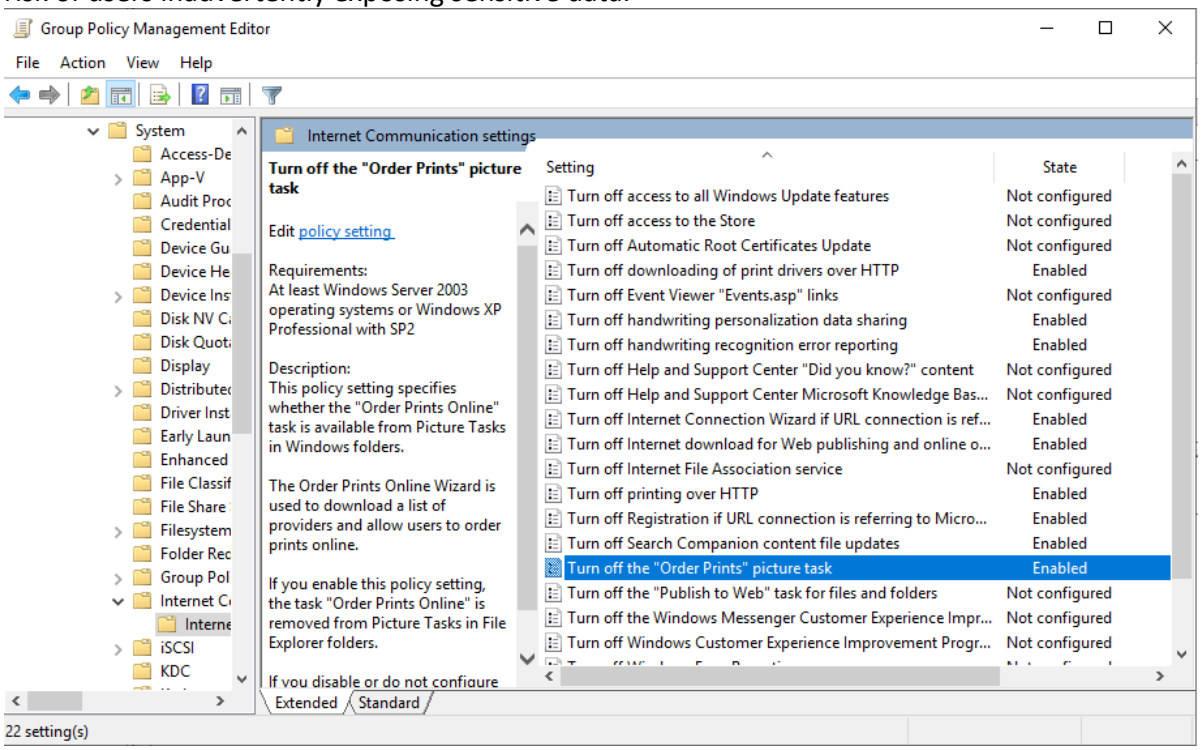


Image 216-Ensure 'Turn off the "Order Prints" picture task' is set to 'Enabled'

7.7.7.1.10 Ensure 'Turn off the "Publish to Web" task for files and folders' is set to 'Enabled'

This policy setting determines whether the tasks "Publish this file to the Web," "Publish this folder to the Web," and "Publish the selected items to the Web" are accessible from File and Folder Tasks in Windows folders. The recommended state for this setting is Enabled. The rationale behind this is to prevent users from inadvertently publishing confidential or sensitive information to public services outside the organization's control.

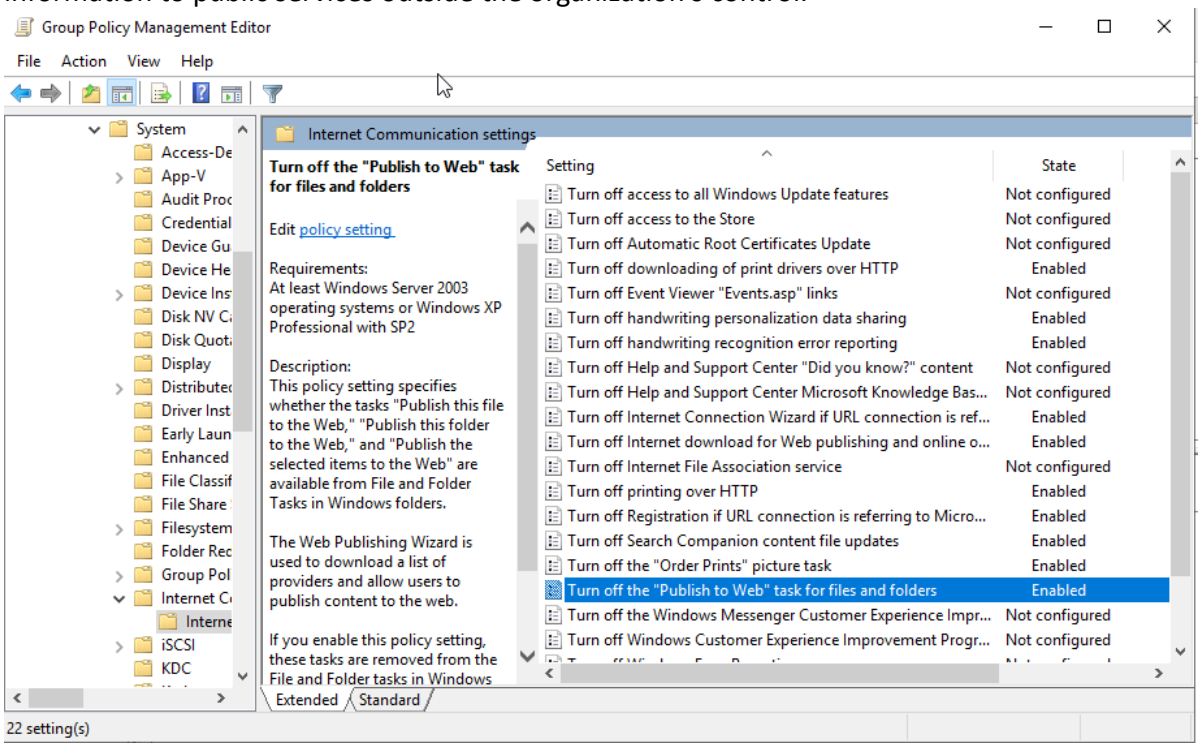


Image 217-Ensure 'Turn off the "Publish to Web" task for files and folders' is set to 'Enabled'

7.7.7.1.11 Ensure 'Turn off the Windows Messenger Customer Experience Improvement Program' is set to 'Enabled'

This policy setting determines if Windows Messenger is allowed to collect anonymous usage data. Microsoft uses this data, gathered through the Customer Experience Improvement Program, to identify and fix software issues more rapidly. Enabling this setting limits the amount of data Microsoft can collect for these purposes. The recommended state for this setting is Enabled. This is because large enterprise environments often prefer to prevent the collection of information from their managed client computers.

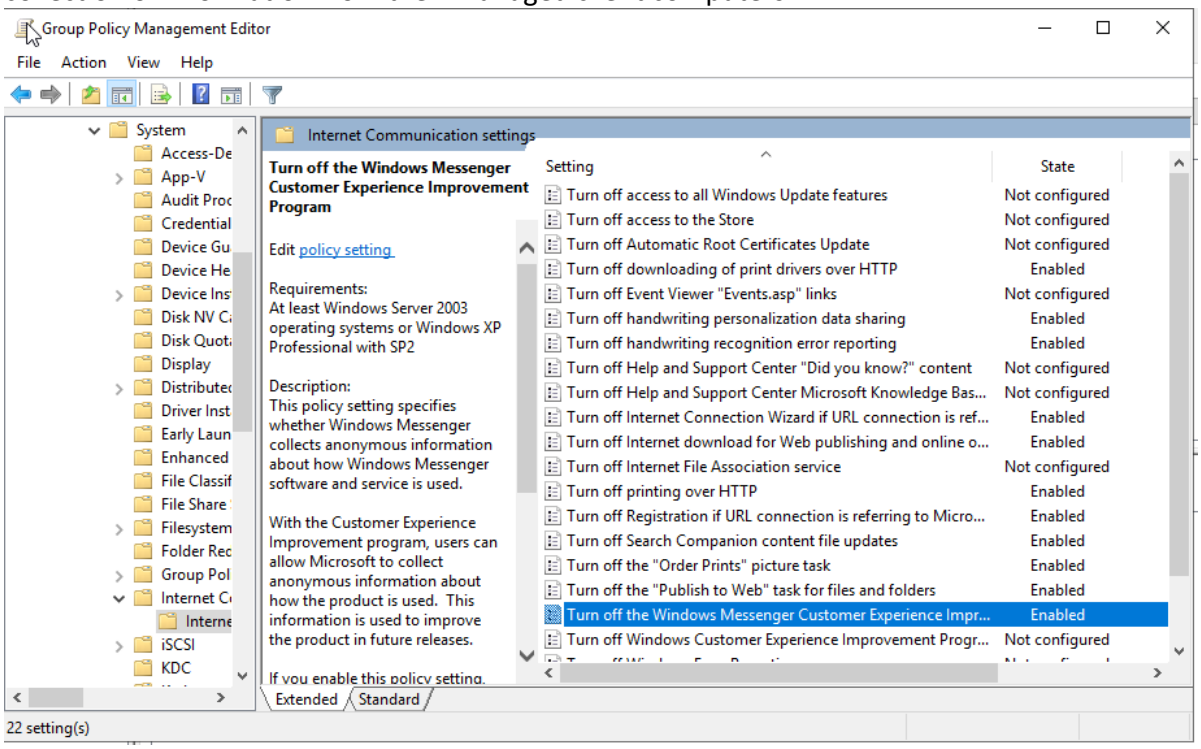


Image 218-Ensure 'Turn off the Windows Messenger Customer Experience Improvement Program' is set to 'Enabled'

7.7.7.1.12 Ensure 'Turn off Windows Customer Experience Improvement Program' is set to 'Enabled'

This policy setting determines whether the Windows Customer Experience Improvement Program can collect anonymous data on how Windows is used. Microsoft utilizes this data to enhance frequently used features and to identify and address software issues more efficiently. Enabling this setting will limit the amount of data Microsoft can collect for these purposes. The recommended state for this setting is Enabled, as large enterprise environments often prefer to restrict data collection from their managed client computers.

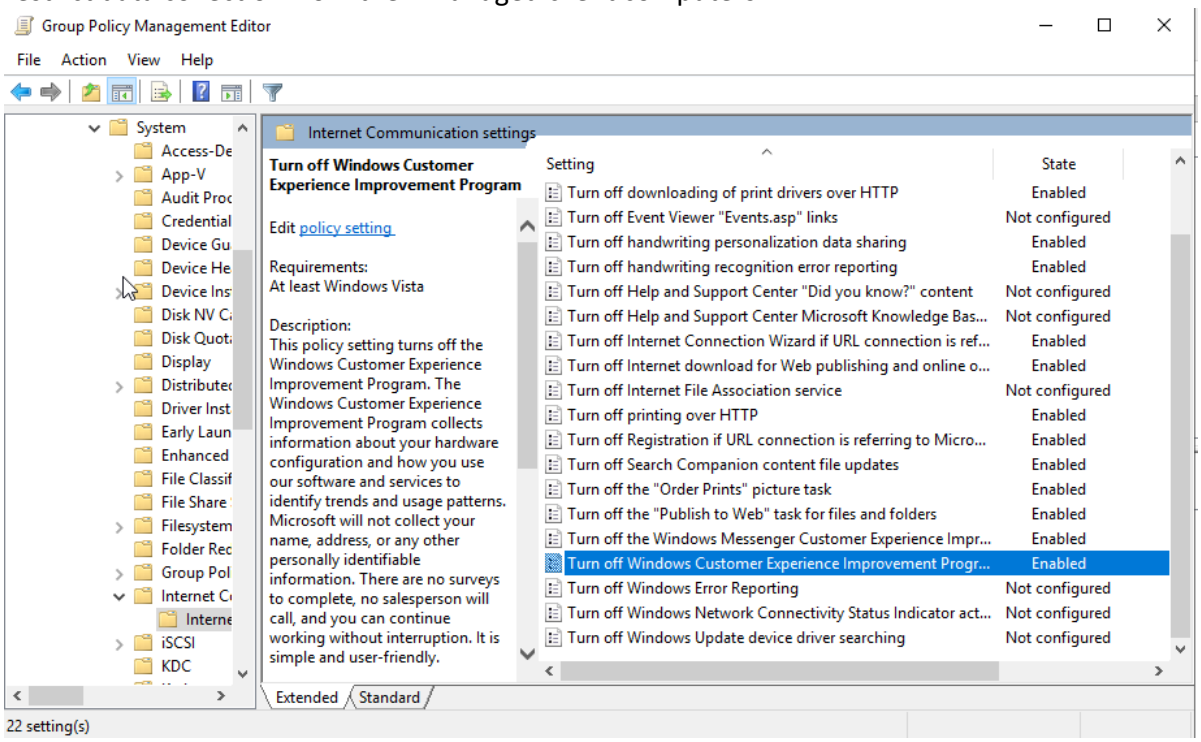


Image 219-Ensure 'Turn off Windows Customer Experience Improvement Program' is set to 'Enabled'

7.7.7.1.13 Ensure 'Turn off Windows Error Reporting' is set to 'Enabled'

This policy setting determines whether errors are reported to Microsoft. Error Reporting provides information about system or application failures to help improve product quality. The recommended state for this setting is Enabled. In a secure, enterprise-managed environment, errors should be reported directly to IT staff for troubleshooting and resolution, rather than being sent to Microsoft. Reporting errors directly to Microsoft does not benefit the corporation and may risk inadvertently disclosing sensitive data.

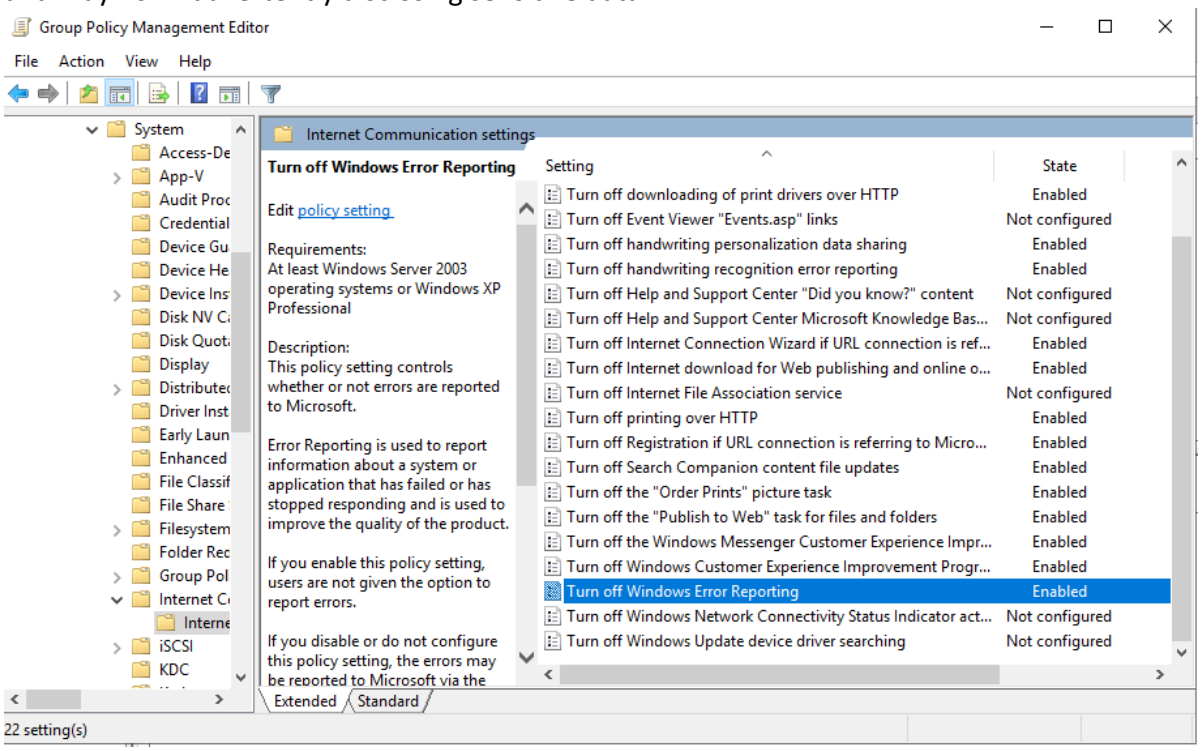


Image 220-Ensure 'Turn off Windows Error Reporting' is set to 'Enabled'

7.7.8 Kerberos

7.7.8.1 Ensure 'Support device authentication using certificate' is set to 'Enabled: Automatic'

This policy setting enables the use of certificates for Kerberos authentication to the domain. Device authentication with certificates requires connectivity to a domain controller that supports certificate authentication for computer accounts. The recommended configuration for this setting is Enabled: Automatic. Using certificate-based authentication provides stronger security compared to traditional username and password methods, and setting it to Automatic ensures that certificate-based authentication is used whenever possible.

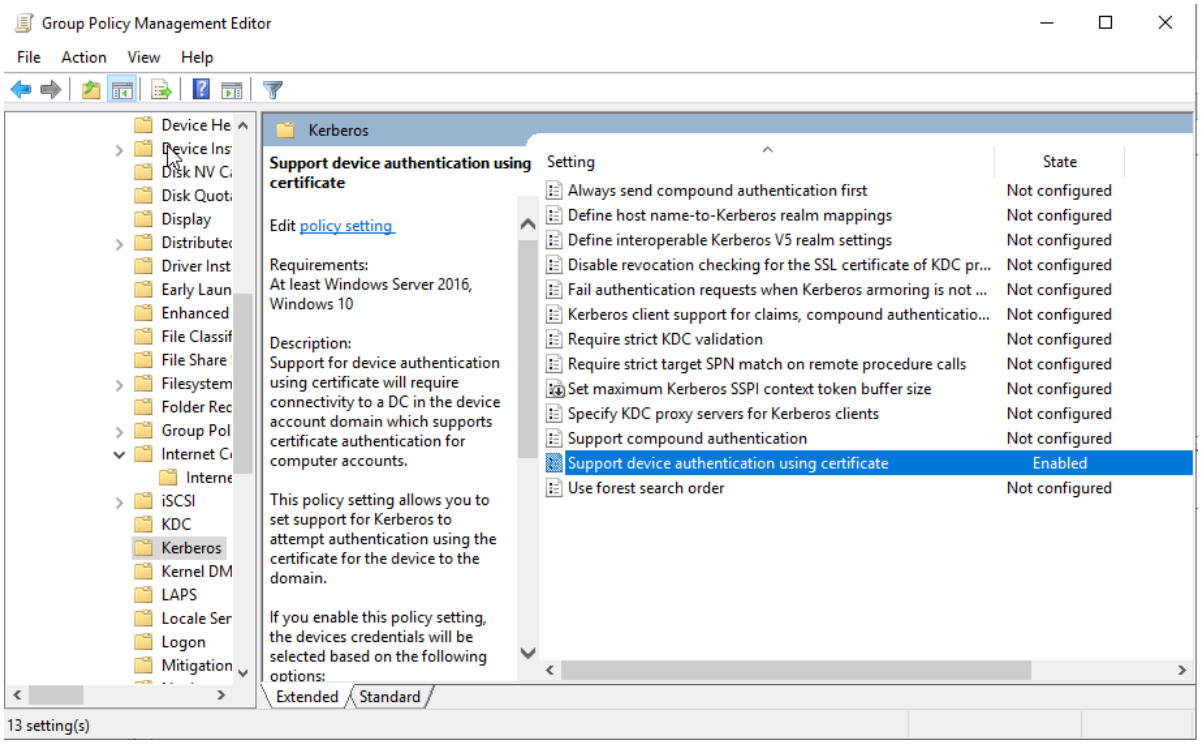


Image 221-Ensure 'Support device authentication using certificate' is set to 'Enabled: Automatic'

7.7.9 Kernel DMA Protection

7.7.9.1 Ensure 'Support device authentication using certificate' is set to 'Enabled: Automatic'

This policy aims to enhance security against external Direct Memory Access (DMA) devices by providing greater control over the detection and management of external DMA-capable devices that lack DMA Remapping, device memory isolation, and sandboxing capabilities. The recommended configuration for this setting is Enabled: Block All. Note that this policy does not apply to 1394, PCMCIA, or ExpressCard devices and is effective only on Windows 10 version R1803 or later, with a UEFI BIOS required for functionality. For additional details, see: Kernel DMA Protection for Thunderbolt™ 3 (Windows 10) | Microsoft Docs. The rationale behind this policy is that device memory sandboxing uses the I/O Memory Management Unit (IOMMU) to prevent unauthorized I/O or memory access by peripherals.

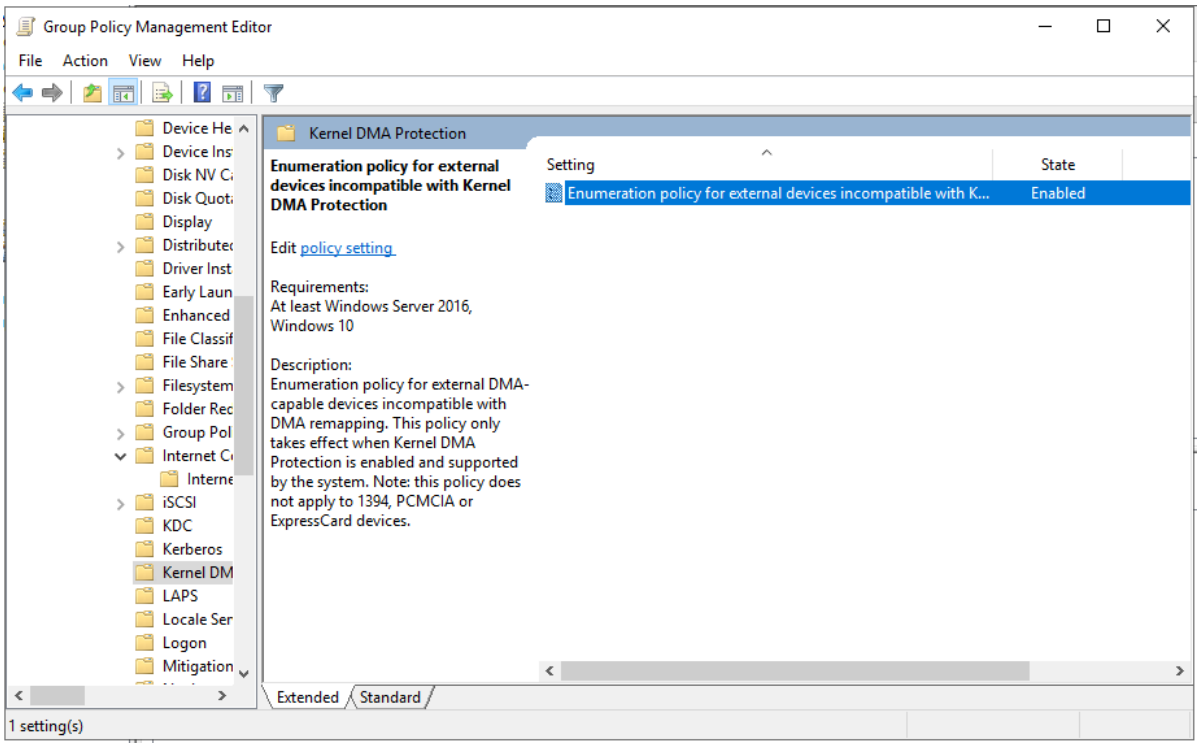


Image 222-Ensure 'Support device authentication using certificate' is set to 'Enabled: Automatic'

7.7.10 Locale Services

7.7.10.1 Ensure 'Disallow copying of user input methods to the system account for sign-in' is set to 'Enabled'

This policy restricts the automatic transfer of user input methods to the system account for use on the sign-in screen, ensuring that only the input methods enabled in the system account are available. The recommended configuration for this setting is Enabled. This approach enhances the security of the system account by limiting the input methods accessible during sign-in.

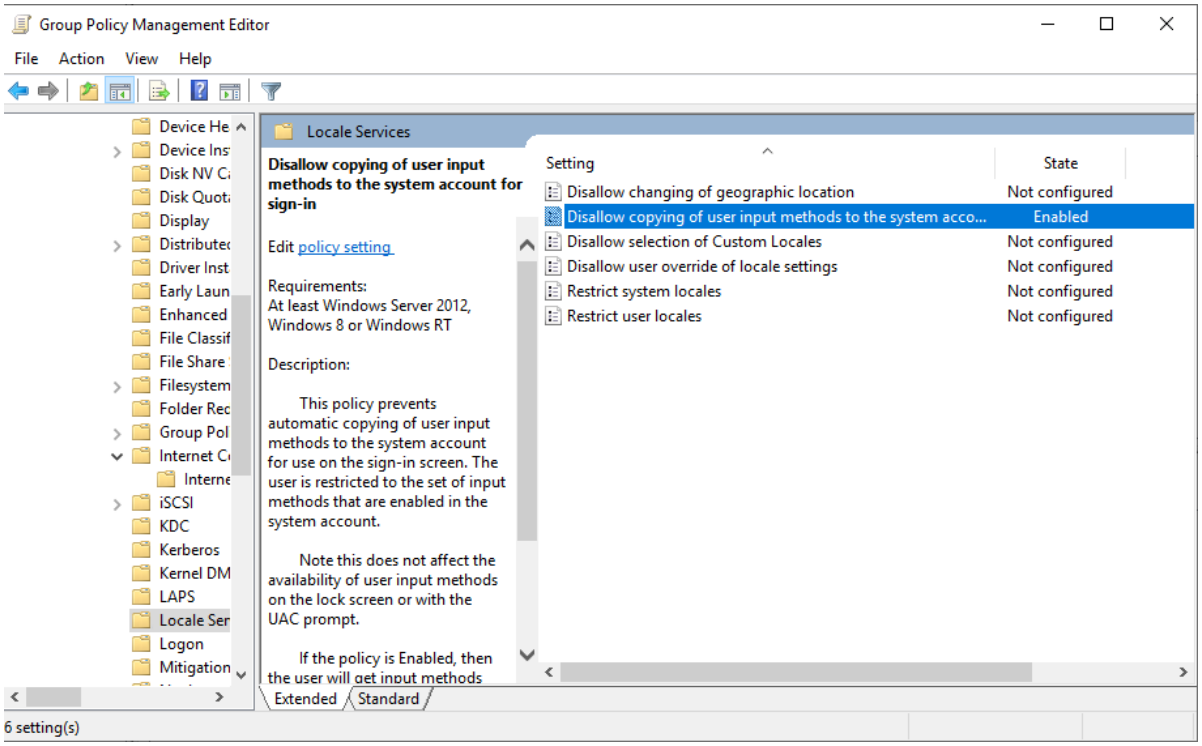


Image 223-Ensure 'Disallow copying of user input methods to the system account for sign-in' is set to 'Enabled'

7.7.11 Logon

7.7.11.1 Ensure 'Block user from showing account details on sign-in' is set to 'Enabled'

This policy prevents displaying account details, such as email addresses or usernames, on the sign-in screen. The recommended configuration for this setting is Enabled. This measure helps protect against potential attackers who might gain physical access to the console or connect via Remote Desktop Services and attempt to guess or brute-force the password based on the visible username of the last logged-in user.

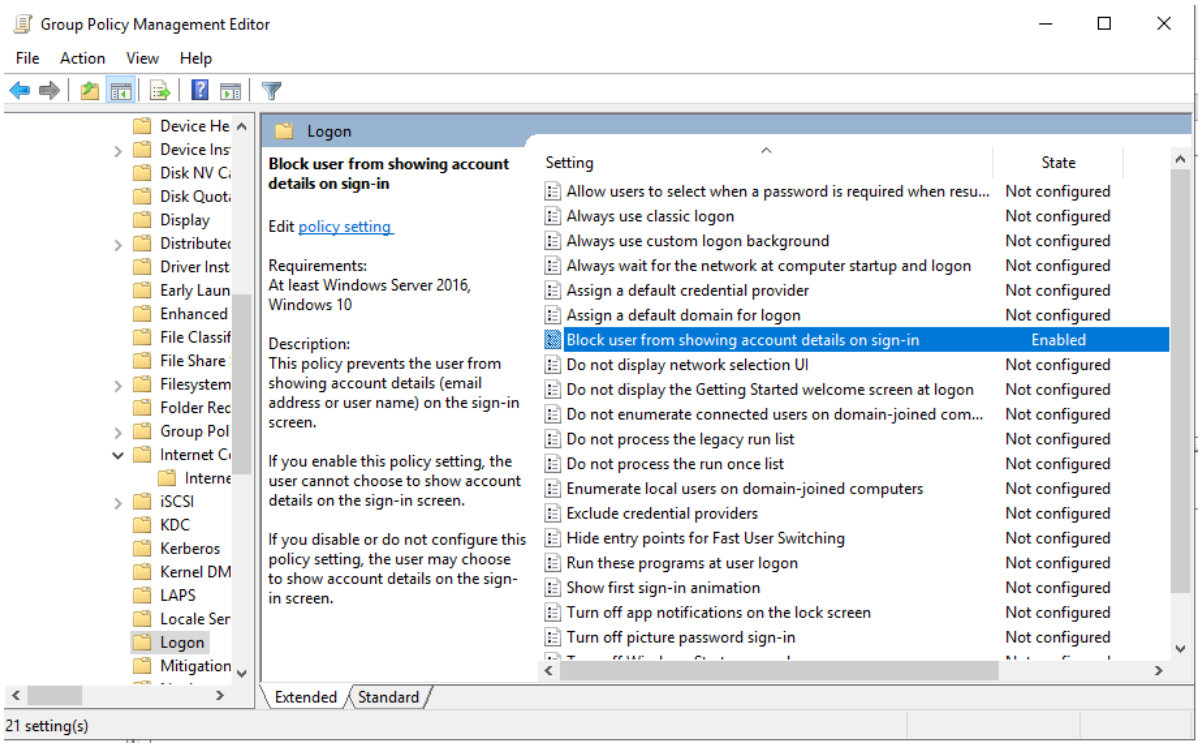


Image 224-Ensure 'Block user from showing account details on sign-in' is set to 'Enabled'

7.7.11.2 Ensure 'Do not display network selection UI' is set to 'Enabled'

This policy setting determines whether users can access and interact with network options on the logon screen. The recommended configuration is Enabled. This setting helps prevent unauthorized individuals from disconnecting the PC from its network or connecting it to different networks without first logging into Windows.

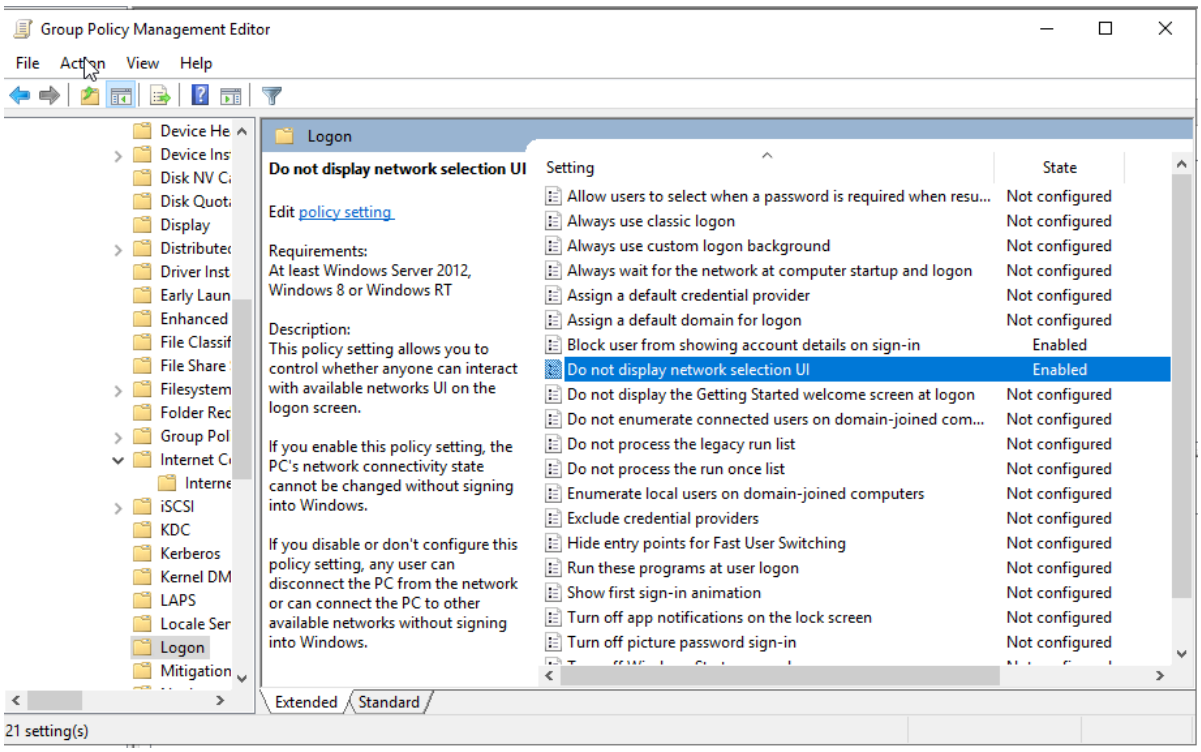


Image 225-Ensure 'Do not display network selection UI' is set to 'Enabled'

7.7.11.3 Ensure 'Turn off app notifications on the lock screen' is set to 'Enabled'

This policy setting controls whether app notifications are shown on the lock screen. The recommended configuration is Enabled. This helps protect sensitive business or personal information that might otherwise be displayed in notifications on the lock screen.

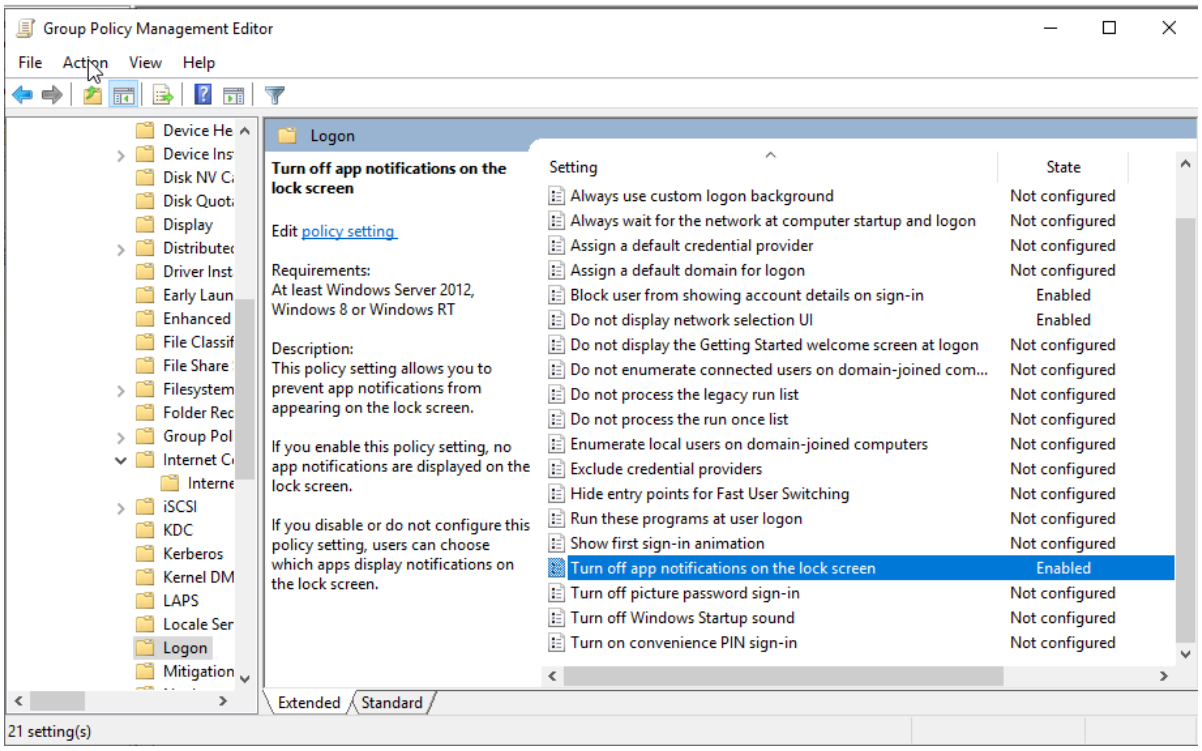


Image 226-Ensure 'Turn off app notifications on the lock screen' is set to 'Enabled'

7.7.11.4 Ensure 'Turn on convenience PIN sign-in' is set to 'Disabled'

This policy setting determines whether domain users can sign in using a convenience PIN. In Windows 10, the convenience PIN feature was replaced by Passport, which offers enhanced security. For configuring Passport for domain users, refer to the policies under Computer Configuration\Administrative Templates\Windows Components\Microsoft Passport for Work. Note that using this feature will cache the user's domain password in the system vault. The recommended state for this setting is Disabled. This is because a PIN, which uses a limited set of characters, is generally less secure than a password.

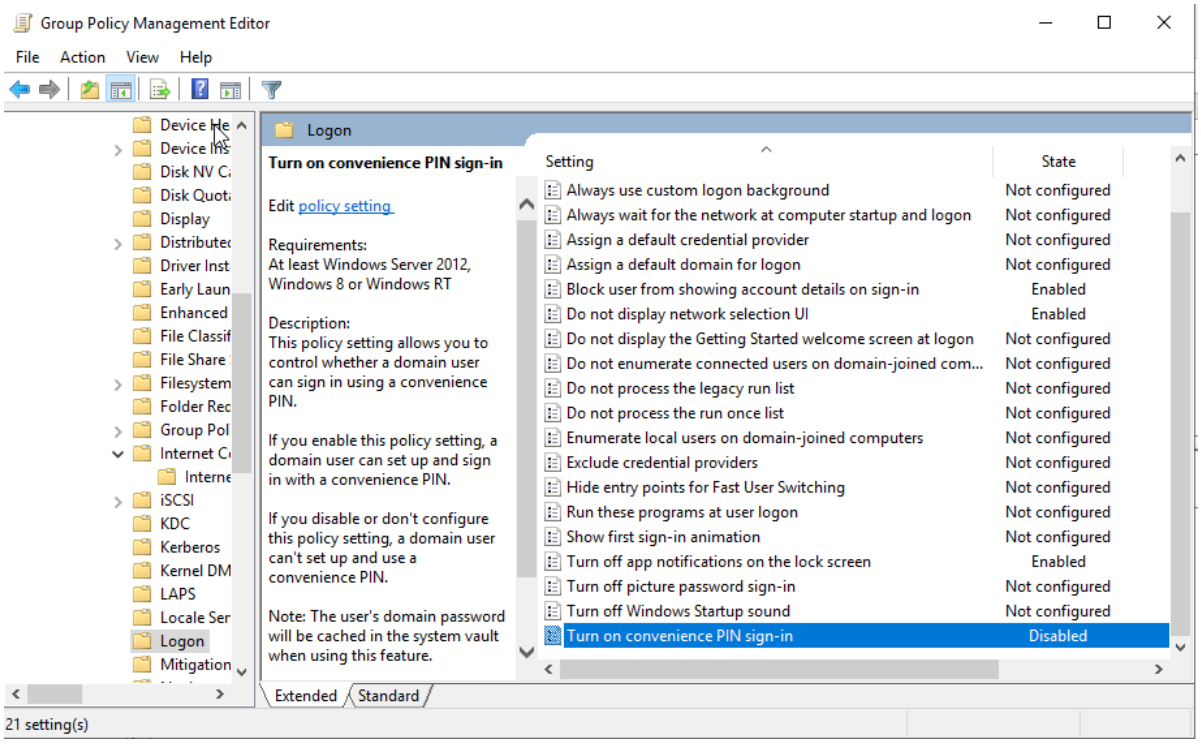


Image 227-Ensure 'Turn on convenience PIN sign-in' is set to 'Disabled'

7.7.12 OS Policies

7.7.12.1 Ensure 'Allow Clipboard synchronization across devices' is set to 'Disabled'

This policy setting controls whether Clipboard contents can be synchronized across devices. The recommended state for this setting is Disabled. This is because, for privacy reasons, clipboard data should remain local to the system and not be shared across devices.

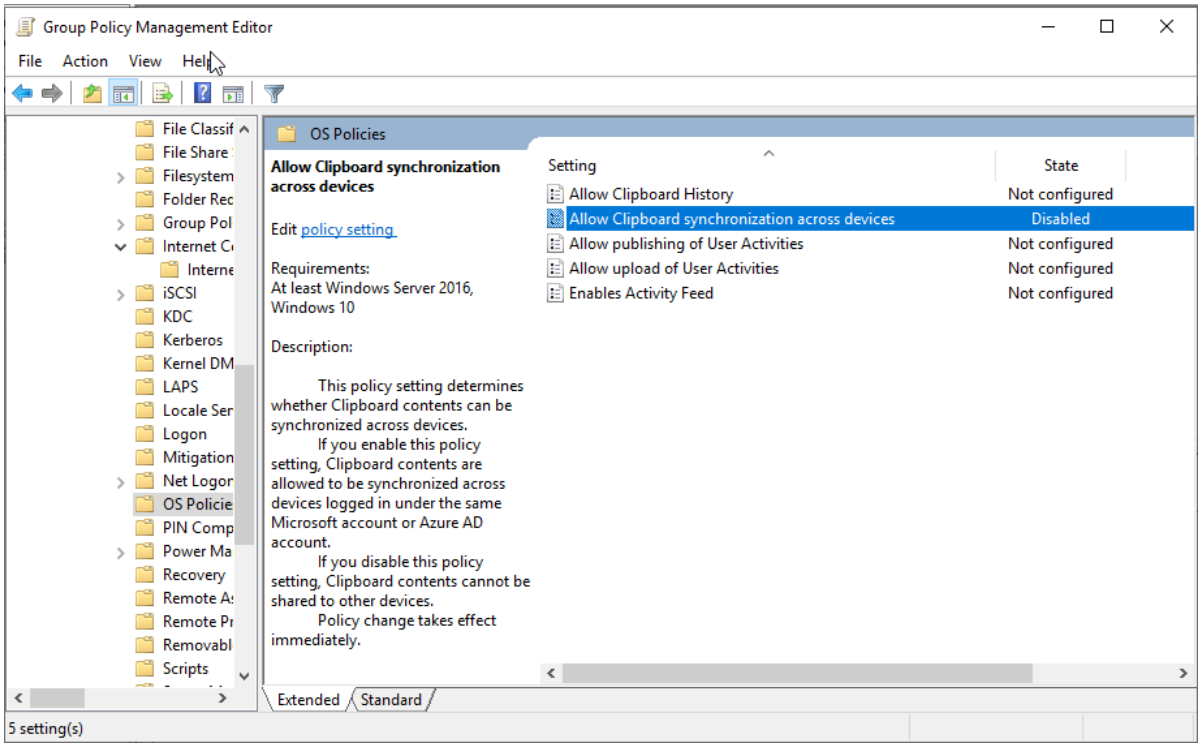


Image 228-Ensure 'Allow Clipboard synchronization across devices' is set to 'Disabled'

7.7.12.2 Ensure 'Allow upload of User Activities' is set to 'Disabled'

This policy setting controls whether published User Activities can be uploaded to the cloud. The recommended state for this setting is Disabled. This is due to privacy concerns, as sending this data to third parties could potentially expose sensitive information.

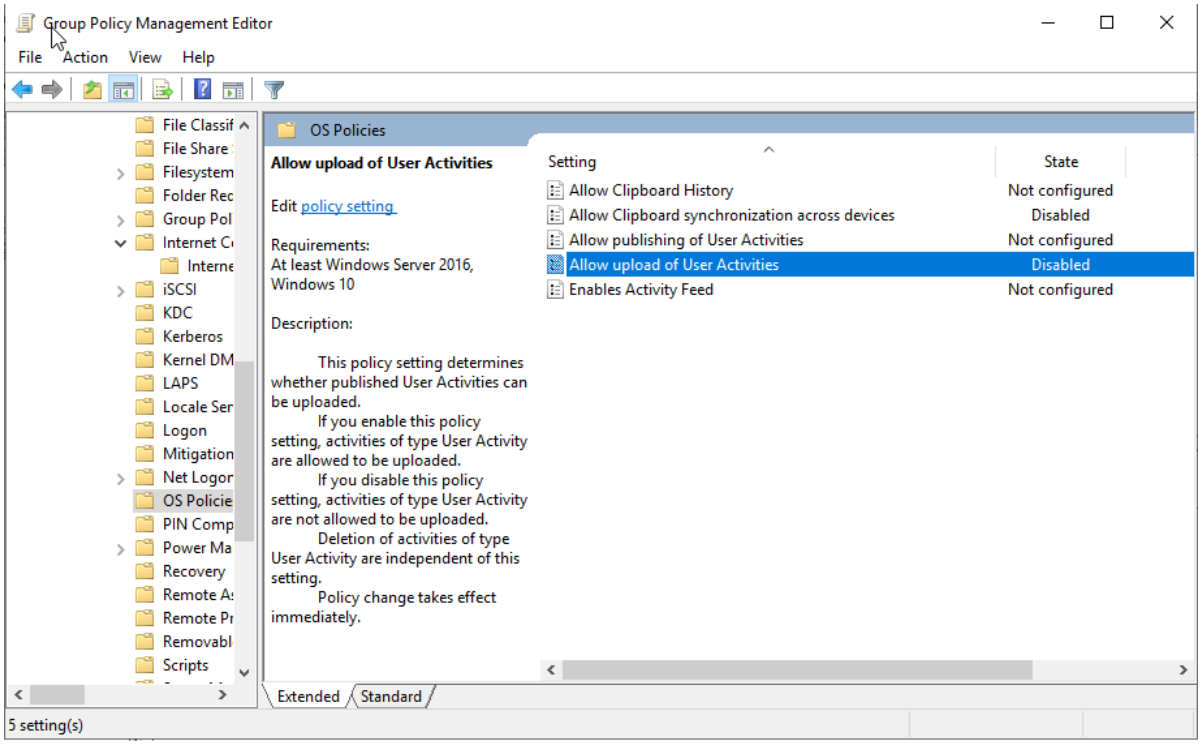


Image 229-Ensure 'Allow upload of User Activities' is set to 'Disabled'

7.7.13 Power Management

7.7.13.1 Sleep Settings

7.7.13.1.1 Ensure 'Allow network connectivity during connected-standby (on battery)' is set to 'Disabled'

This policy setting controls whether network connectivity is maintained during standby on systems with modern standby capabilities. The recommended state for this setting is Disabled. This configuration prevents the computer from being accessible to attackers over a WLAN network while it is unattended, on battery power, and in a sleep state.

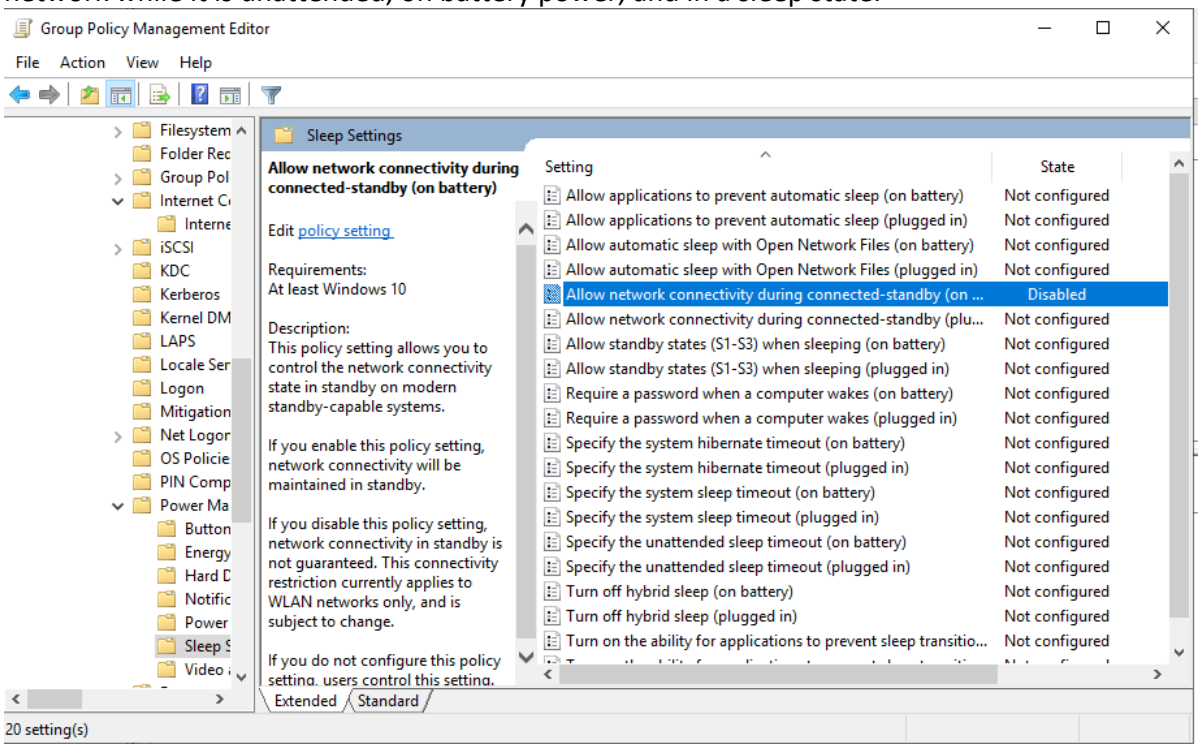


Image 230-Ensure 'Allow network connectivity during connected-standby (on battery)' is set to 'Disabled'

7.7.13.1.2 Ensure 'Allow network connectivity during connected-standby (plugged in)' is set to 'Disabled'

This policy setting manages the network connectivity status during standby on systems that support modern standby. The recommended state for this setting is Disabled. By disabling this option, you ensure that the computer remains inaccessible to attackers over a WLAN network when it is unattended, plugged in, and in a sleep mode.

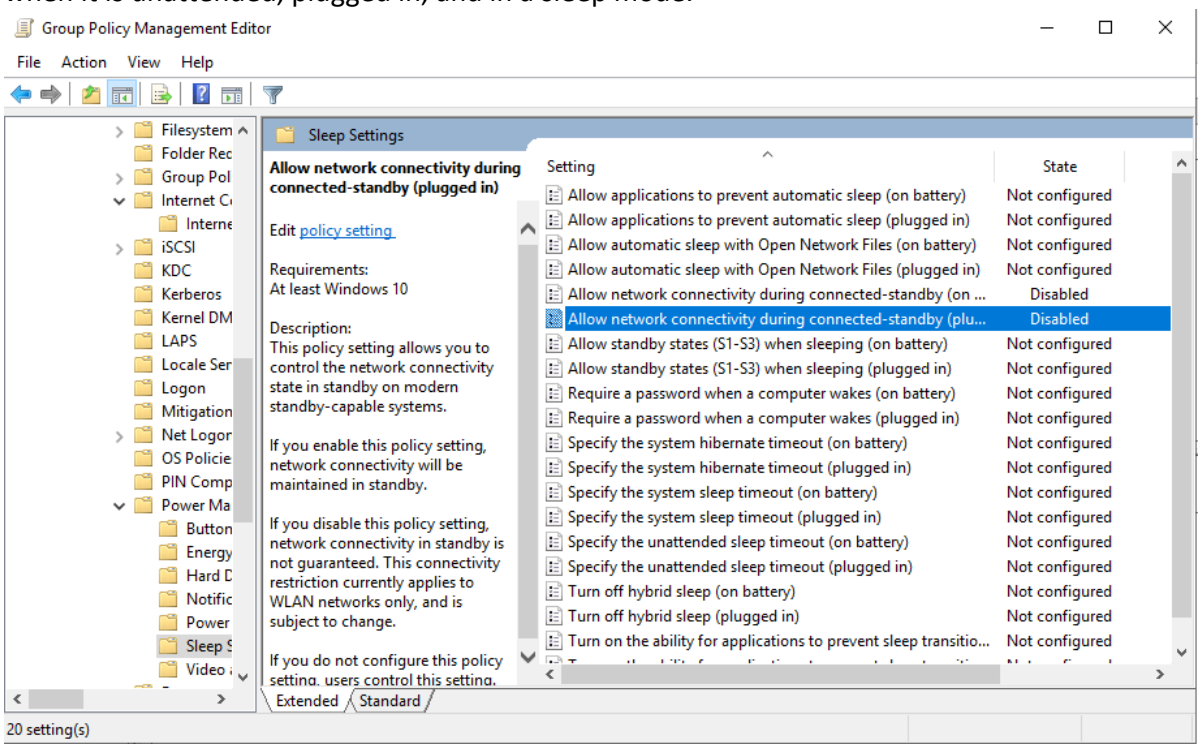


Image 231-Ensure 'Allow network connectivity during connected-standby (plugged in)' is set to 'Disabled'

7.7.13.1.3 Ensure 'Require a password when a computer wakes (on battery)' is set to 'Enabled'

This policy setting determines if a user is required to enter a password when the system resumes from sleep. The recommended configuration is to enable this setting. Enabling it ensures that anyone who wakes an unattended computer from sleep must provide login credentials before accessing the system.

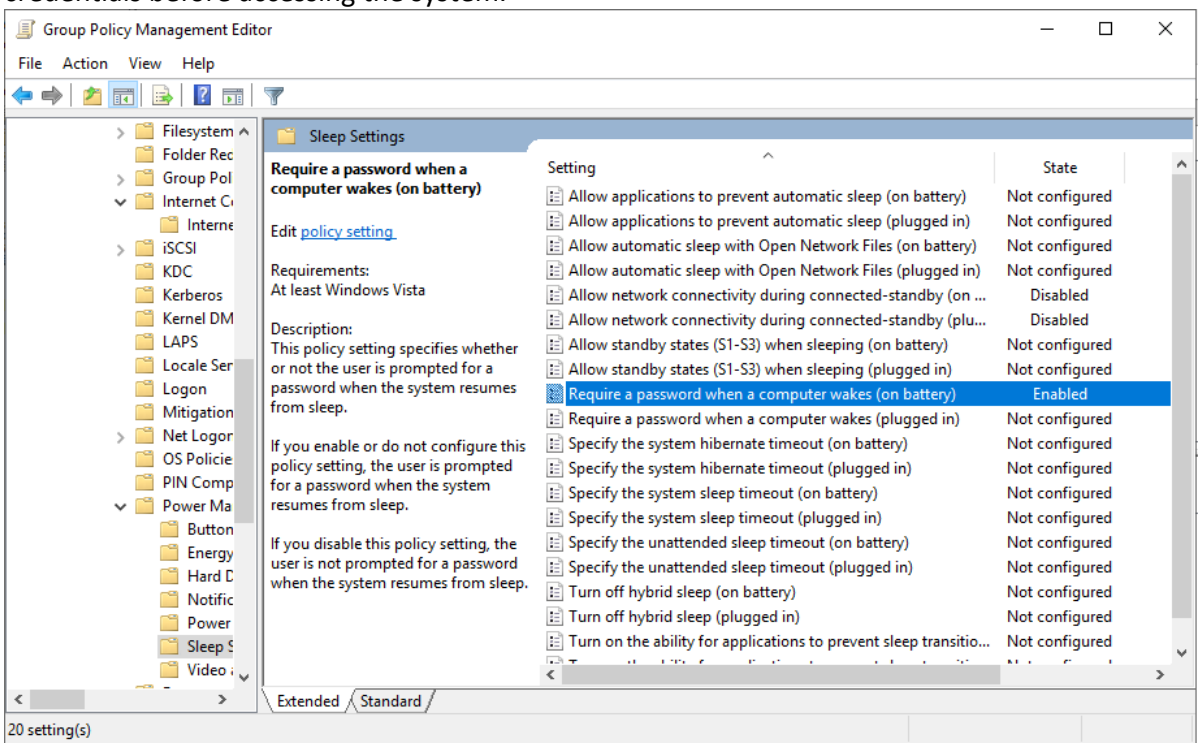


Image 232-Ensure 'Require a password when a computer wakes (on battery)' is set to 'Enabled'

7.7.13.1.4 Ensure 'Require a password when a computer wakes (plugged in)' is set to 'Enabled'

This policy setting controls whether a password prompt is required when the system resumes from sleep. The recommended state for this setting is to enable it. Doing so ensures that anyone who wakes an unattended computer from sleep must enter login credentials before gaining access to the system.

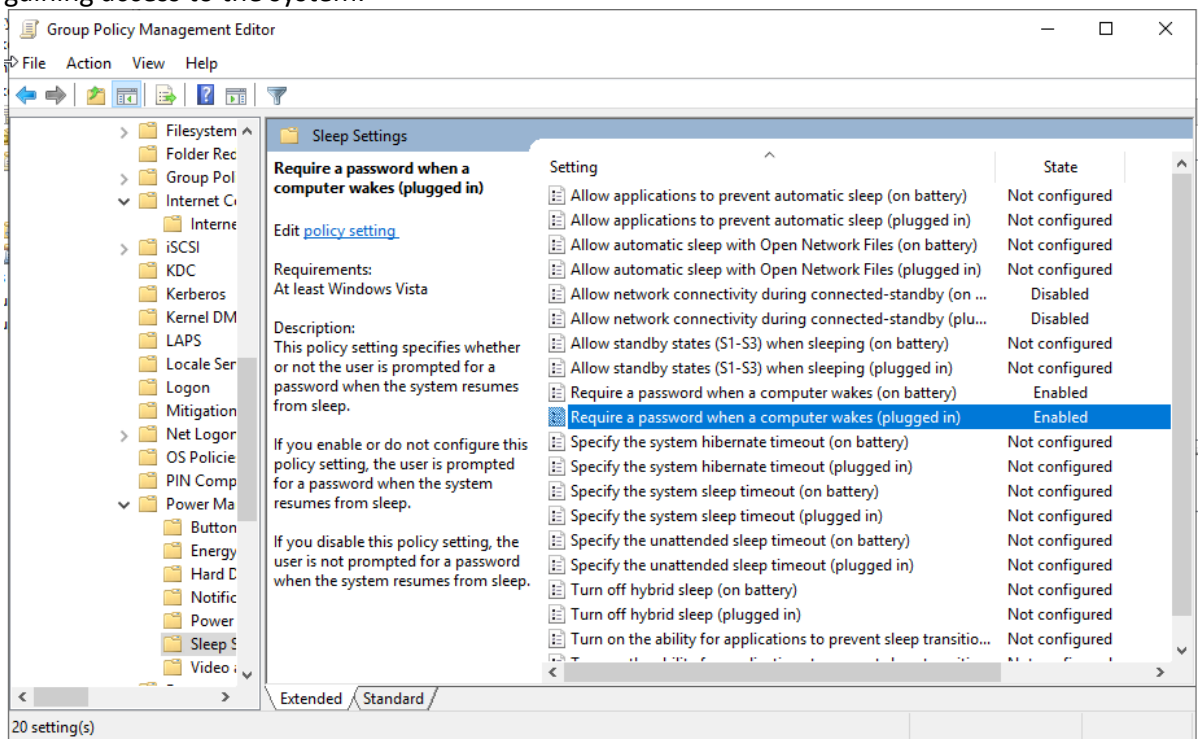


Image 233-Ensure 'Require a password when a computer wakes (plugged in)' is set to 'Enabled'

7.7.14 Remote Assistance

7.7.14.1 Ensure 'Configure Offer Remote Assistance' is set to 'Disabled'

This policy setting controls whether unsolicited Remote Assistance can be offered on the computer. When disabled, help desk and support personnel will not be able to initiate remote assistance proactively, but they can still respond to user-initiated requests for help. The recommended state for this setting is to disable it, as this reduces the risk of users being deceived into accepting remote assistance from malicious sources.

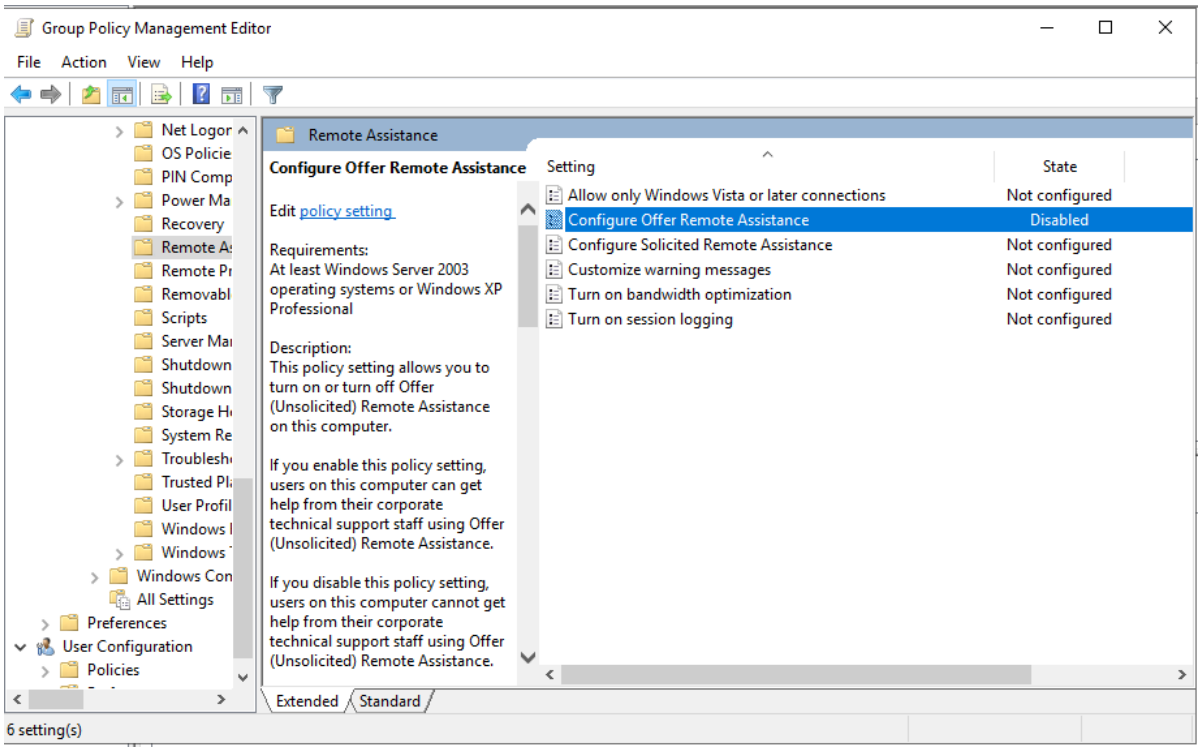


Image 234-Ensure 'Configure Offer Remote Assistance' is set to 'Disabled'

7.7.14.2 Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled'

This policy setting controls whether solicited (request-based) Remote Assistance is enabled on the computer. The recommended state for this setting is to disable it. While this minimizes the risk that a rogue administrator might gain unauthorized access to a user's desktop session, it does not prevent an expert from attempting to connect. The user still has the option to deny the connection or grant only view-only access. Remote control requires explicit approval from the user, who must click "Yes" to allow an expert to take control of their workstation.

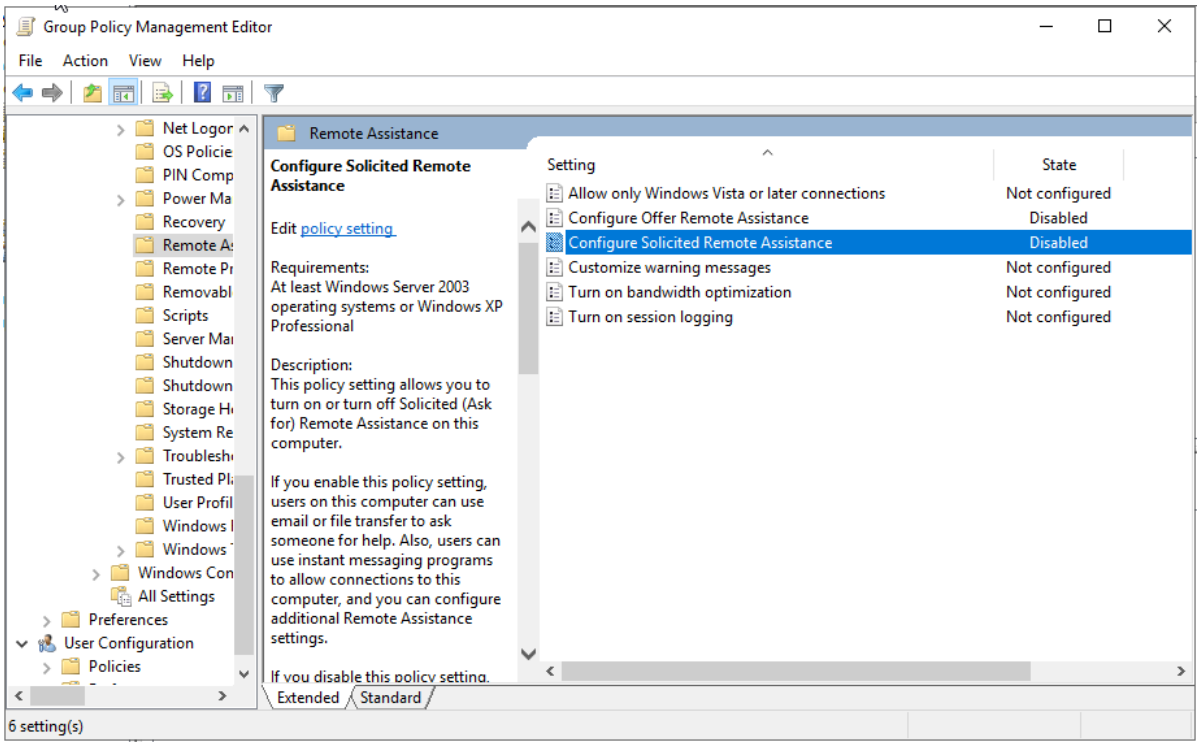


Image 235-Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled'

7.7.15 Remote Procedure Call

7.7.15.1 Ensure 'Enable RPC Endpoint Mapper Client Authentication' is set to 'Enabled'

This policy setting controls whether RPC clients must authenticate with the Endpoint Mapper Service when making calls that include authentication information. Windows NT4 (all service packs) cannot handle such authentication details with its Endpoint Mapper Service. Applying this policy to Domain Controllers can create issues with one-way forest trusts, as noted in Microsoft KB3073942, so it is not recommended for Domain Controllers. This setting will only take effect after a system reboot. The recommended state for this setting is enabled to prevent unauthorized access and potential disclosure of information to unauthenticated users.

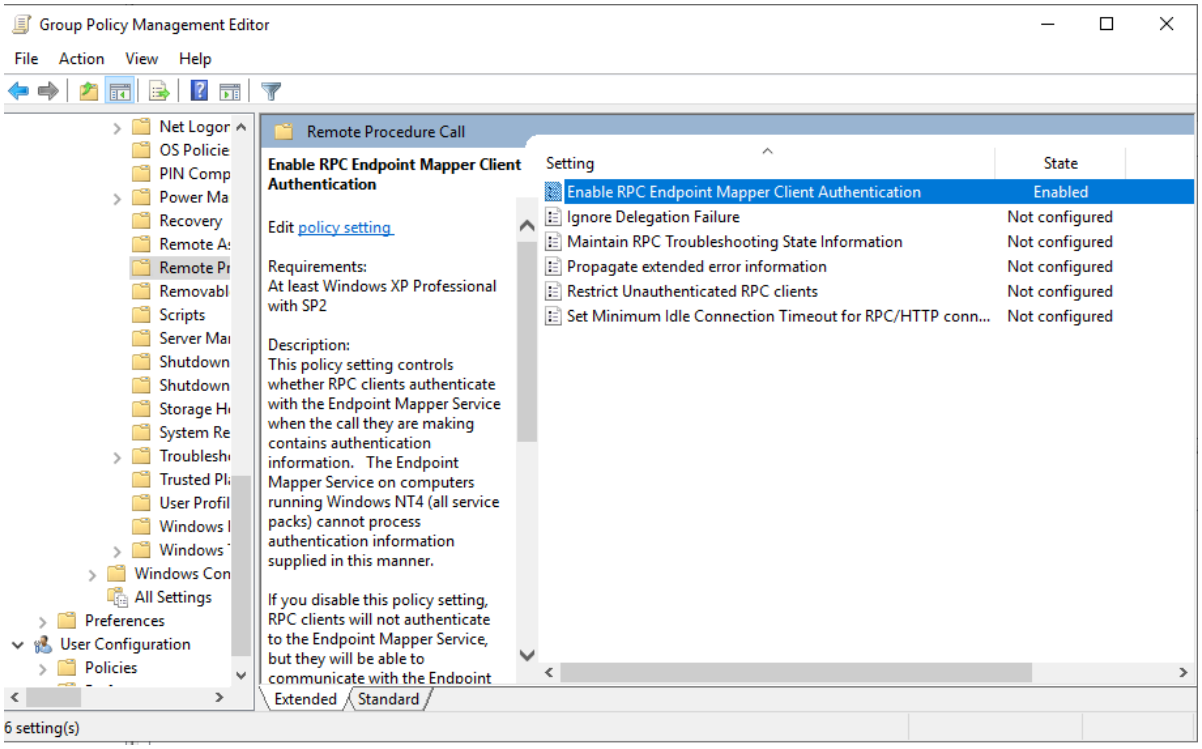


Image 236-Ensure 'Enable RPC Endpoint Mapper Client Authentication' is set to 'Enabled'

7.7.15.2 Ensure 'Restrict Unauthenticated RPC clients' is set to 'Enabled: Authenticated'

This policy setting controls how the RPC server runtime manages unauthenticated RPC clients attempting to connect to RPC servers. It affects all RPC applications and should be used cautiously in a domain environment due to its potential impact on various functionalities, including group policy processing. Reverting changes to this setting may require manual adjustments on each affected machine and should never be applied to Domain Controllers.

Clients will be considered authenticated if they use a named pipe or RPC Security to communicate. RPC interfaces specifically set to be accessible by unauthenticated clients might be exempt from this policy, depending on its configuration:

- "None" allows all RPC clients to connect.
- "Authenticated" permits only authenticated RPC clients, with possible exemptions for specified interfaces.
- "Authenticated without exceptions" restricts connections to authenticated RPC clients only, with no exemptions, and is not recommended due to potential serious issues.

Note that changes to this policy will only take effect after a system reboot. The recommended state is "Enabled: Authenticated" to mitigate security risks associated with unauthenticated RPC communication.

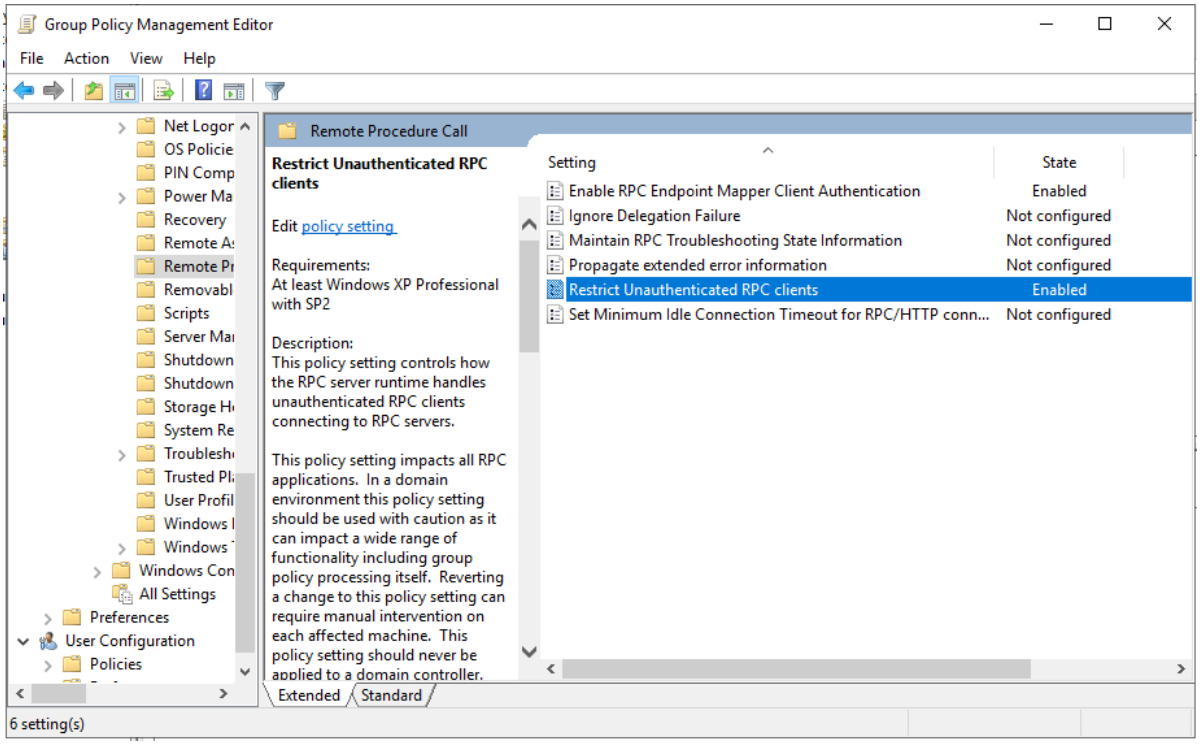


Image 237-Ensure 'Restrict Unauthenticated RPC clients' is set to 'Enabled: Authenticated'

7.7.16 Troubleshooting and Diagnostics

7.7.16.1 Microsoft Support Diagnostic Tool

7.7.16.1.1 Ensure 'Microsoft Support Diagnostic Tool: Turn on MSDT interactive communication with support provider' is set to 'Disabled'

This policy setting manages the Microsoft Support Diagnostic Tool (MSDT) interactions with support providers, as MSDT collects diagnostic data for analysis by support professionals. The recommended state for this setting is Disabled. This recommendation is based on privacy concerns, as sending diagnostic data to third parties could expose sensitive information.

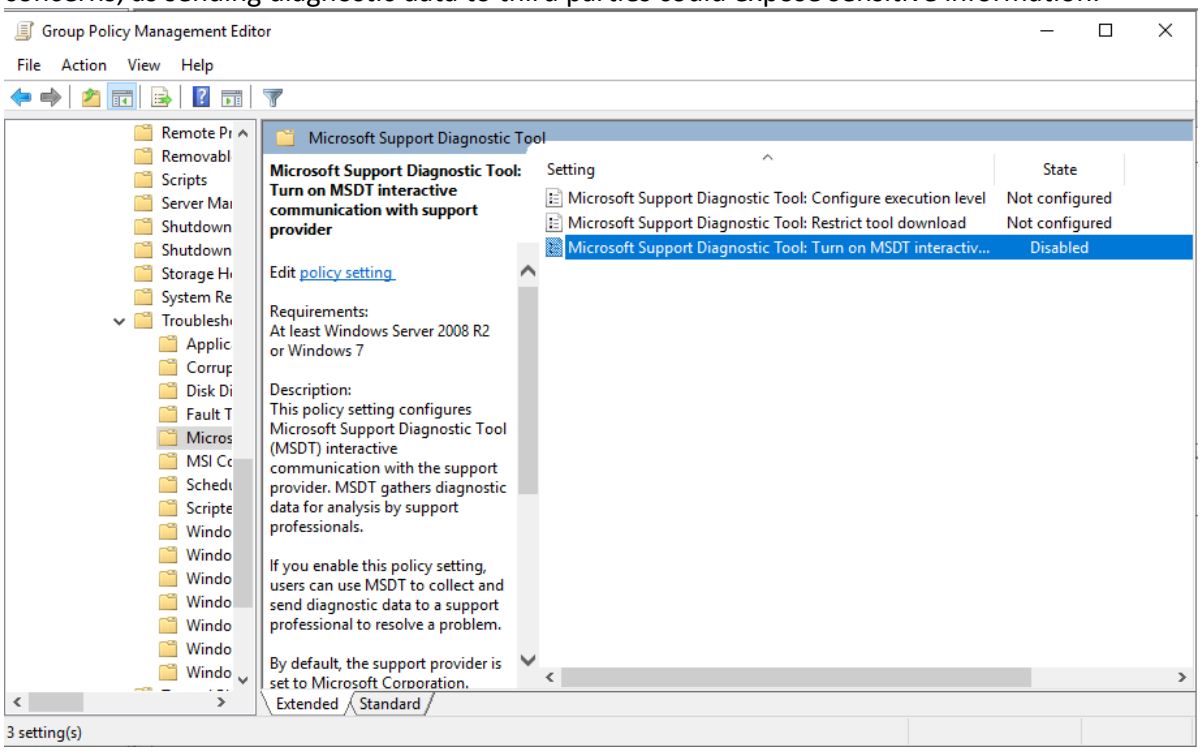


Image 238-Ensure 'Microsoft Support Diagnostic Tool: Turn on MSDT interactive communication with support provider' is set to 'Disabled'

7.7.16.2 Windows Performance PerfTrack

7.7.16.2.1 Ensure 'Enable/Disable PerfTrack' is set to 'Disabled'

This policy setting determines whether responsiveness events should be tracked. The recommended state for this setting is **Disabled**. When enabled, aggregated data from these events is sent to Microsoft. Although there are options to limit tracking to specific users, set consent levels, and designate programs for error reports, it is generally advised to disable this feature centrally. This approach helps prevent unauthorized or unwanted use, data leakage, and unintended communications.

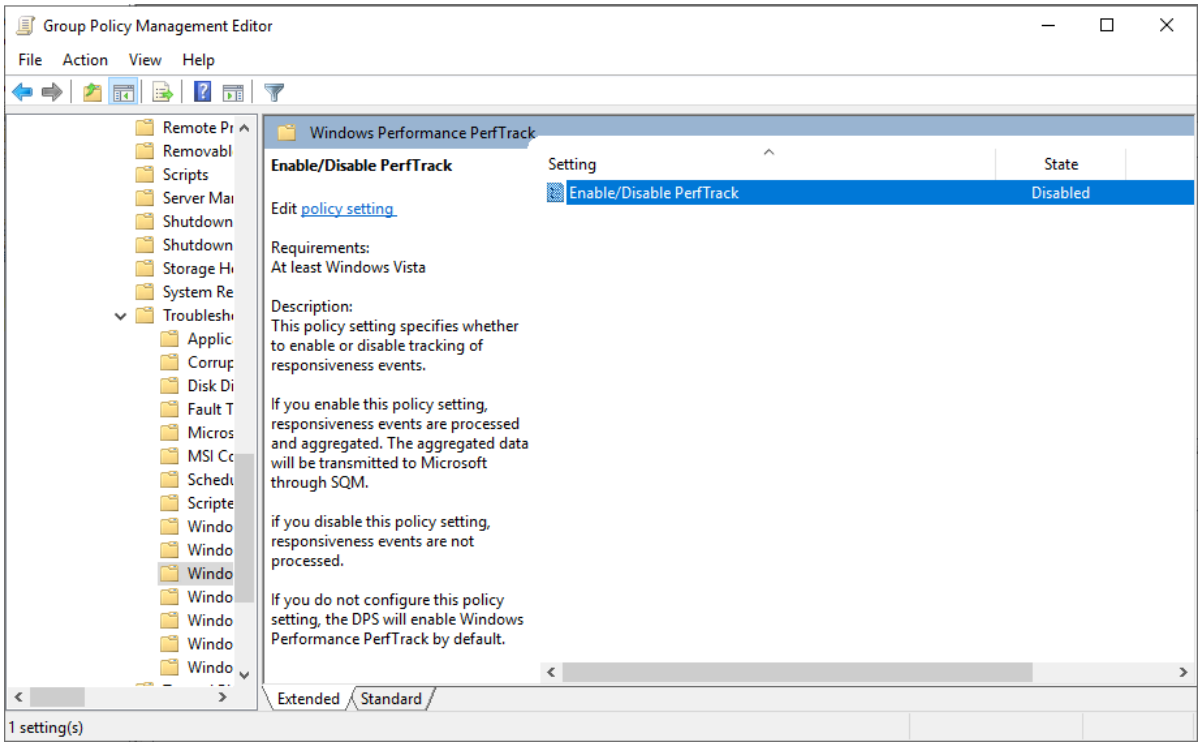


Image 239-Ensure 'Enable/Disable PerfTrack' is set to 'Disabled'

7.7.17 User Profiles

7.7.17.1 Ensure 'Turn off the advertising ID' is set to 'Enabled'

This policy setting disables the advertising ID, which stops apps from using it to track user activity across different applications. The recommended state for this setting is Enabled. The rationale behind this is that even anonymous tracking for advertising purposes can raise privacy concerns. In a managed enterprise environment, there is generally no need for applications to track users for targeted advertising.

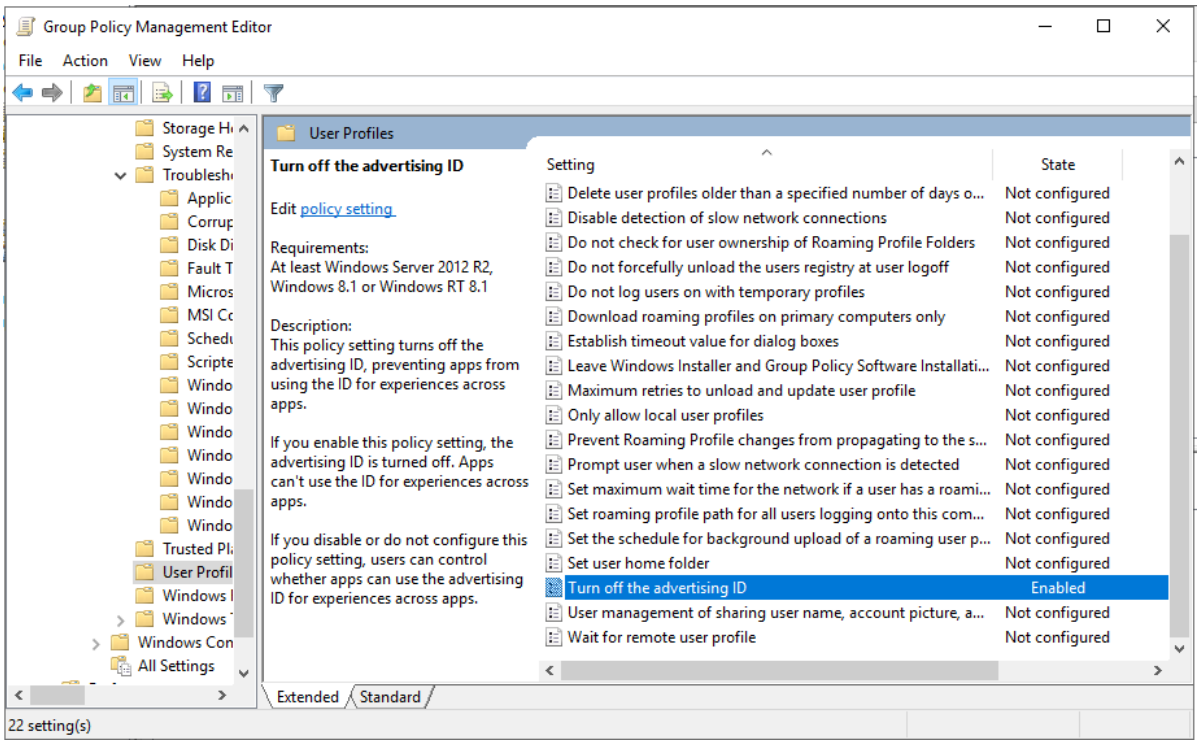


Image 240-Ensure 'Turn off the advertising ID' is set to 'Enabled'

7.7.18 Windows Time Service

7.7.18.1 Time Providers

7.7.18.1.1 Ensure 'Enable Windows NTP Client' is set to 'Enabled'

This policy setting determines whether the Windows NTP Client is enabled. When enabled, the Windows NTP Client allows the synchronization of the system clock with NTP servers. The recommended state for this setting is Enabled. However, if a third-party time provider is used in the environment, this recommendation may need to be adjusted. Accurate and reliable timekeeping is crucial for various services and security functions, such as distributed applications, authentication, multi-user databases, and logging. Using an NTP client helps ensure time accuracy, which is essential for reviewing security-related events.

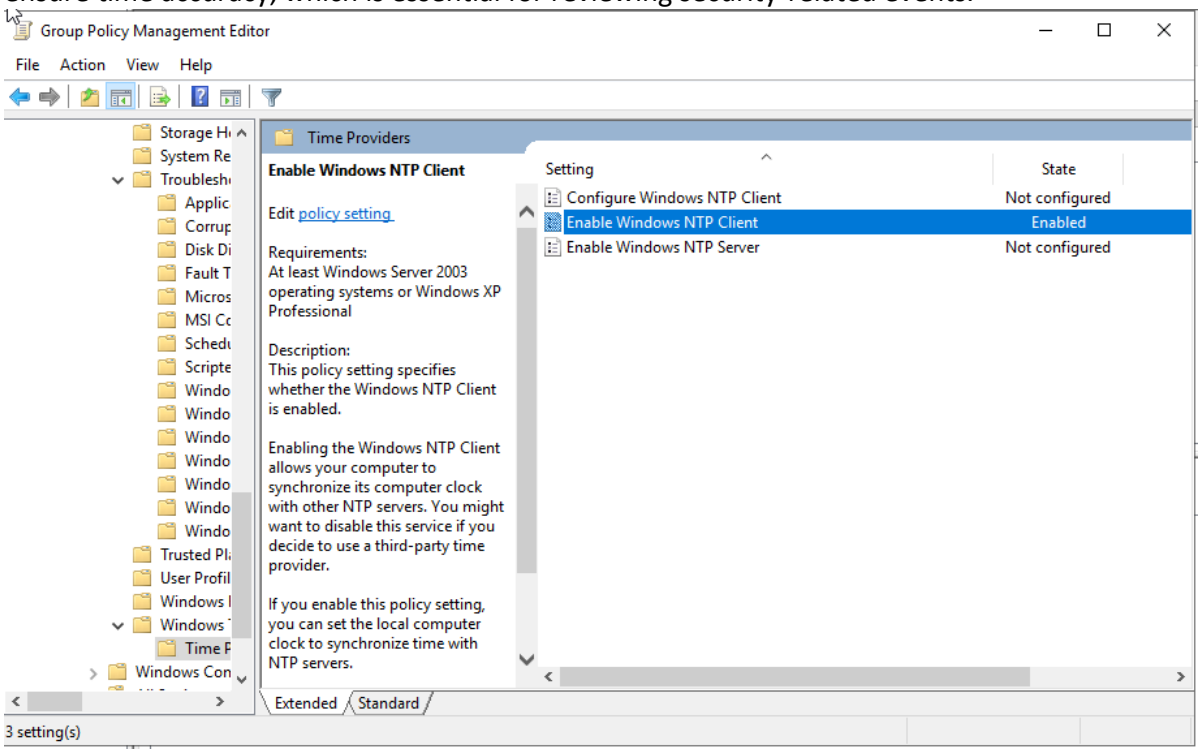


Image 241-Ensure 'Enable Windows NTP Client' is set to 'Enabled'

7.7.18.1.2 Ensure 'Enable Windows NTP Server' is set to 'Disabled'

This policy setting determines whether the Windows NTP Server is enabled. Disabling this setting prevents the system from functioning as an NTP Server, which means it will no longer provide time synchronization services to other systems (NTP Clients). The recommended state for this setting is Disabled. However, it is generally advisable not to disable the Windows NTP Server on Domain Controllers, as it plays a crucial role in NT5DS (domain hierarchy-based) time synchronization. Proper time synchronization is essential in an enterprise environment for maintaining the accuracy of Kerberos authentication timestamps and security logging. Ideally, time synchronization should be managed through a dedicated NTP server, and member servers and workstations should not serve as time sources for other clients.

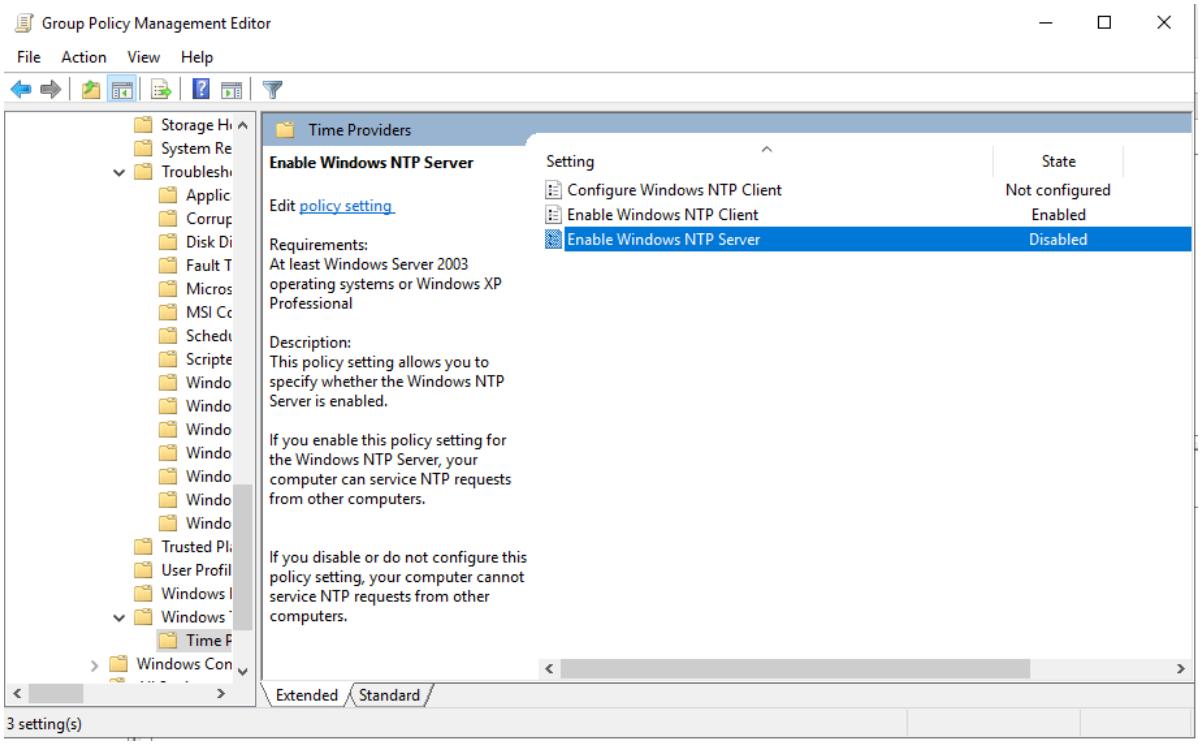


Image 242-Ensure 'Enable Windows NTP Server' is set to 'Disabled'

7.8 Windows Components

The Windows Components section in Group Policy allows administrators to manage and configure built-in features and applications of the Windows operating system. This includes settings for components like Internet Explorer, Windows Defender, and Windows Update. By using this section, administrators can control how these features behave, ensuring they meet organizational requirements and enhance security and functionality.

7.8.1 App Package Deployment

7.8.1.1 Ensure 'Allow a Windows app to share application data between users' is set to 'Disabled'

This policy setting controls whether a Windows app can share data between users who have installed the app. The data is shared via the SharedLocal folder, which can be accessed through the Windows.Storage API. The recommended state for this setting is Disabled. The rationale is that disabling this feature helps prevent users from inadvertently sharing sensitive information with others on the same system.

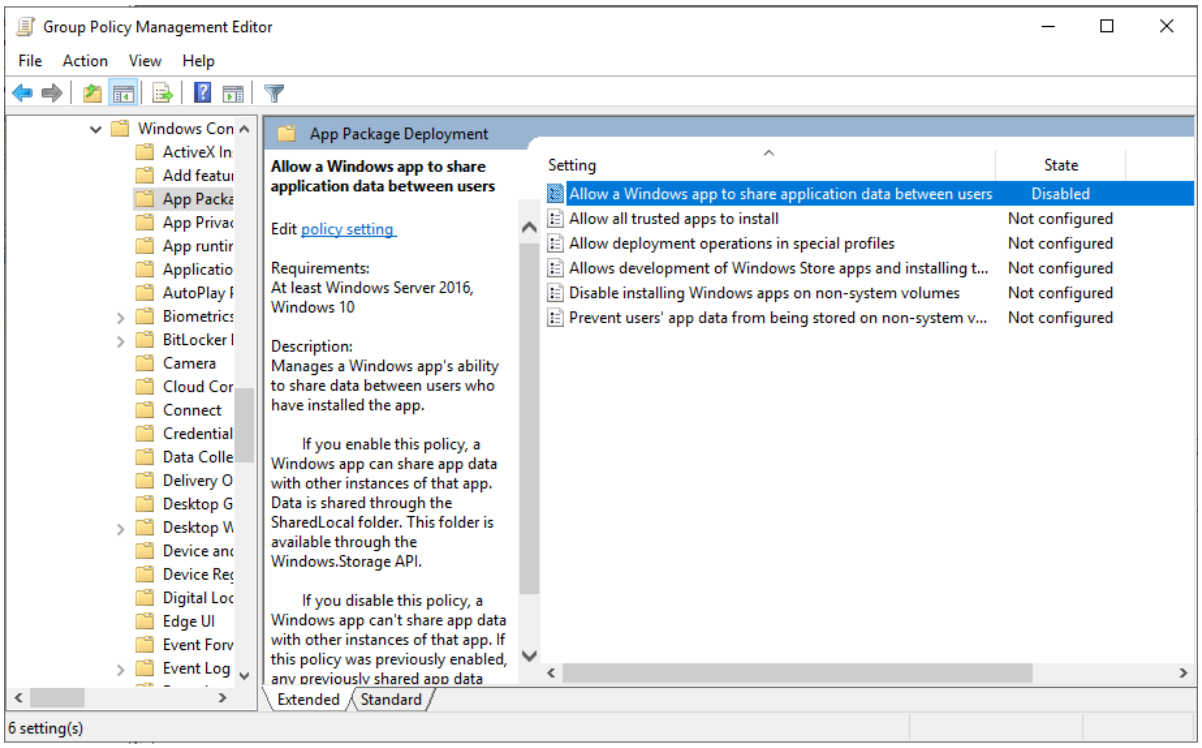


Image 243-Ensure 'Allow a Windows app to share application data between users' is set to 'Disabled'

7.8.2 App runtime

7.8.2.1 Ensure 'Allow Microsoft accounts to be optional' is set to 'Enabled'

This policy setting allows you to determine whether Microsoft accounts are required for Windows Store apps that need an account for sign-in. This applies only to those Windows Store apps that support the feature. The recommended state for this setting is Enabled. Enabling this setting allows an organization to use its own enterprise user accounts instead of Microsoft accounts for accessing Windows Store apps. This approach enhances control over credentials, as Microsoft accounts are not centrally manageable and cannot adhere to enterprise security policies, potentially putting data accessed via these accounts at risk.

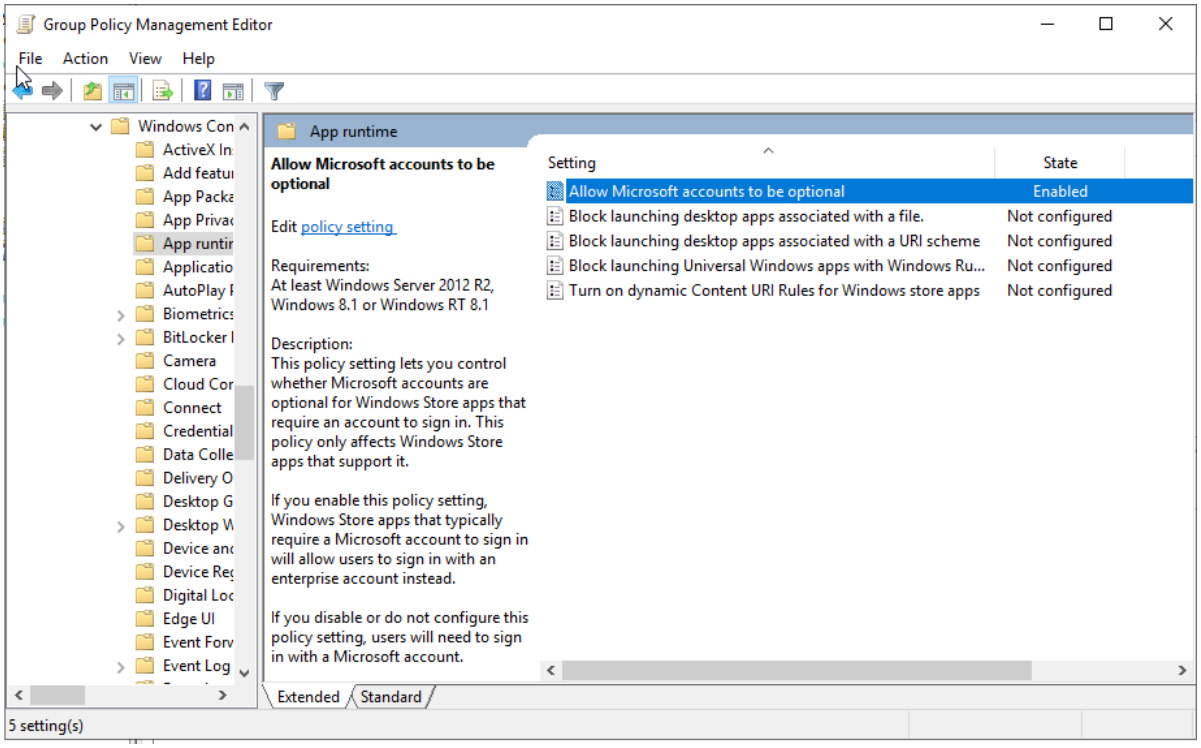


Image 244-Ensure 'Allow Microsoft accounts to be optional' is set to 'Enabled'

7.8.3 AutoPlay Policies

7.8.3.1 Ensure 'Disallow Autoplay for non-volume devices' is set to 'Enabled'

This policy setting disables AutoPlay for Media Transfer Protocol (MTP) devices such as cameras and phones. The recommended state for this setting is **Enabled**. Disabling AutoPlay helps protect against potential attacks where malicious programs could be automatically launched from MTP devices, potentially causing harm to the client computer or its data.

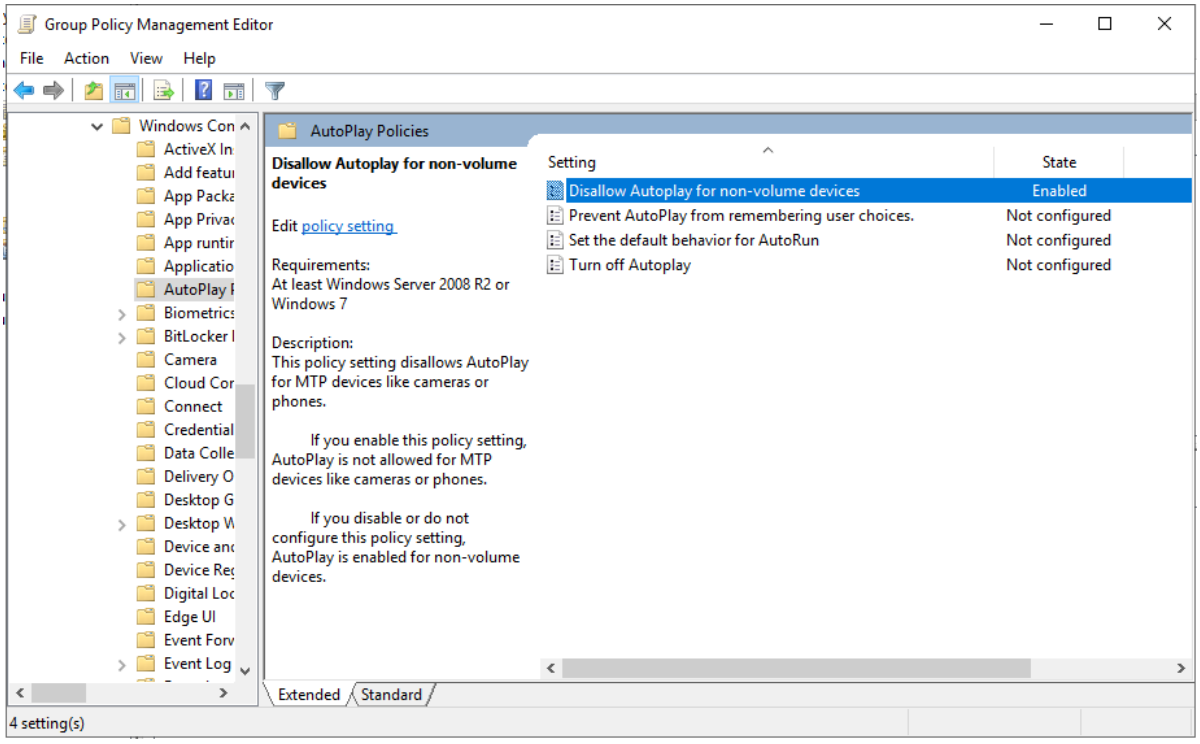


Image 245-Ensure 'Disallow Autoplay for non-volume devices' is set to 'Enabled'

7.8.3.2 Ensure 'Set the default behavior for AutoRun' is set to 'Enabled: Do not execute any autorun commands'

This policy setting defines the default behavior for Autorun commands, which are typically stored in autorun.inf files and often used to launch installation programs or other routines. The recommended state for this setting is Enabled: Do not execute any autorun commands.

Prior to Windows Vista, inserting media with an autorun command would automatically execute the program without user intervention, posing a significant security risk. Since Windows Vista, the default behavior has been to prompt the user for confirmation before running any autorun commands, with these commands appearing as handlers in the Autoplay dialog.

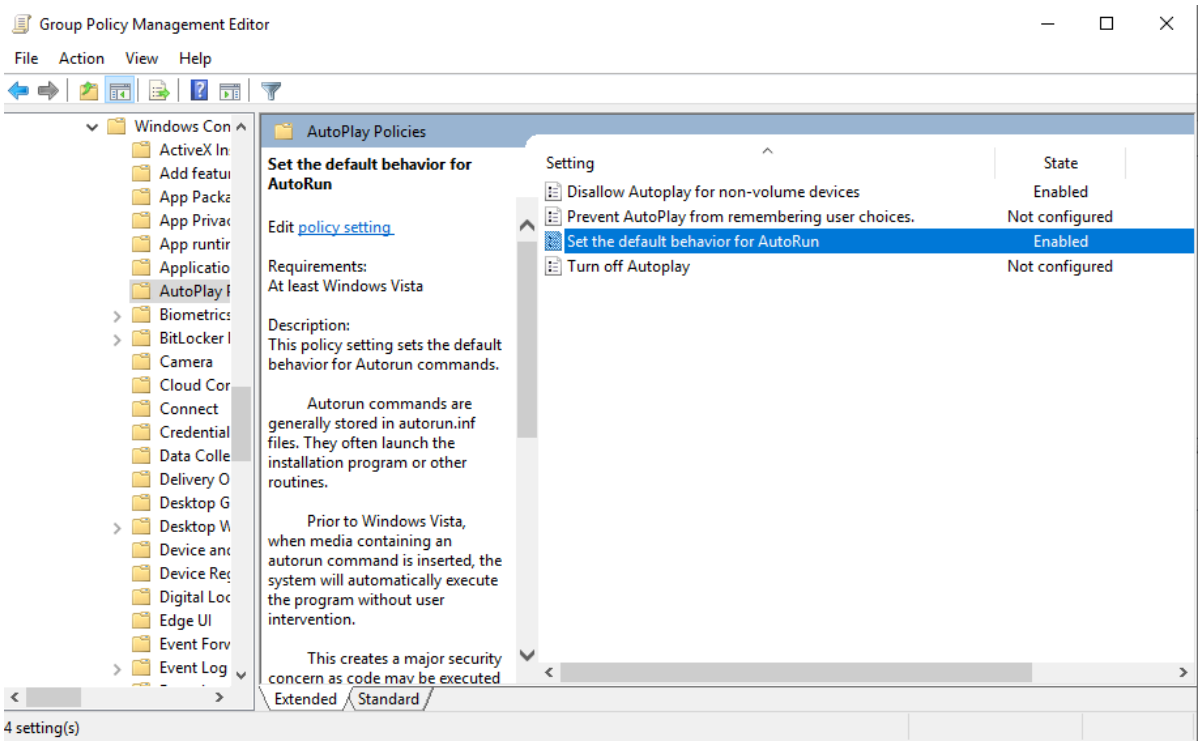


Image 246-Ensure 'Set the default behavior for AutoRun' is set to 'Enabled: Do not execute any autorun commands'

7.8.3.3 Ensure 'Turn off Autoplay' is set to 'Enabled: All drives'

Autoplay begins reading from a drive as soon as media is inserted, which can cause setup files for programs or audio media to start immediately. This feature can be exploited by attackers to launch malicious programs that could damage the computer or its data. While Autoplay is disabled by default on certain removable drives like floppy disks and network drives, it remains active on CD-ROM drives. Note that this policy setting cannot enable Autoplay on drives where it is disabled by default. The recommended configuration is **Enabled: All drives** to ensure consistent behavior across all media types.

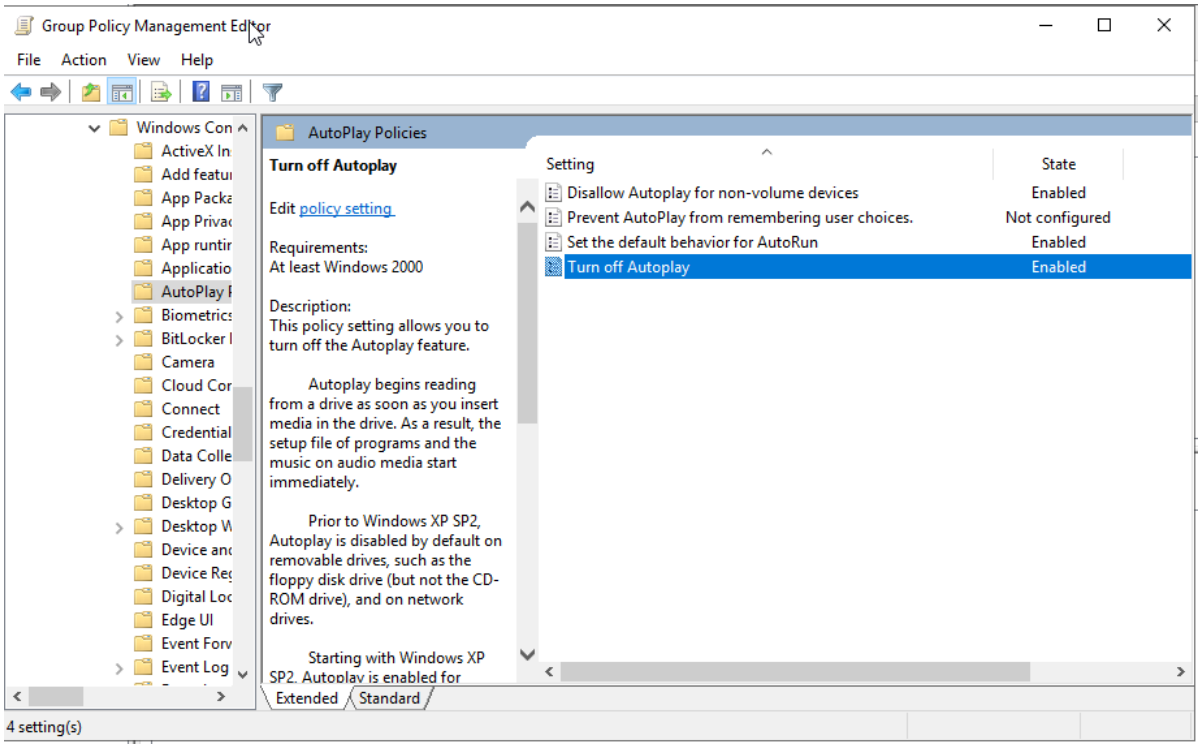


Image 247-Ensure 'Turn off Autoplay' is set to 'Enabled: All drives'

7.8.4 Biometrics

7.8.4.1 Facial Features

7.8.4.1.1 Ensure 'Turn off Autoplay' is set to 'Enabled: All drives'

This policy setting specifies whether enhanced anti-spoofing measures are applied to devices that support this feature. The recommended configuration is **Enabled**. As enterprise environments increasingly support a diverse array of mobile devices, strengthening security on these devices is crucial for protecting against unauthorized access to the network.

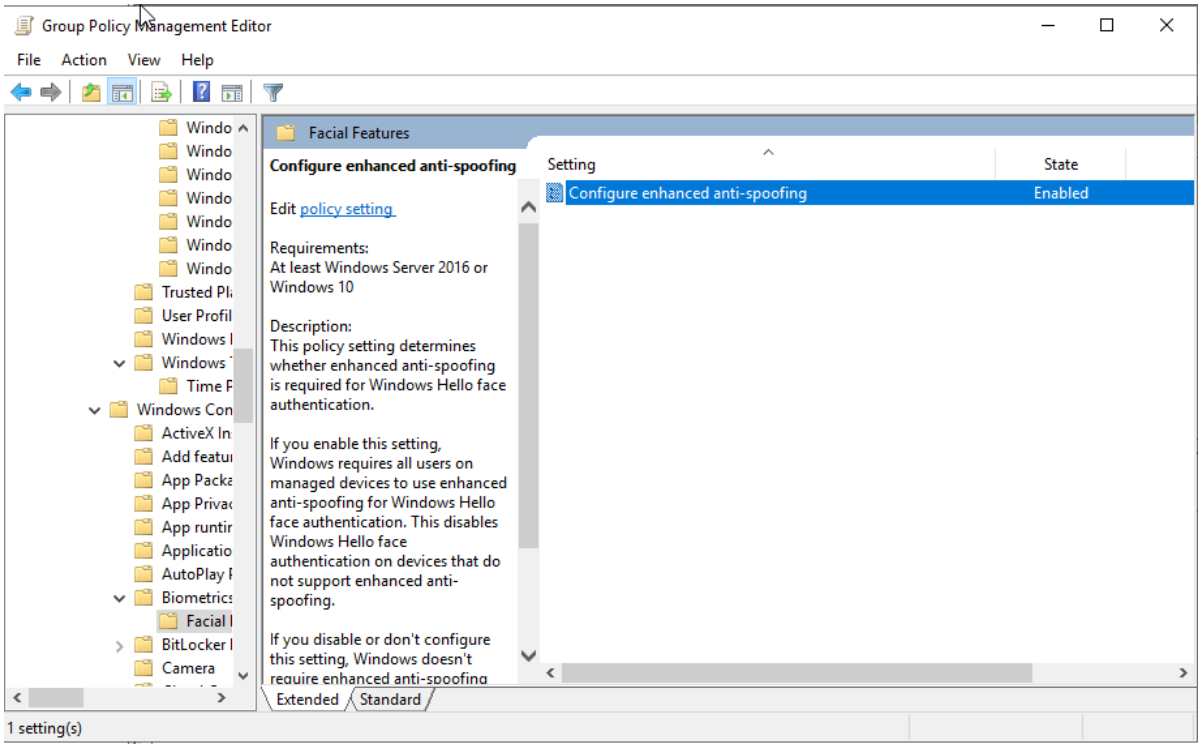


Image 248-Ensure 'Turn off Autoplay' is set to 'Enabled: All drives'

7.8.5 Camera

7.8.5.1 Ensure 'Allow Use of Camera' is set to 'Disabled'

This policy setting regulates whether camera devices are allowed on the machine. The recommended configuration is **Disabled**. In high-security environments, cameras can present significant privacy and data exfiltration risks, so disabling them helps mitigate these potential threats.

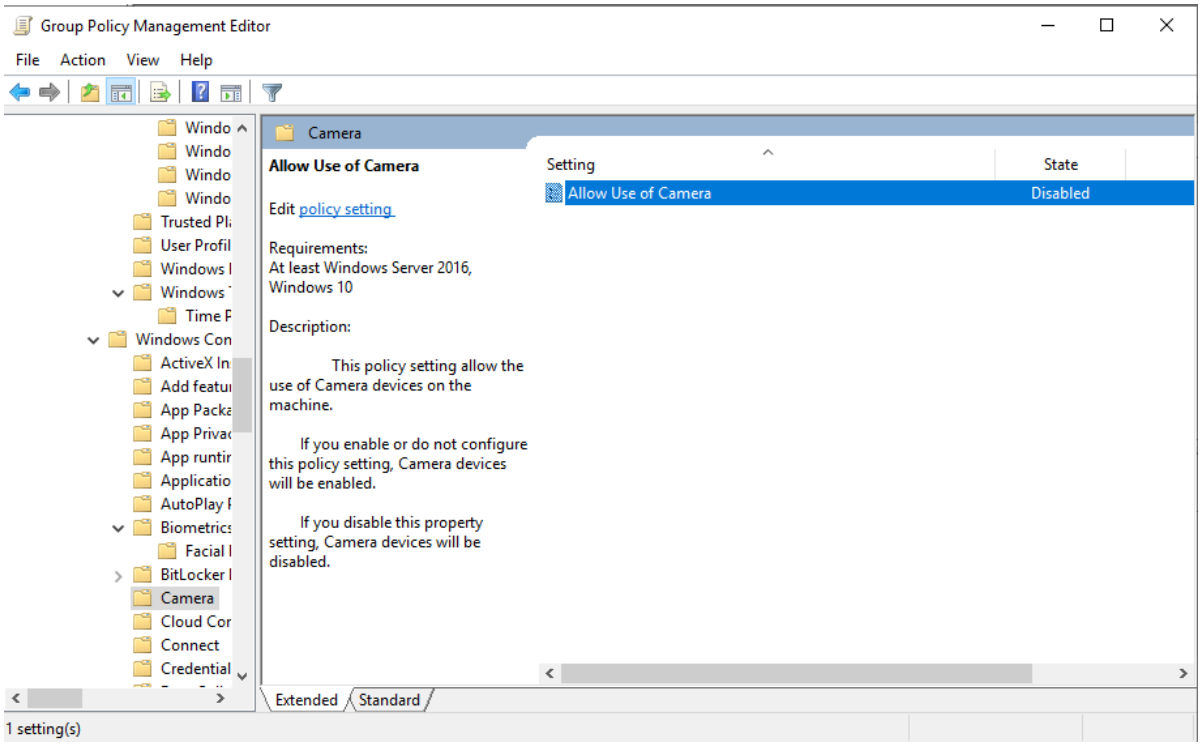


Image 249-Ensure 'Allow Use of Camera' is set to 'Disabled'

7.8.6 Cloud Content

7.8.6.1 Ensure 'Turn off Microsoft consumer experiences' is set to 'Enabled'

This policy setting disables features designed to enhance the use of devices and Microsoft accounts for consumers. The recommended state for this setting is Enabled. Note that, according to Microsoft TechNet, this policy applies only to Windows 10 Enterprise and Windows 10 Education editions. In an enterprise environment, it is crucial to avoid the automatic installation of apps, particularly those that may transmit data to third parties, as it poses security risks.

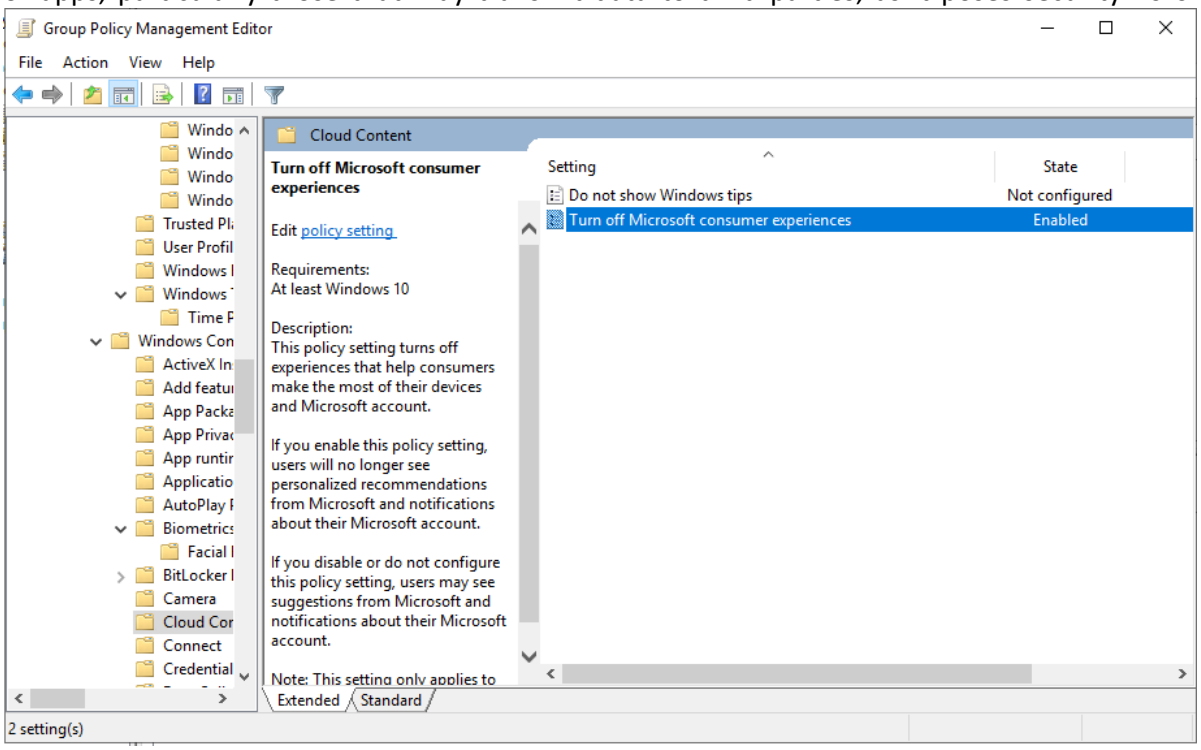


Image 250-Ensure 'Turn off Microsoft consumer experiences' is set to 'Enabled'

7.8.7 Connect

7.8.7.1 Ensure 'Require pin for pairing' is set to 'Enabled: First Time' OR 'Enabled: Always'

This policy setting determines if a PIN is required when pairing with a wireless display device. The recommended configuration is either **Enabled: First Time** or **Enabled: Always**. If this setting is not configured or is disabled, a PIN will not be needed for pairing, which increases the risk of unauthorized access to the device.

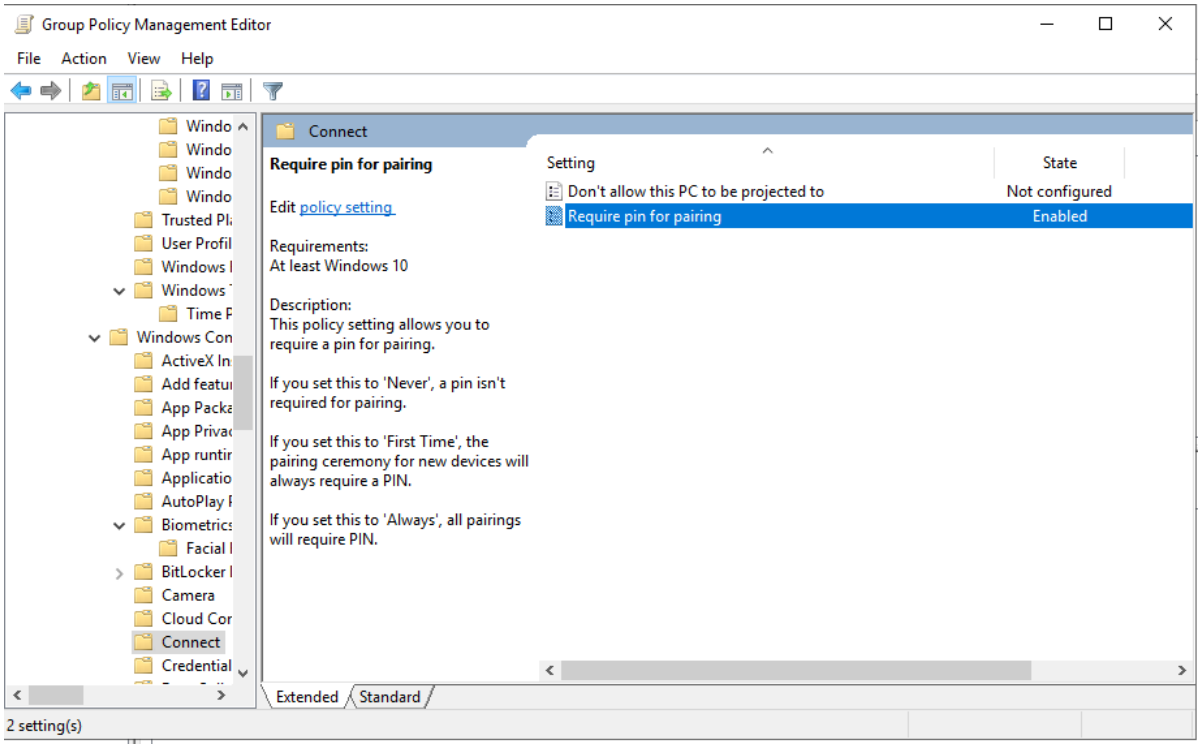


Image 251-Ensure 'Require pin for pairing' is set to 'Enabled: First Time' OR 'Enabled: Always'

7.8.8 Credential User Interface

7.8.8.1 Ensure 'Do not display the password reveal button' is set to 'Enabled'

This policy setting lets you control whether the password reveal button is displayed during password entry. The recommended configuration is to have this feature **Enabled**. This can be particularly helpful when entering a long and complex password, especially on a touchscreen. However, there is a risk that someone might see your password if they are secretly watching your screen.

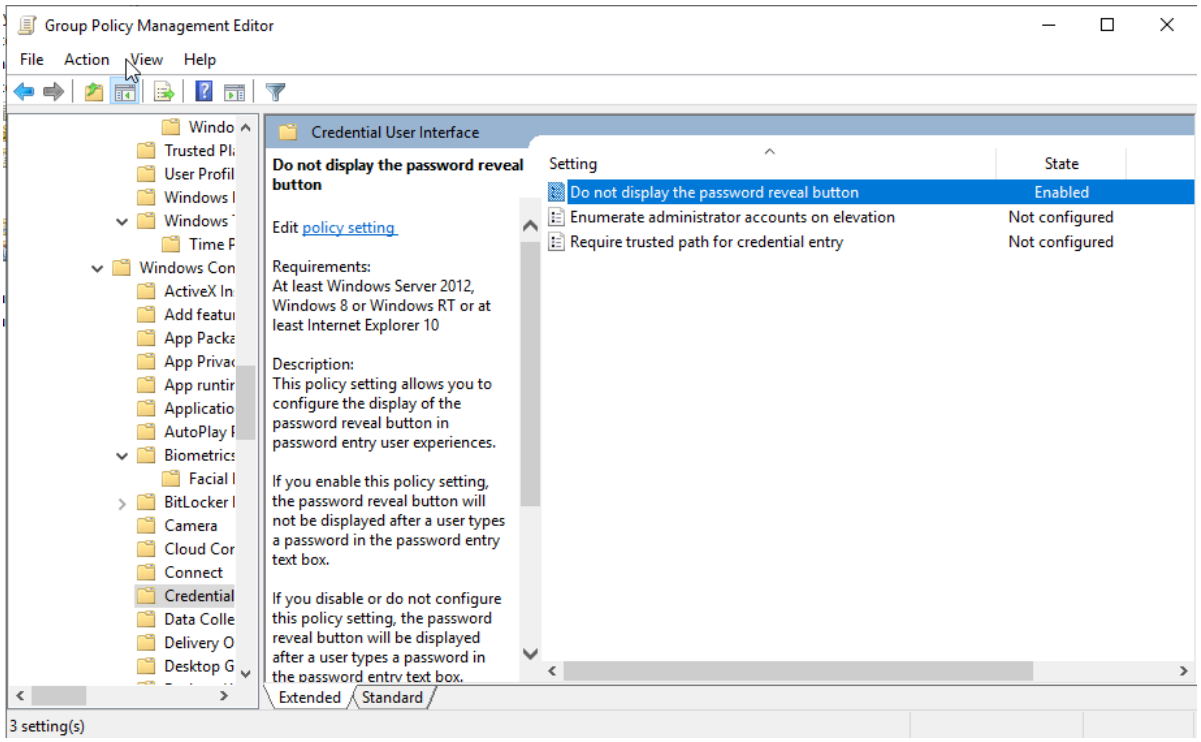


Image 252-Ensure 'Do not display the password reveal button' is set to 'Enabled'

7.8.8.2 Ensure 'Enumerate administrator accounts on elevation' is set to 'Disabled'

This policy setting determines whether administrator accounts are shown when a user tries to elevate a running application. The recommended configuration is **Disabled**. This helps prevent the exposure of administrator account names, which could otherwise make it somewhat easier for a malicious user who has gained access to the system to attempt to crack the passwords of these accounts.

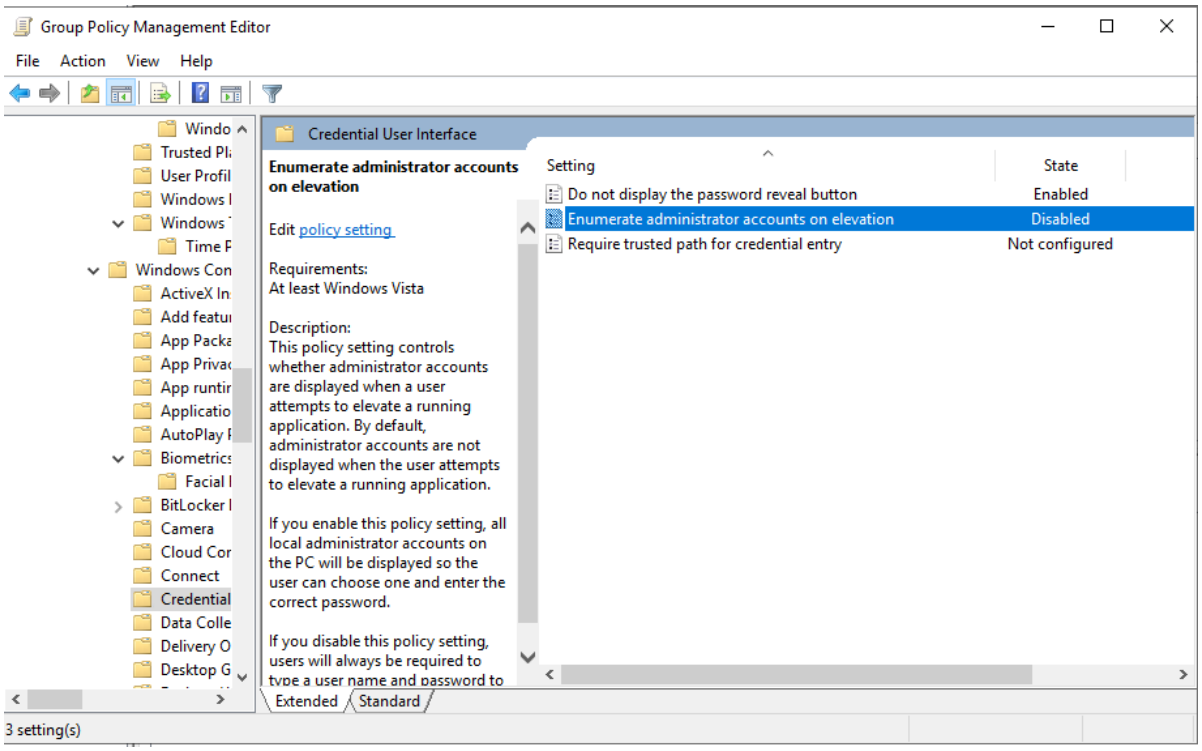


Image 253-Ensure 'Enumerate administrator accounts on elevation' is set to 'Disabled'

7.8.9 Credential User Interface

7.8.9.1 Ensure 'Configure Authenticated Proxy usage for the Connected User Experience and Telemetry service' is set to 'Enabled: Disable Authenticated Proxy usage'

This policy setting controls whether the Connected User Experience and Telemetry service can use an authenticated proxy to send data to Microsoft. The recommended state is: Enabled: Disable Authenticated Proxy usage. This is advised because sending data to third parties presents security risks and should be limited to necessary cases only.

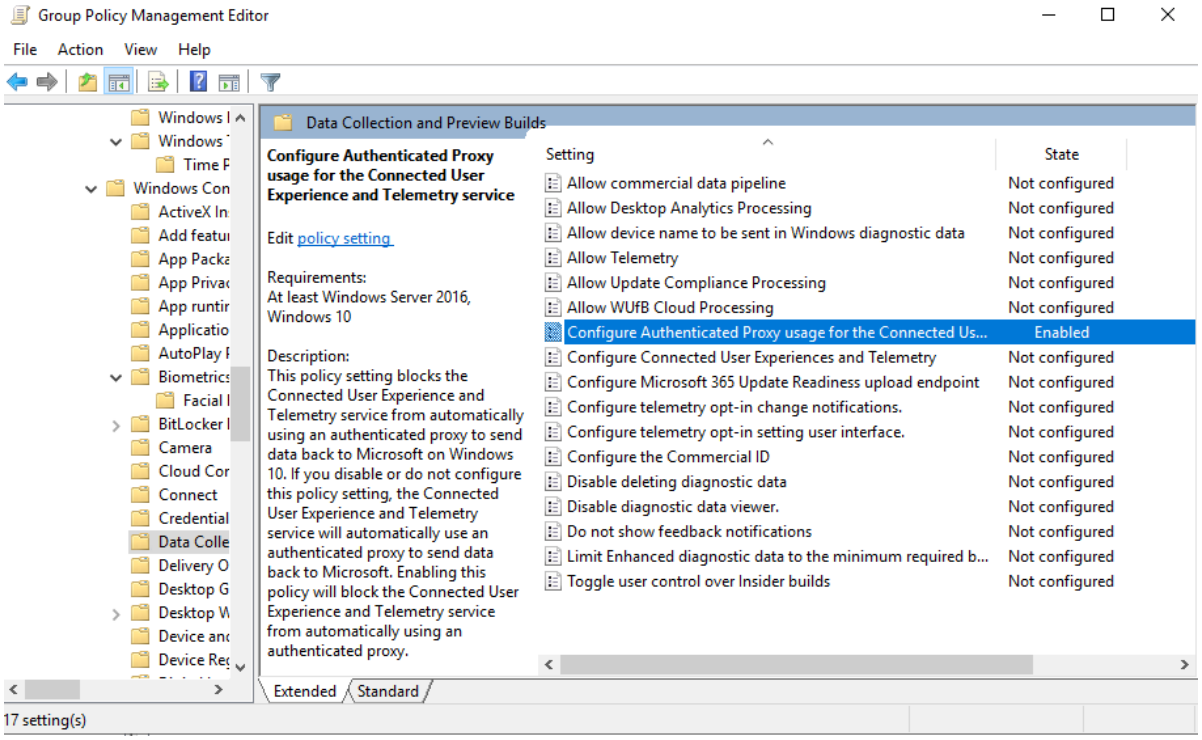


Image 254-Ensure 'Configure Authenticated Proxy usage for the Connected User Experience and Telemetry service' is set to 'Enabled: Disable Authenticated Proxy usage'

7.8.9.2 Ensure 'Do not show feedback notifications' is set to 'Enabled'

This policy setting enables an organization to stop its devices from displaying feedback questions from Microsoft. The recommended state is: Enabled. This ensures that users do not send feedback to third-party vendors in an enterprise-managed environment.

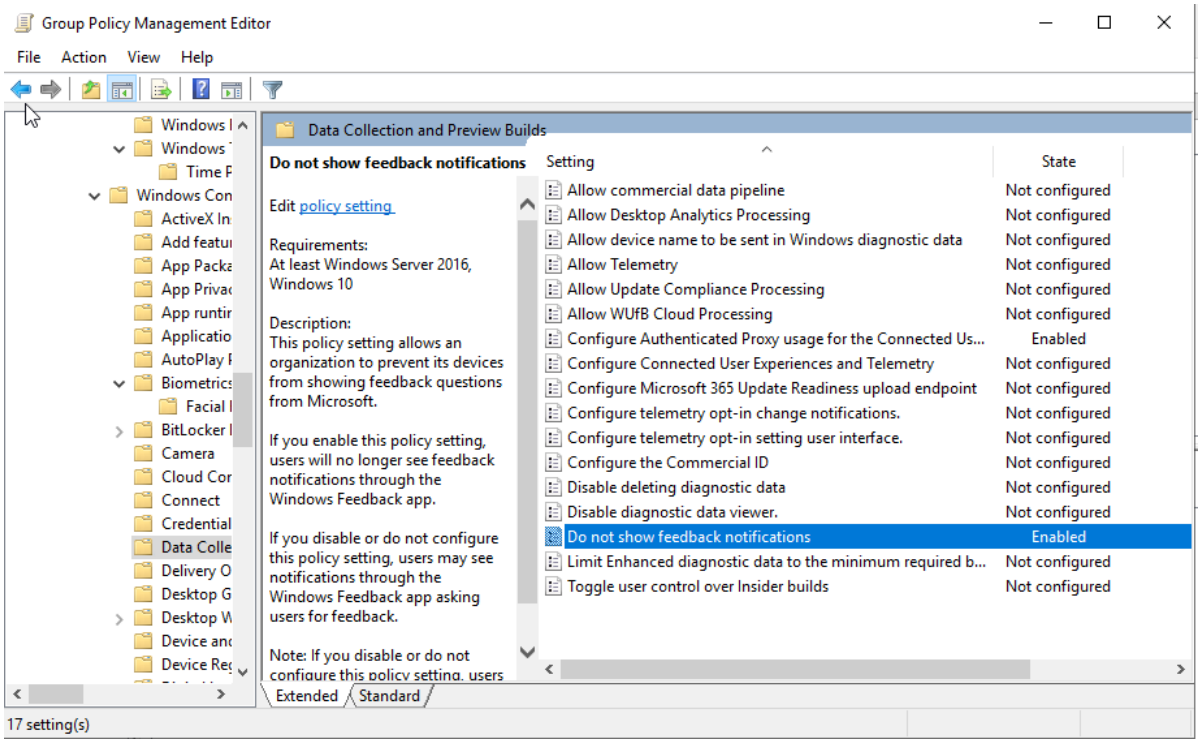


Image 255-Ensure 'Do not show feedback notifications' is set to 'Enabled'

7.8.9.3 Ensure 'Toggle user control over Insider builds' is set to 'Disabled'

This policy setting controls whether users can access Insider build options in the Advanced Options of Windows Update. These options, found under "Get Insider builds," allow users to download and install preview software for Windows. The recommended state for this setting is: Disabled. This policy only affects devices running Windows Server 2016 up to Release 1703. For Release 1709 and later, Microsoft suggests using the "Manage preview builds" setting. This policy remains in the benchmark to ensure compliance for older Windows Server 2016 versions. Allowing experimental features in an enterprise environment can introduce bugs and security vulnerabilities, increasing the risk of unauthorized access. It is safer to use only production-ready builds.

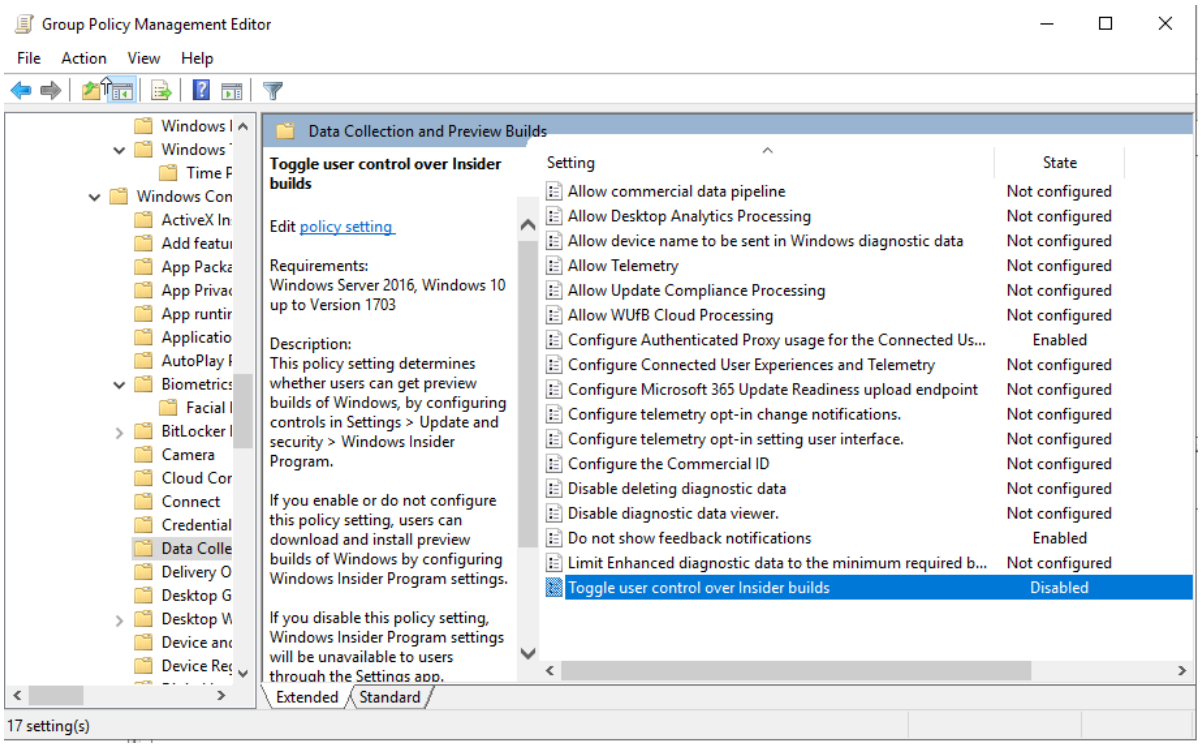


Image 256-Ensure 'Toggle user control over Insider builds' is set to 'Disabled'

7.8.10 Event Log Service

7.8.10.1 Application

7.8.10.1.1 Ensure 'Application: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'

This policy setting manages how Event Logs behave when they reach their maximum size. The recommended state for this setting is: Disabled. The retention of old events depends on the "Backup log automatically when full" policy setting. Disabling this setting could prevent new events from being recorded, which may hinder the ability to diagnose system issues or detect unauthorized activities.

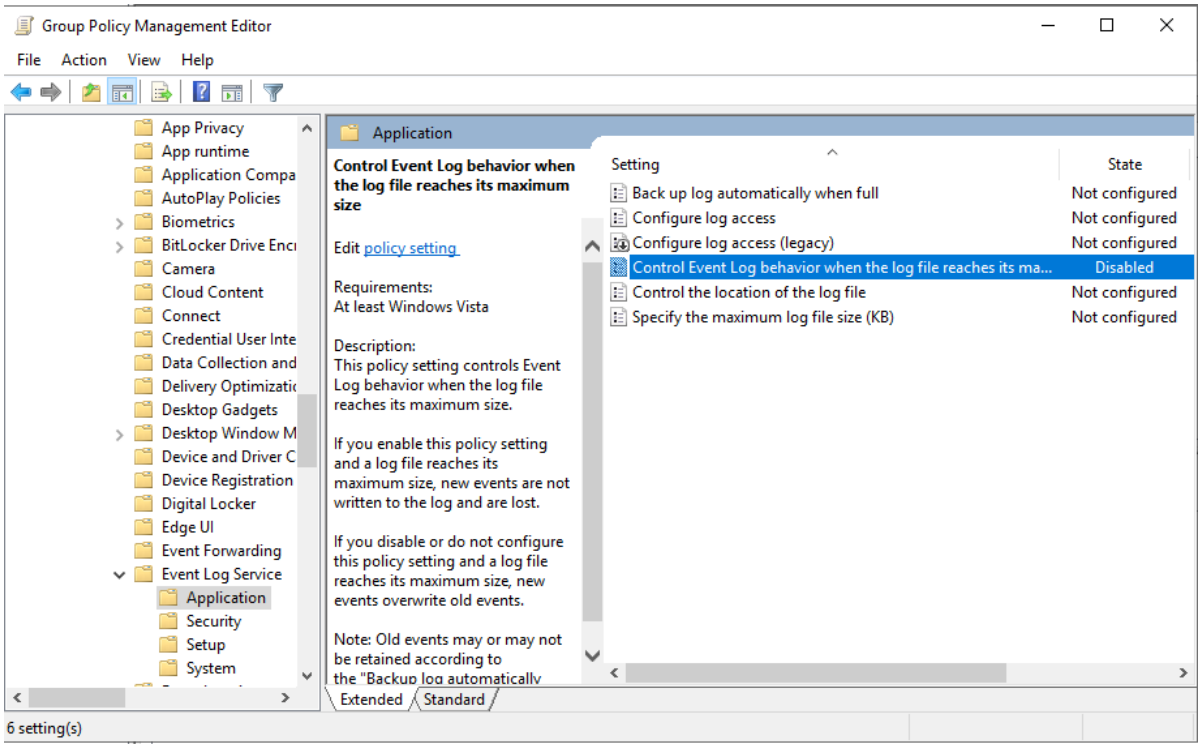


Image 257-Ensure 'Application: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'

7.8.10.1.2 Ensure 'Application: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'

This policy setting manages the behavior of Event Logs when they reach their maximum size. The recommended state for this setting is: Disabled. The retention of old events depends on the "Backup log automatically when full" policy setting. Disabling this setting could prevent new events from being recorded, which may hinder the ability to diagnose system issues or detect unauthorized activities.

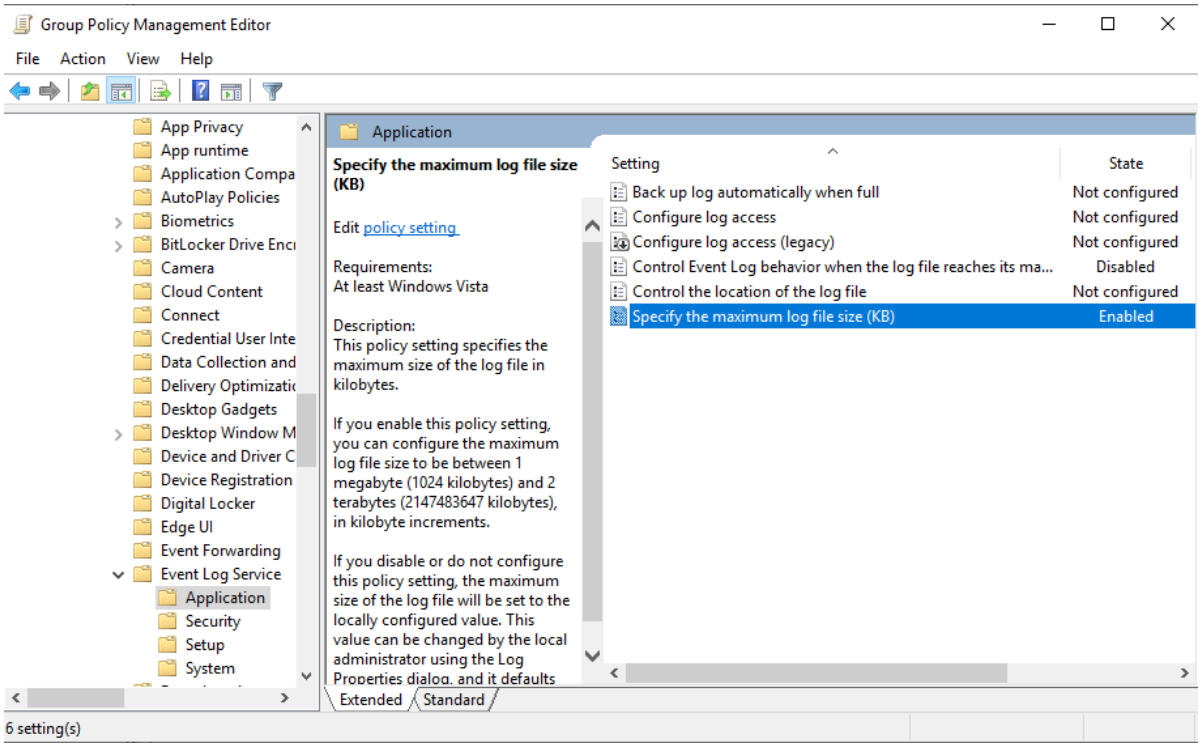


Image 258-Ensure 'Application: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'

7.8.10.2 Security

7.8.10.2.1 Ensure 'Security: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'

This policy setting controls how the Event Log behaves when it reaches its maximum size. The recommended state is Disabled. If new events aren't recorded, it may be challenging to diagnose system issues or detect unauthorized activities.

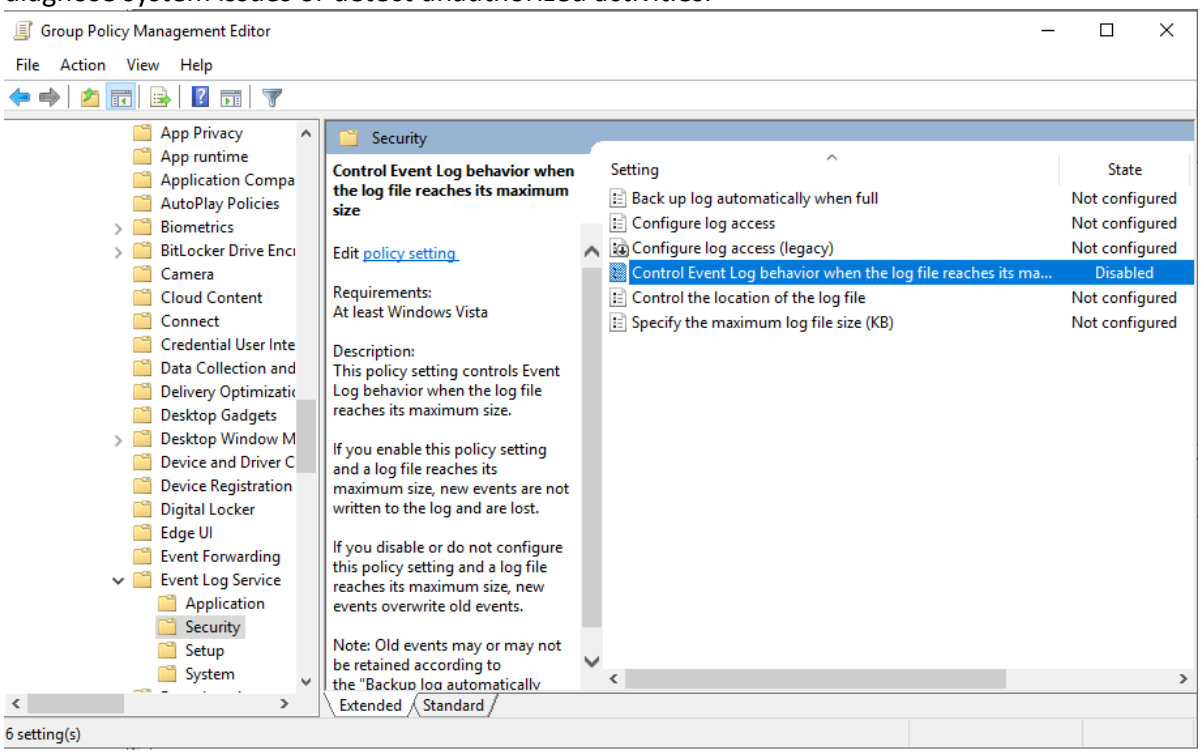


Image 259-Ensure 'Security: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'

7.8.10.2.2 Ensure 'Security: Specify the maximum log file size (KB)' is set to 'Enabled: 196,608 or greater'

This policy setting defines the maximum log file size in kilobytes, ranging from 1 MB (1,024 KB) to 4 TB (4,194,240 KB). The recommended configuration is Enabled with a size of 196,608 KB or more. If events are not logged, identifying the cause of system issues or unauthorized actions may become difficult.

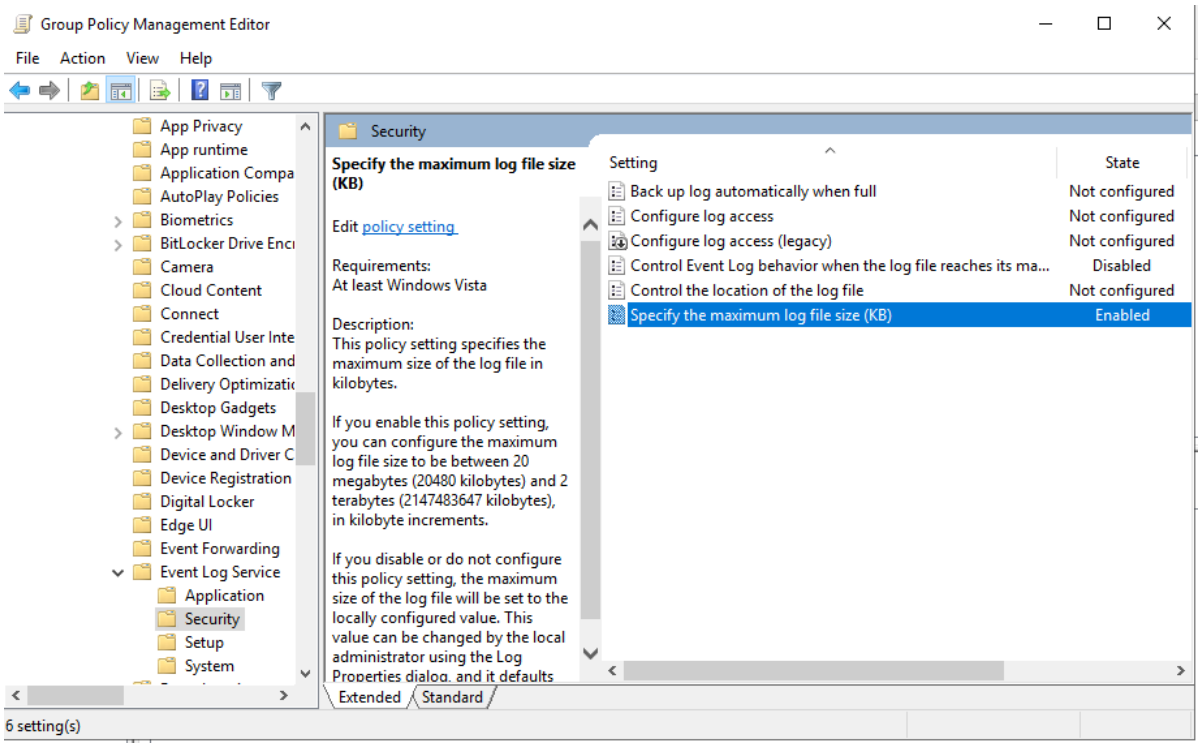


Image 260-Ensure 'Security: Specify the maximum log file size (KB)' is set to 'Enabled: 196,608 or greater'

7.8.10.3 Setup

7.8.10.3.1 Ensure 'Setup: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'

This policy setting manages how the Event Log behaves when it reaches its maximum size. The recommended configuration is Disabled. If new events are not recorded, it may be challenging to trace system issues or detect unauthorized activities.

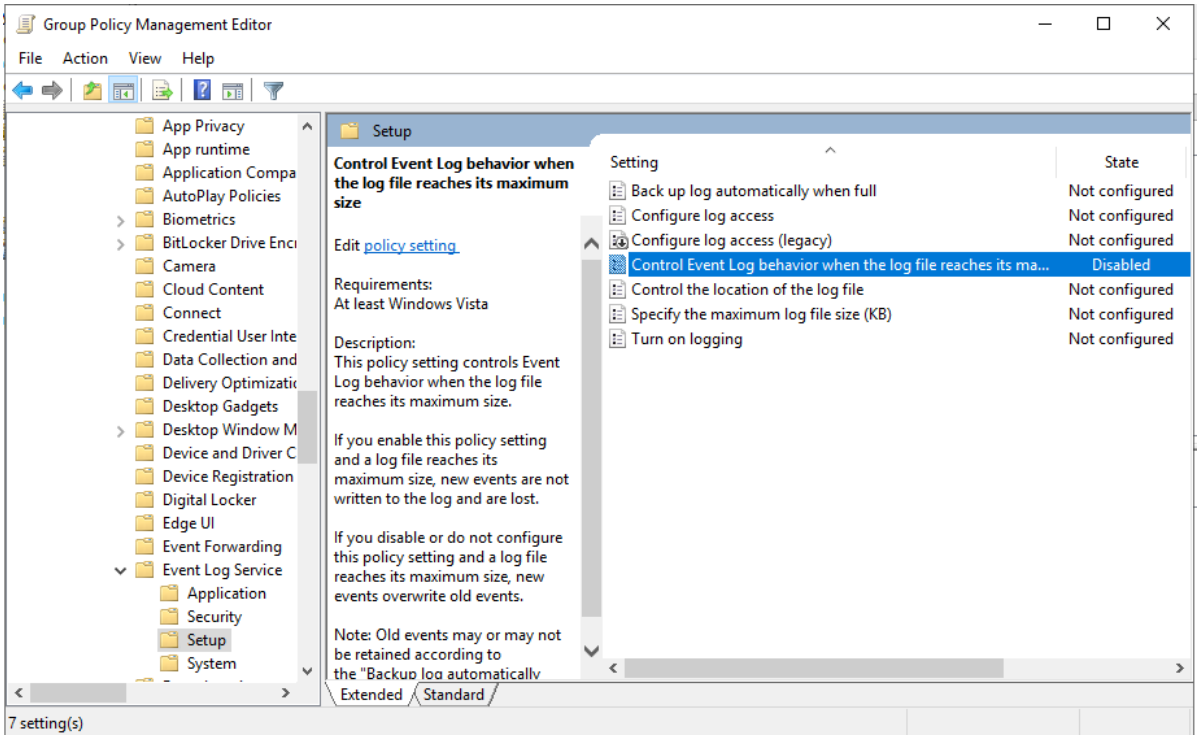


Image 261-Ensure 'Setup: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'

7.8.10.3.2 Ensure 'Setup: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'

This policy setting defines the maximum size of the log file in kilobytes, which can range from 1 megabyte to 4 terabytes in kilobyte increments. The recommended configuration is Enabled with a size of 32,768 kilobytes or more. If events are not logged, identifying system issues or unauthorized activities may become difficult.

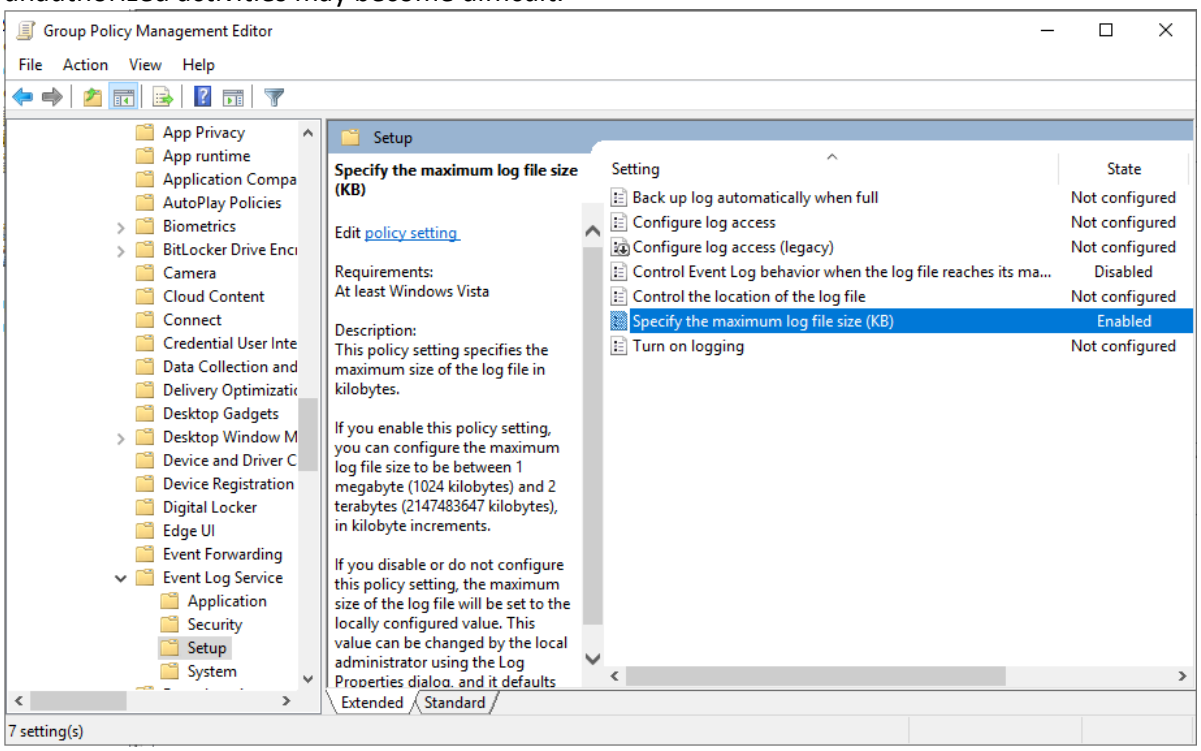


Image 262-Ensure 'Setup: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'

7.8.10.4 System

7.8.10.4.1 Ensure 'System: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'

This policy setting manages how the Event Log behaves when it reaches its maximum size. The recommended state is Disabled. If new events are not logged, it can hinder the ability to identify system issues or detect unauthorized activities.

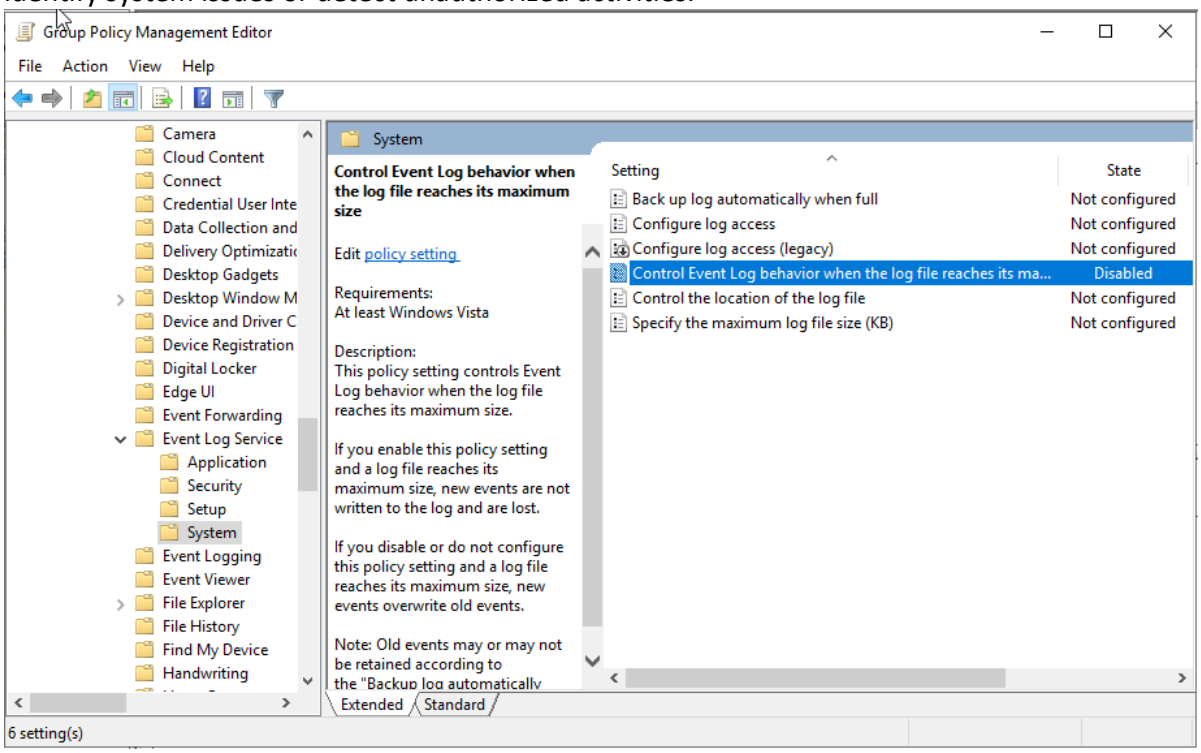


Image 263-Ensure 'System: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'

7.8.10.4.2 Ensure 'System: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'

This policy setting defines the maximum log file size in kilobytes, which can range from 1 megabyte (1,024 KB) to 4 terabytes (4,194,240 KB) in kilobyte increments. The recommended configuration is to enable this setting with a size of 32,768 KB or more. Proper event recording is essential for diagnosing system issues and detecting unauthorized activities.

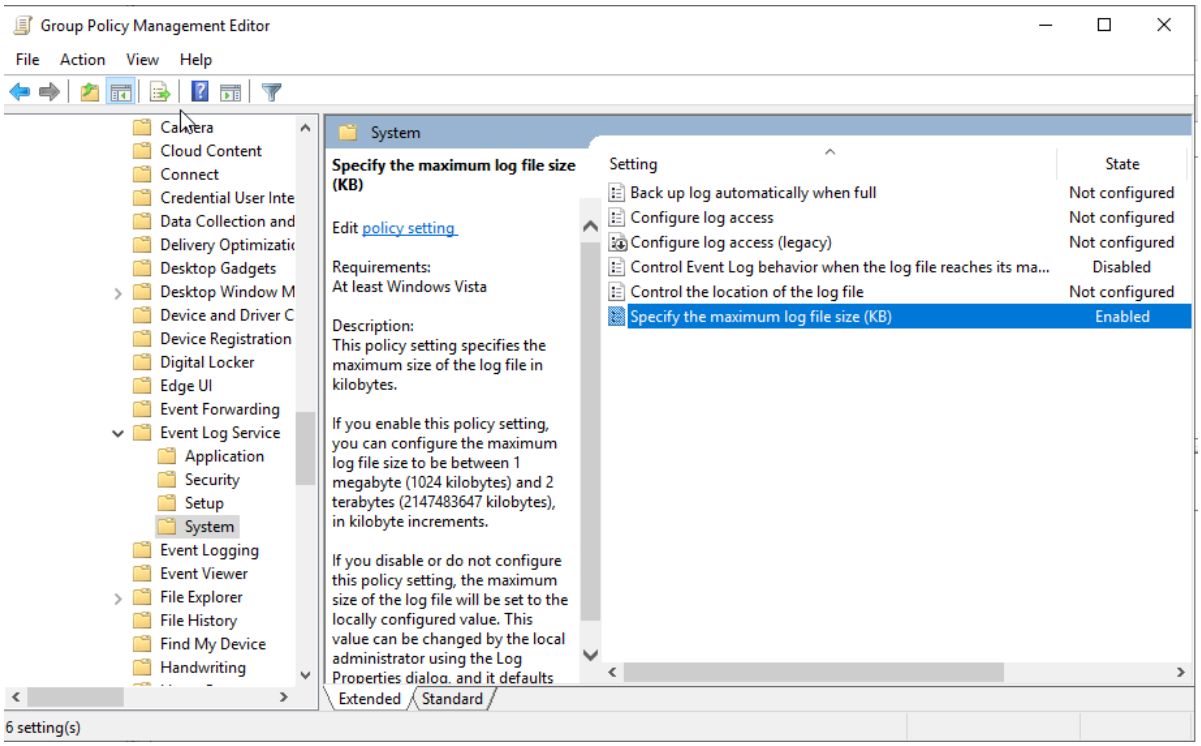


Image 264-Ensure 'System: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'

7.8.11 File Explorer (formerly Windows Explorer)

7.8.11.1 Ensure 'Turn off Data Execution Prevention for Explorer' is set to 'Disabled'

Disabling Data Execution Prevention (DEP) can allow certain legacy plug-in applications to function without causing Explorer to terminate. The recommended setting is to keep DEP enabled (Disabled for this policy setting). DEP is a crucial security feature in Explorer that helps mitigate the impact of specific types of malware. Exceptions may be needed for legacy software that is incompatible with DEP.

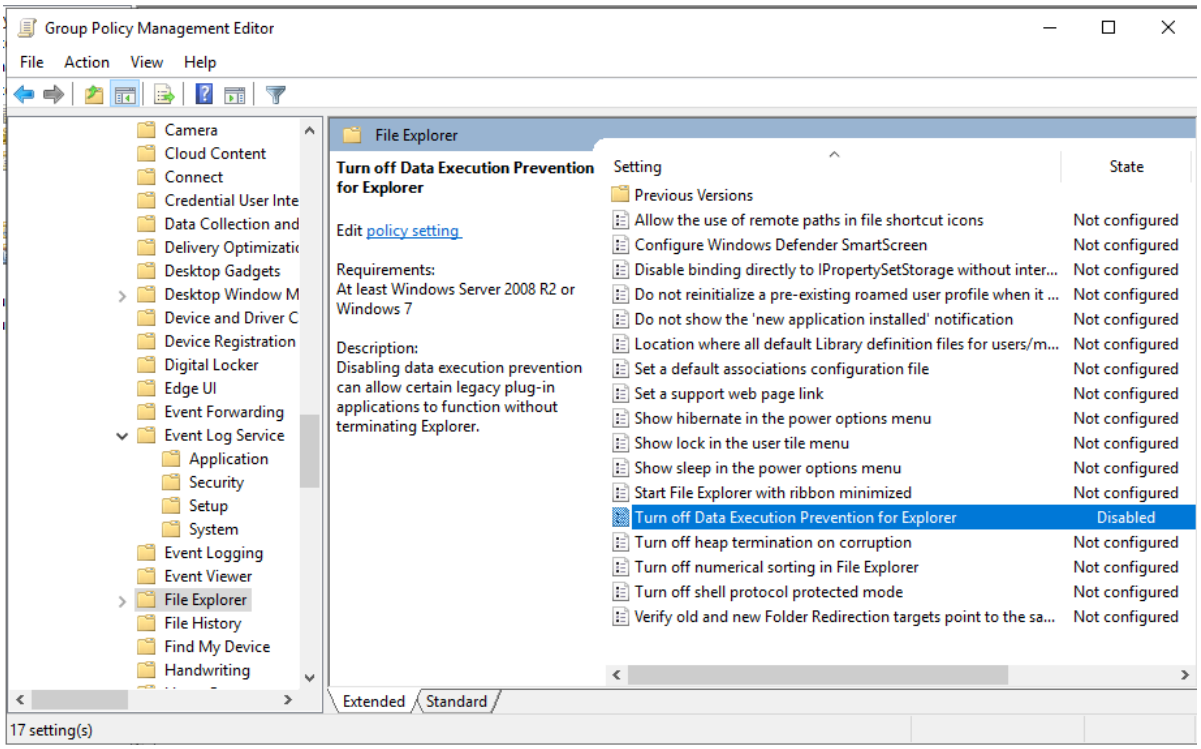


Image 265-Ensure 'Turn off Data Execution Prevention for Explorer' is set to 'Disabled'

7.8.11.2 Ensure 'Turn off heap termination on corruption' is set to 'Disabled'

Without heap termination on corruption, legacy plug-in applications might continue to run even when a File Explorer session is corrupted. Enabling heap termination on corruption prevents this. The recommended setting is to disable this policy. Allowing applications to run after a session becomes corrupt increases the system's security risk.

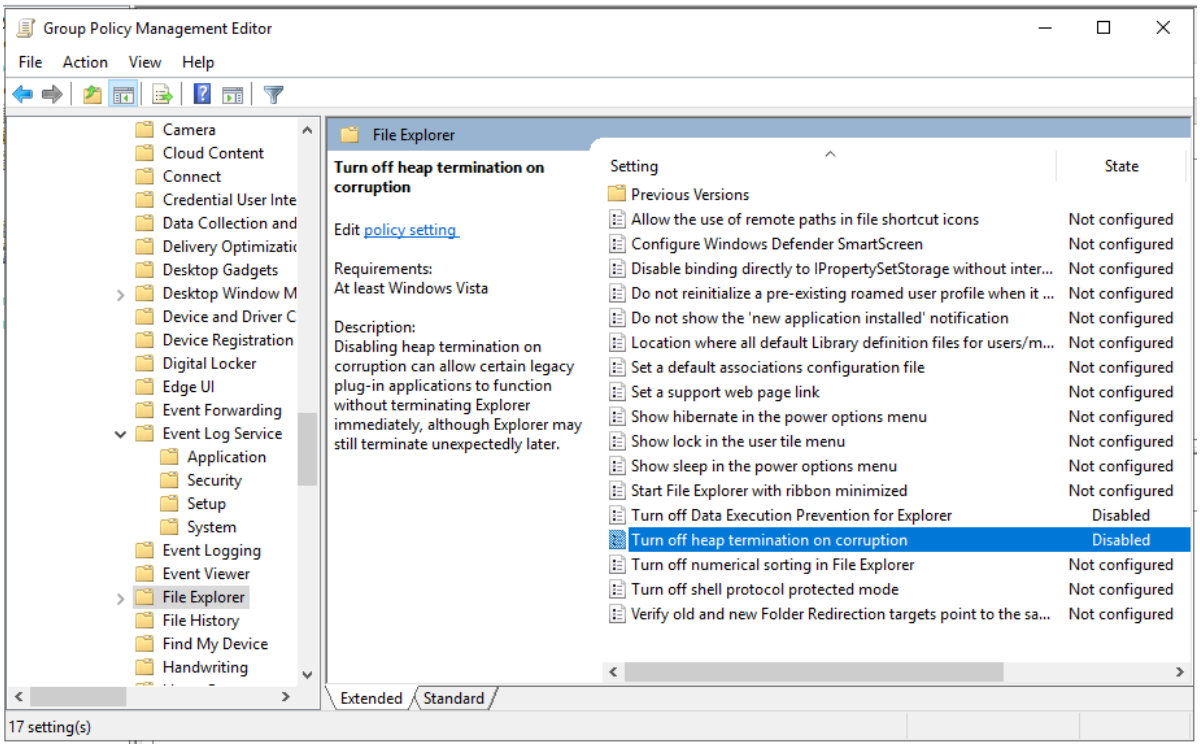


Image 266-Ensure 'Turn off heap termination on corruption' is set to 'Disabled'

7.8.11.3 Ensure 'Turn off shell protocol protected mode' is set to 'Disabled'

This policy setting configures the shell protocol's functionality. In full mode, applications can open folders and launch files, while in protected mode, they can only access a limited set of folders and cannot open files. It is recommended to keep this protocol in protected mode to enhance security. The recommended state for this setting is Disabled, as restricting file and folder access reduces the system's attack surface.

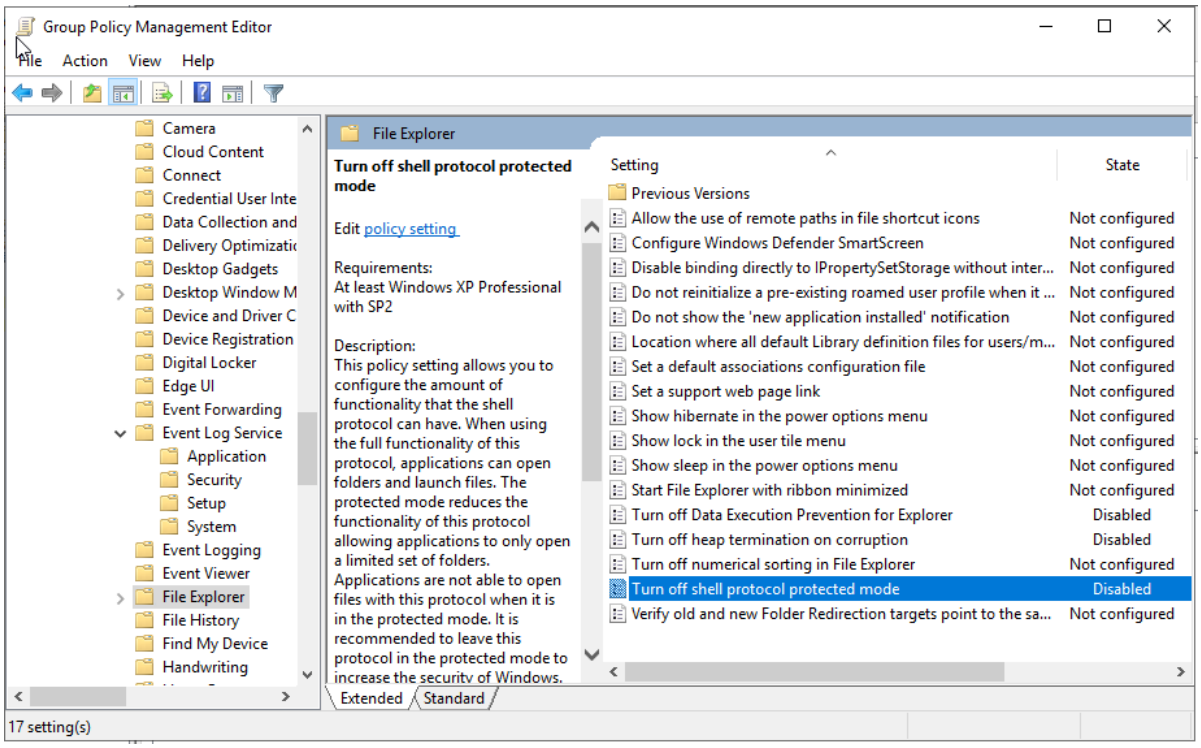


Image 267-Ensure 'Turn off shell protocol protected mode' is set to 'Disabled'

7.8.12 Location and Sensors

7.8.12.1 Ensure 'Turn off shell protocol protected mode' is set to 'Disabled'

This policy setting disables the location feature on the computer. The recommended state for this setting is Enabled. Disabling location services prevents software from accessing location data, which enhances security by reducing the risk of exposing your location. While there are legitimate uses for location tracking, such as mapping software, it is generally not advisable to enable these features in high-security environments.

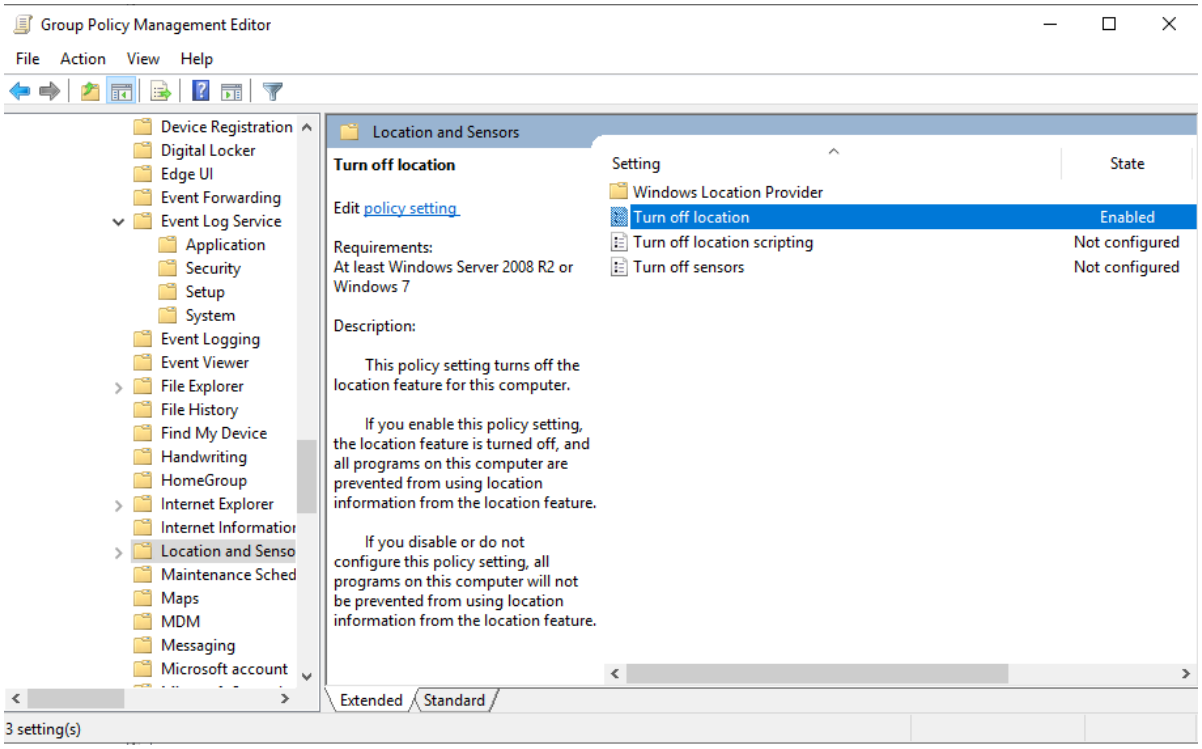


Image 268-Ensure 'Turn off shell protocol protected mode' is set to 'Disabled'

7.8.13 Messaging

7.8.13.1 Ensure 'Allow Message Service Cloud Sync' is set to 'Disabled'

This policy setting controls whether cellular text messages can be backed up and restored through Microsoft's cloud services. The recommended state for this setting is Disabled. In high-security environments, sending data to third-party services is discouraged as it may include sensitive information.

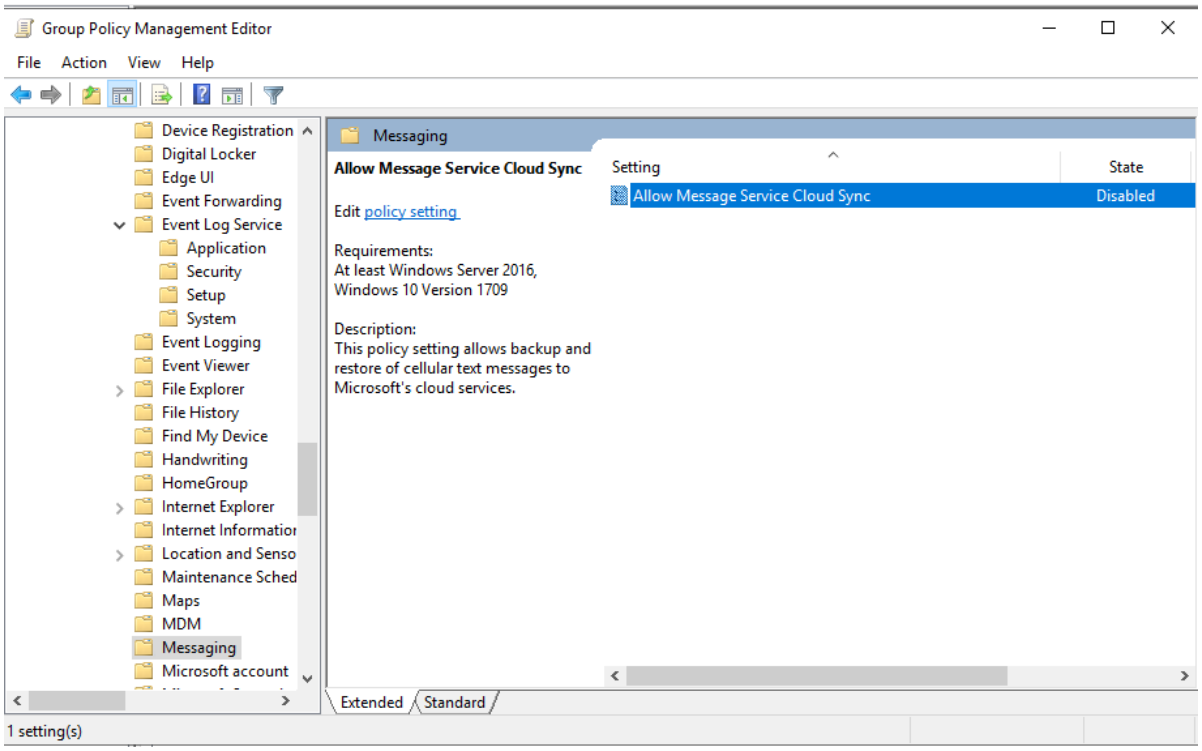


Image 269-Ensure 'Allow Message Service Cloud Sync' is set to 'Disabled'

7.8.14 Microsoft account

7.8.14.1 Ensure 'Block all consumer Microsoft account user authentication' is set to 'Enabled'

This setting controls whether applications and services on the device can use Microsoft account authentication through the Windows OnlineID and WebAccountManager APIs. The recommended state for this setting is Enabled. Organizations seeking to enforce identity management policies and maintain strict control over account usage on their computers should consider blocking Microsoft accounts, as this may also be necessary to comply with relevant information system standards.

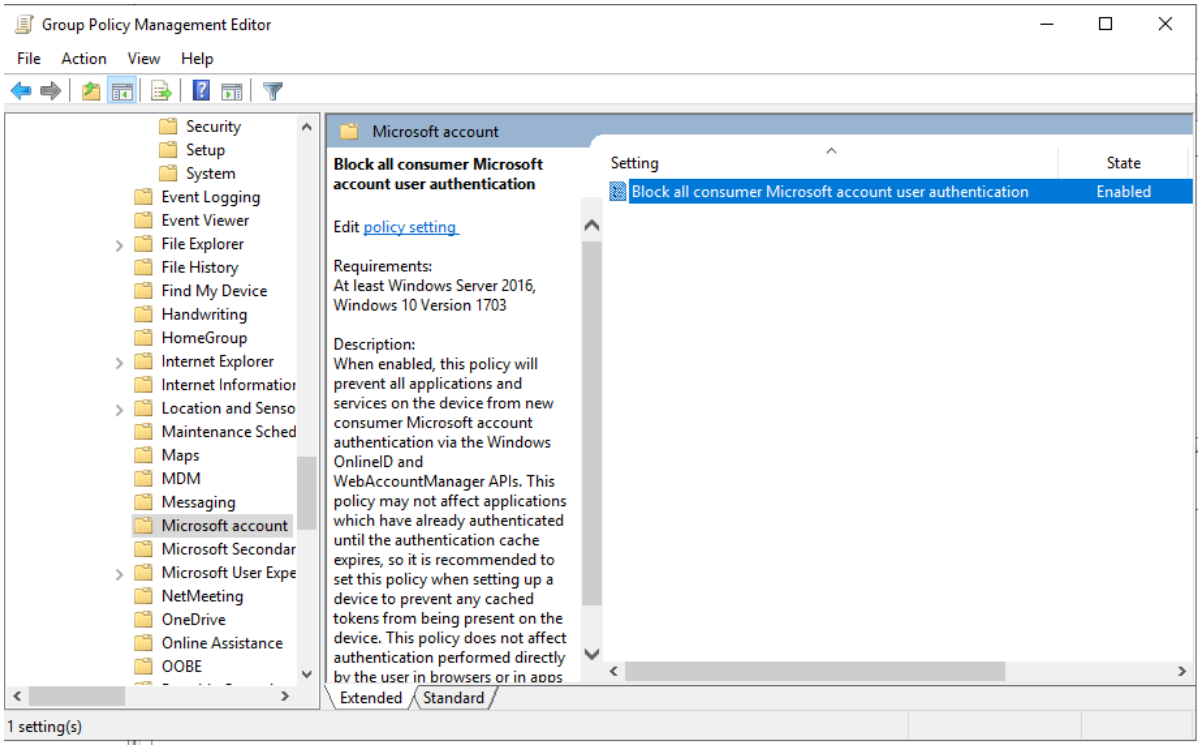


Image 270-Ensure 'Block all consumer Microsoft account user authentication' is set to 'Enabled'

7.8.15 Microsoft account

7.8.15.1 Microsoft Defender Exploit Guard (formerly Windows Defender Exploit Guard)

7.8.15.1.1 Attack Surface Reduction

7.8.15.1.1.1 Ensure 'Configure Attack Surface Reduction rules' is set to 'Enabled'

This policy setting manages the status of Attack Surface Reduction (ASR) rules. It is recommended to keep this setting enabled. Attack surface reduction is designed to block actions and applications commonly exploited by malware to compromise systems.

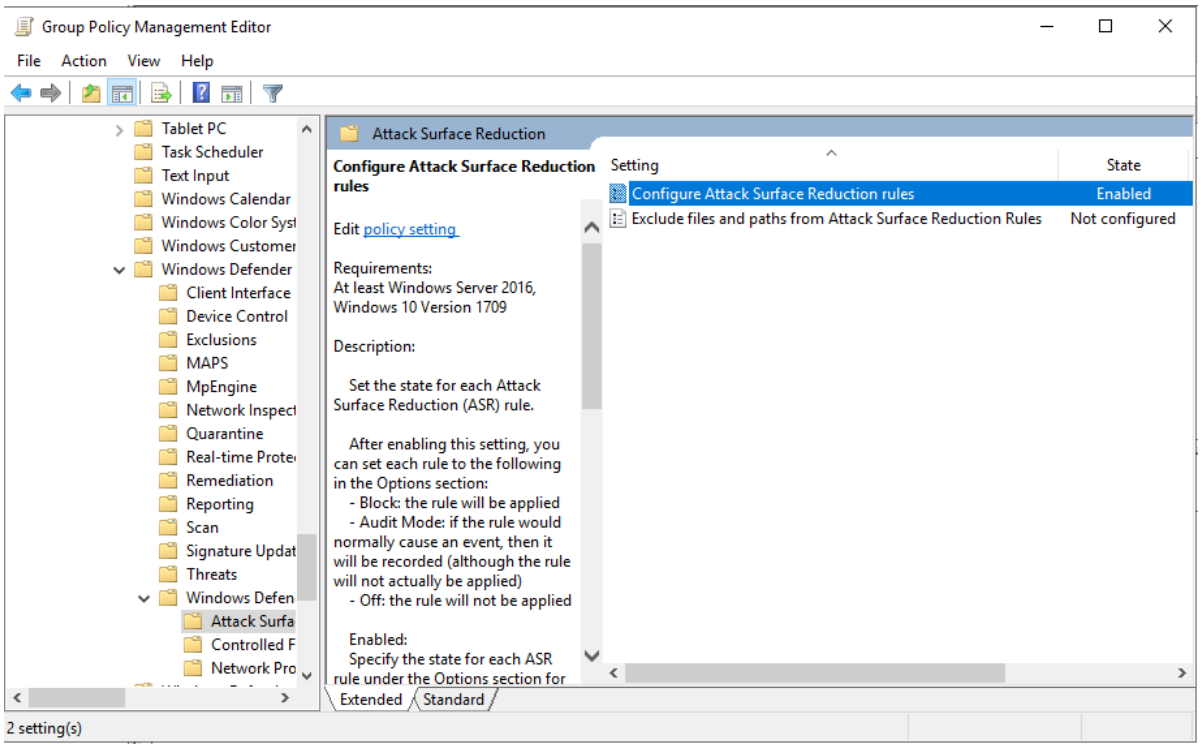


Image 271-Ensure 'Configure Attack Surface Reduction rules' is set to 'Enabled'

7.8.15.1.2 Network Protection

7.8.15.1.2.1 Ensure 'Prevent users and apps from accessing dangerous websites' is set to 'Enabled: Block'

This policy setting manages Microsoft Defender Exploit Guard network protection. The recommended configuration is to enable it with the "Block" option. This setting helps prevent employees from using applications to access harmful domains that could host phishing scams, exploit sites, and other malicious content online.

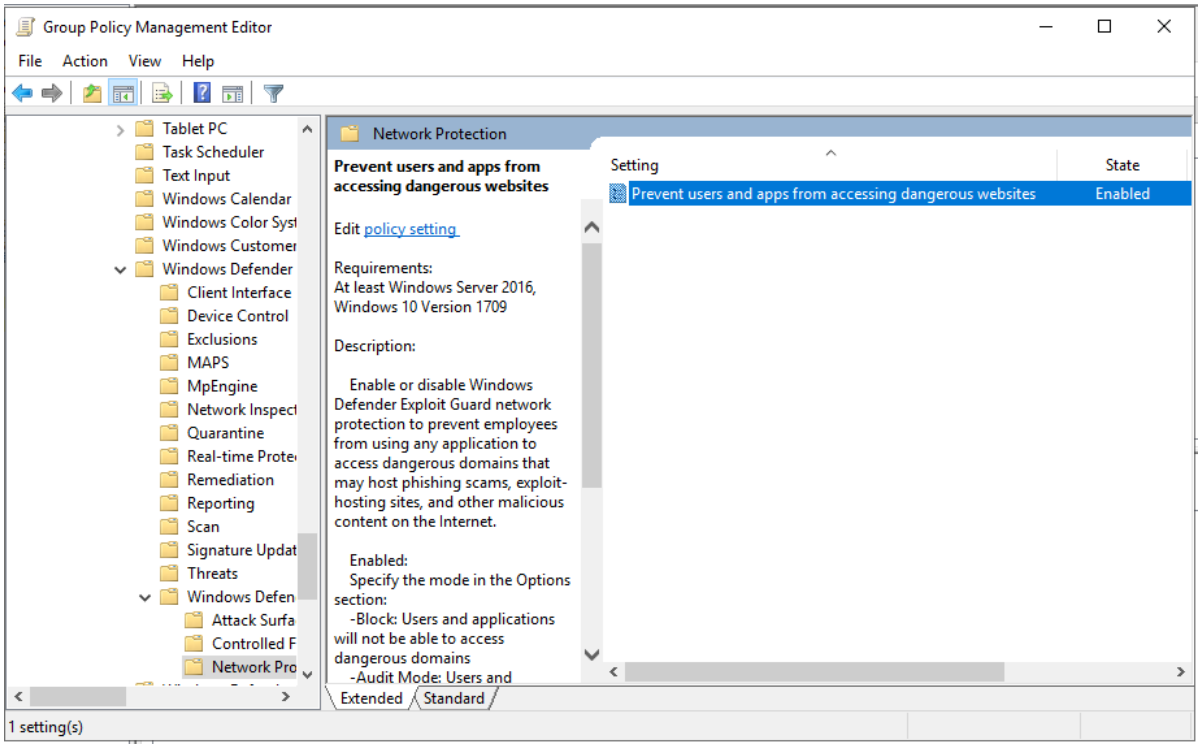


Image 272-Ensure 'Prevent users and apps from accessing dangerous websites' is set to 'Enabled: Block'

7.8.15.2 Real-time Protection

7.8.15.2.1 Ensure 'Scan all downloaded files and attachments' is set to 'Enabled'

This policy setting controls whether all downloaded files and attachments are scanned. The recommended configuration is to enable this feature. Ensuring that antivirus solutions like Microsoft Defender Antivirus are set to scan these files helps to detect and monitor for both suspicious and known malicious activity in real-time.

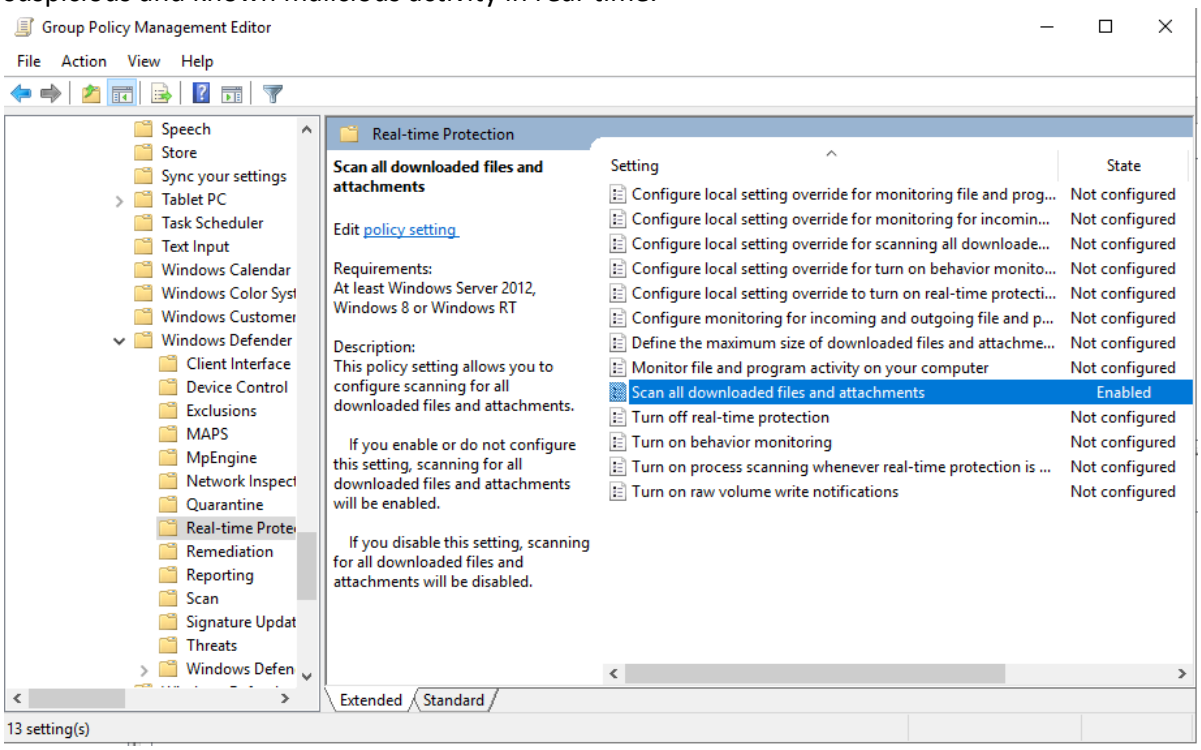


Image 273-Ensure 'Scan all downloaded files and attachments' is set to 'Enabled'

7.8.15.2.2 Ensure 'Turn off real-time protection' is set to 'Disabled'

This policy setting determines whether real-time protection alerts are shown for detected malware. Microsoft Defender Antivirus will notify you if malware or potentially unwanted software tries to install or execute on your computer. The recommended configuration for this setting is to disable it. It's crucial to ensure that antivirus solutions like Microsoft Defender Antivirus are set up to effectively monitor for suspicious and known malicious activities in real-time.

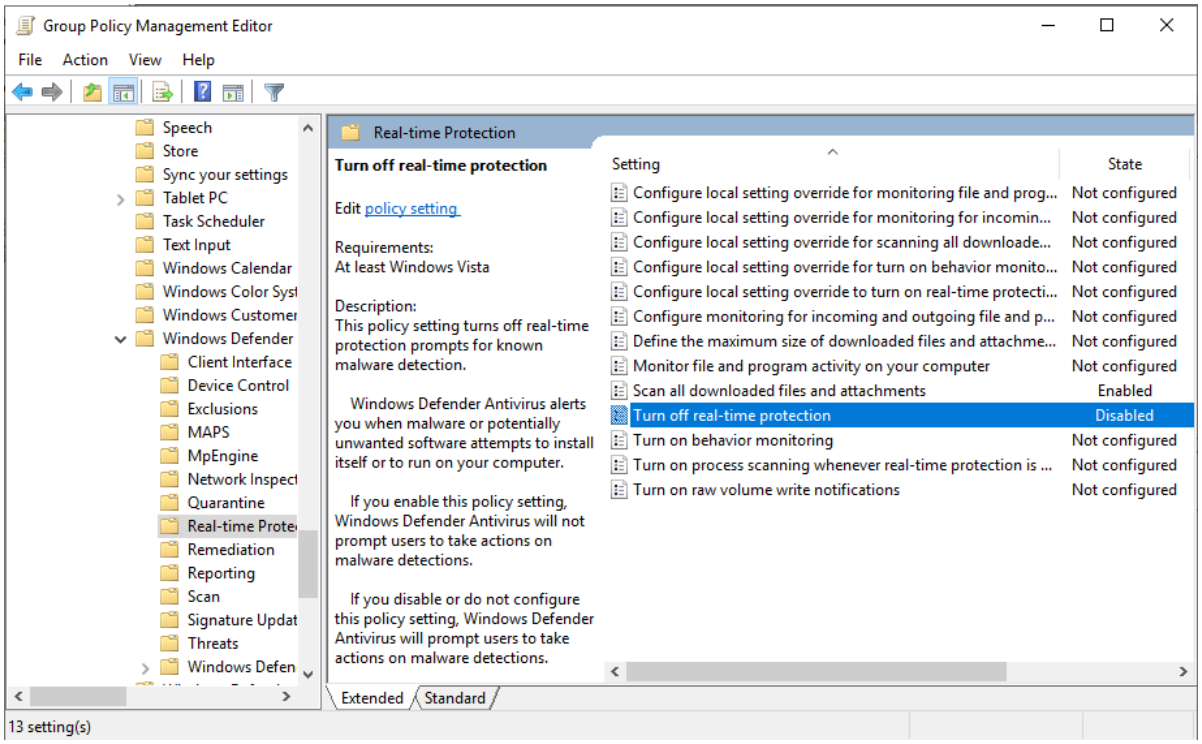


Image 274-Ensure 'Turn off real-time protection' is set to 'Disabled'

7.8.15.2.3 Ensure 'Turn on behavior monitoring' is set to 'Enabled'

This policy setting enables you to configure behavior monitoring for Microsoft Defender Antivirus. It is recommended to keep this setting enabled. Proper configuration of behavior monitoring is essential for detecting suspicious and known malicious activities in real time with Microsoft Defender Antivirus.

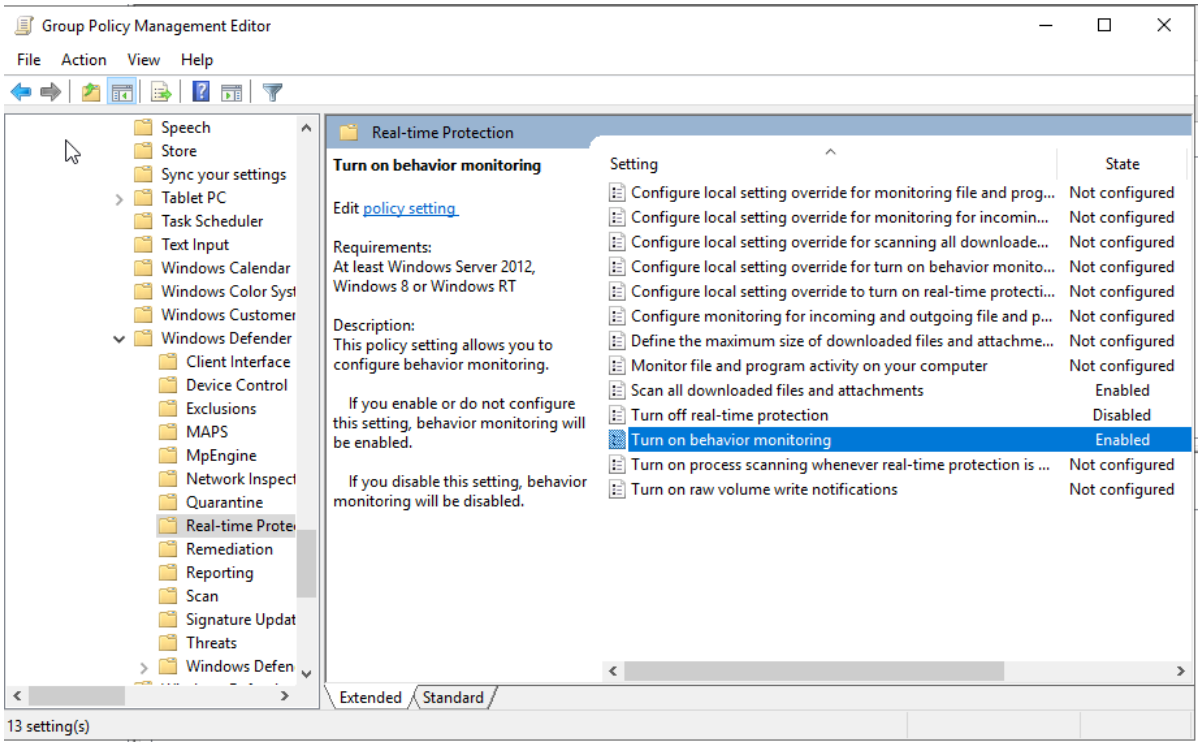


Image 275-Ensure 'Turn on behavior monitoring' is set to 'Enabled'

7.8.15.3 Reporting

7.8.15.3.1 Ensure 'Configure Watson events' is set to 'Disabled'

This policy setting determines whether Watson events, which are reports sent to Microsoft when a program or service crashes or fails, are transmitted. The recommended state for this setting is to disable it. Disabling Watson events can help address privacy concerns by preventing potentially sensitive information from being sent to Microsoft.

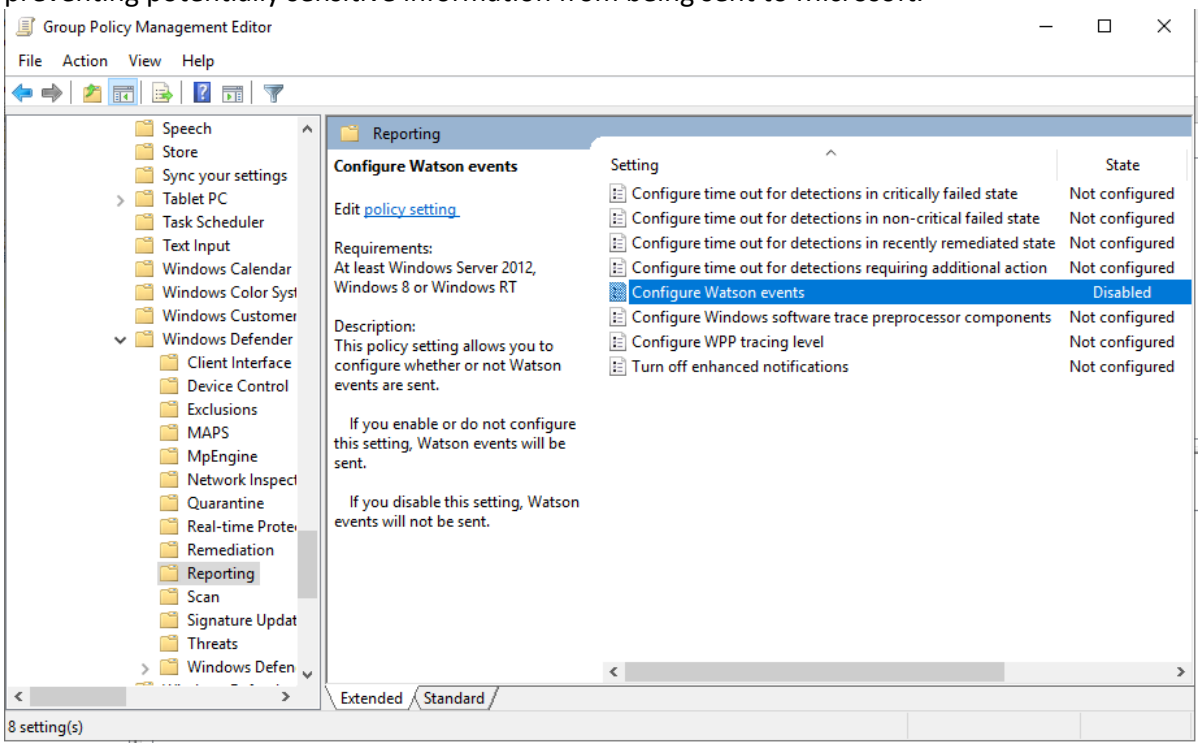


Image 276-Ensure 'Configure Watson events' is set to 'Disabled'

7.8.15.4 Scan

7.8.15.4.1 Ensure 'Scan removable drives' is set to 'Enabled'

This policy setting lets you control whether malicious and unwanted software on removable drives, like USB flash drives, is scanned during a full scan. The recommended configuration for this setting is to enable it. Ensuring that removable drives are included in scans is crucial, as these drives are more likely to carry malicious software from external, unmanaged sources into a managed environment.

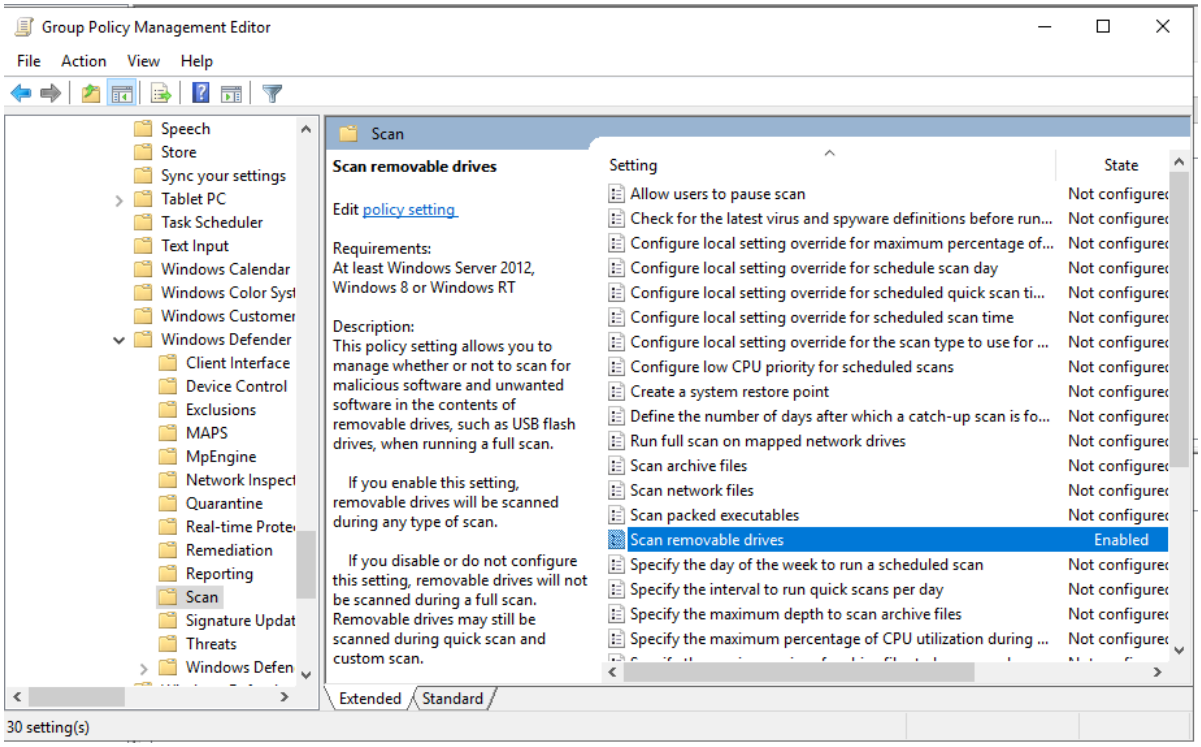


Image 277-Ensure 'Scan removable drives' is set to 'Enabled'

7.8.15.4.2 Ensure 'Turn on e-mail scanning' is set to 'Enabled'

This policy setting allows you to configure email scanning. When enabled, the scanning engine examines mailbox and mail files in their specific formats, such as pst (Outlook), dbx, mbx, mime (Outlook Express), and binhex (Mac), to analyze email bodies and attachments. The recommended setting is to enable this feature. Scanning incoming emails with an antivirus solution like Microsoft Defender Antivirus is crucial, as email attachments are a common method for delivering malicious software.

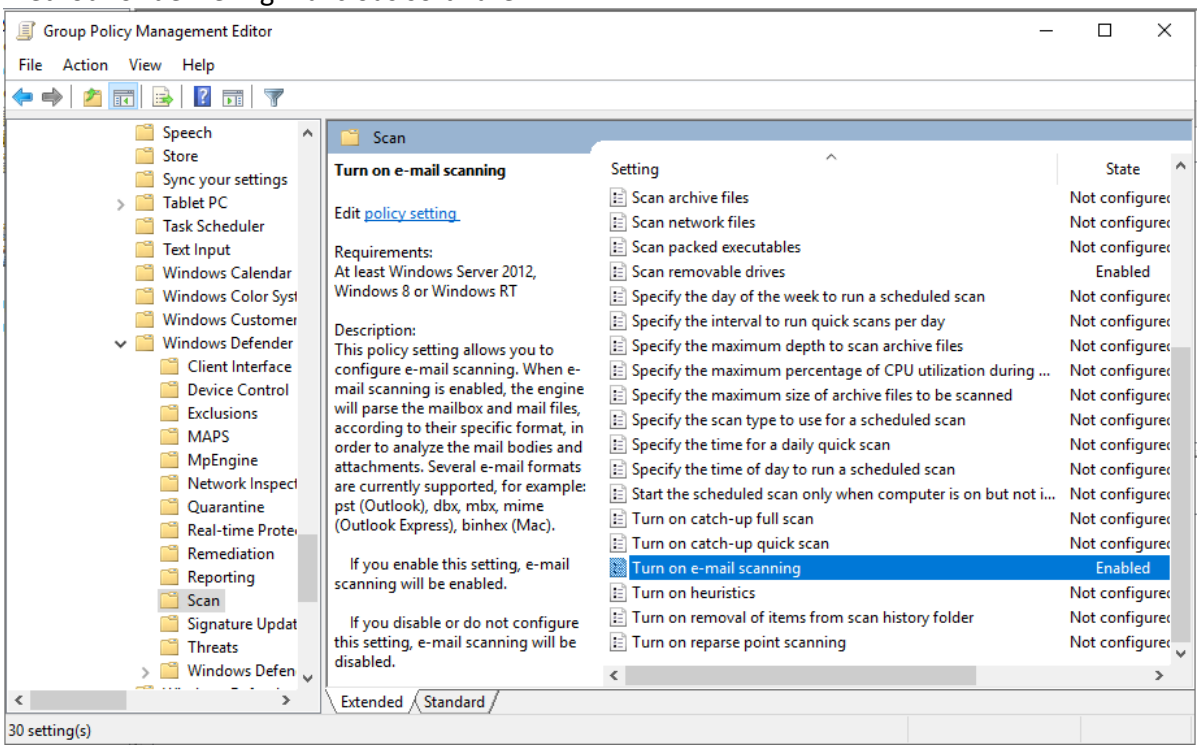


Image 278-Ensure 'Turn on e-mail scanning' is set to 'Enabled'

7.8.15.5 Ensure 'Configure detection for potentially unwanted applications' is set to 'Enabled: Block'

This policy setting governs the detection and handling of Potentially Unwanted Applications (PUAs), which are deceptive application bundlers or their bundled applications that can introduce adware or malware. The recommended state for this setting is to enable blocking. PUAs pose a risk to network security by potentially leading to malware infections, complicating malware identification, and consuming IT resources for cleanup. Therefore, blocking their installation is advisable. For further details, refer to the Microsoft Docs link on blocking potentially unwanted applications with Microsoft Defender Antivirus.

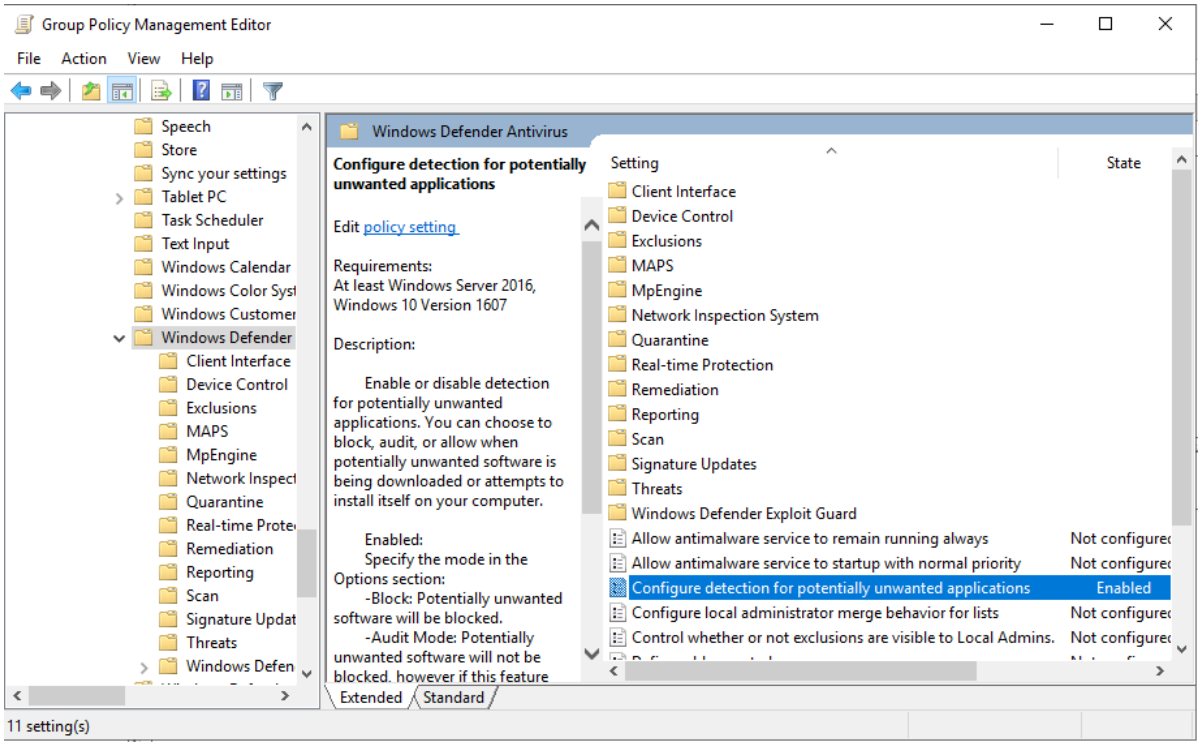


Image 279-Ensure 'Configure detection for potentially unwanted applications' is set to 'Enabled: Block'

7.8.15.6 Ensure 'Turn off Microsoft Defender AntiVirus' is set to 'Disabled'

This policy setting controls whether Microsoft Defender Antivirus is enabled or disabled. When this setting is disabled, Microsoft Defender Antivirus remains active and continues to scan computers for malware and other potentially unwanted software. The recommended state for this setting is disabled to ensure that Microsoft Defender Antivirus, which is a robust and up-to-date antivirus solution, actively protects each computer. However, organizations that opt for a reputable third-party antivirus solution may choose to disable Microsoft Defender Antivirus in favor of their commercial alternative.

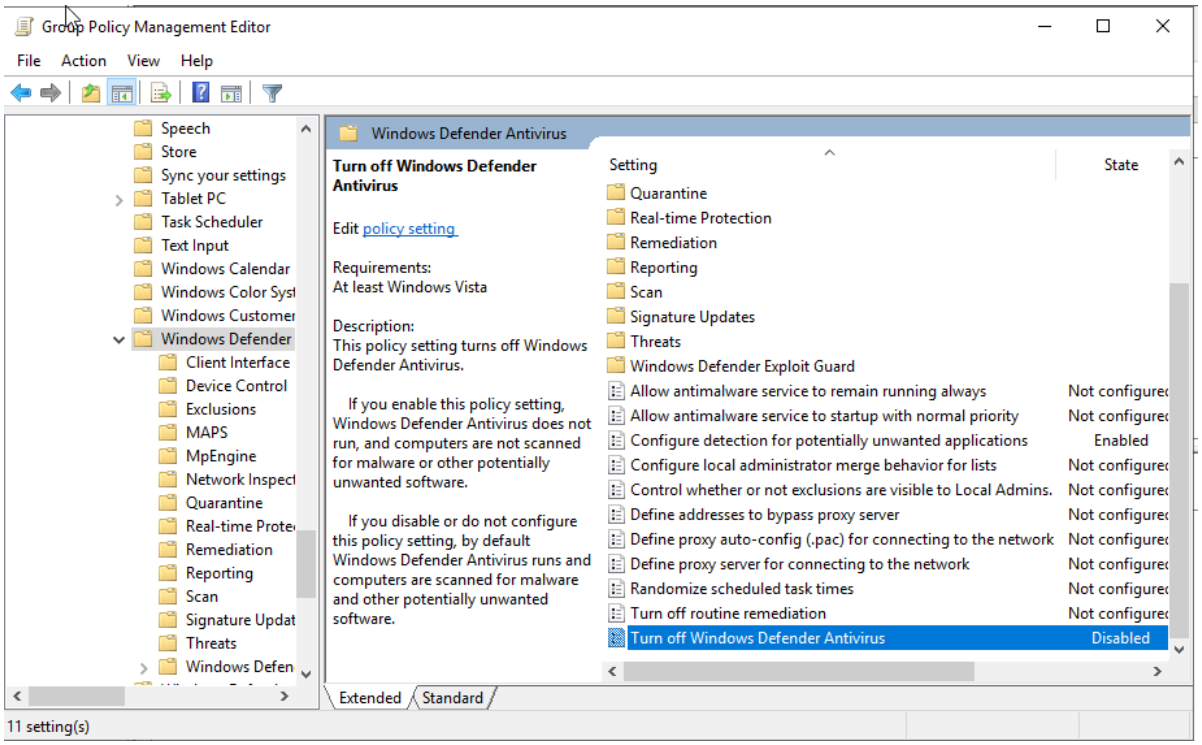


Image 280-Ensure 'Turn off Microsoft Defender AntiVirus' is set to 'Disabled'

7.8.16 OneDrive (formerly SkyDrive)

7.8.16.1 Ensure 'Prevent the usage of OneDrive for file storage' is set to 'Enabled'

This policy setting allows you to restrict apps and features from accessing files on OneDrive via the Next Generation Sync Client. The recommended state for this setting is enabled to prevent users from inadvertently or deliberately uploading sensitive corporate information to the OneDrive cloud service. This precaution is relevant for any cloud-based file storage application installed on a server, not just the one provided with Windows Server.

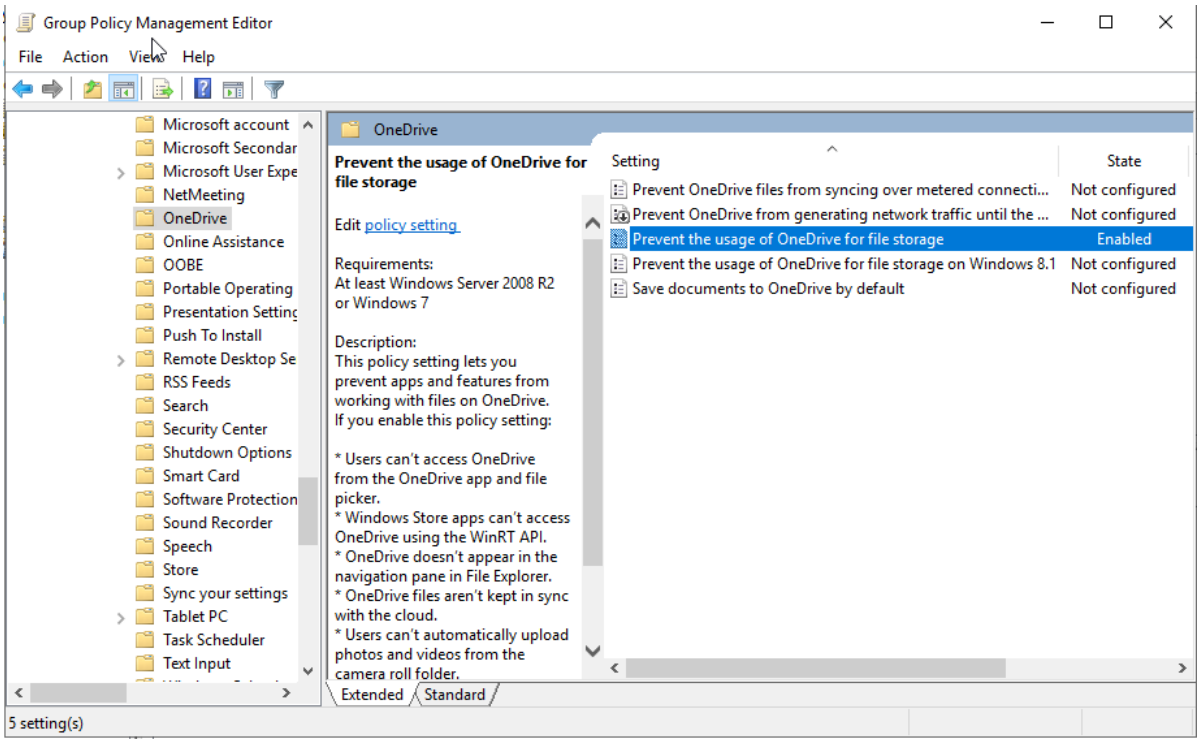


Image 281-Ensure 'Prevent the usage of OneDrive for file storage' is set to 'Enabled'

7.8.17 Push To Install

7.8.17.1 Ensure 'Prevent the usage of OneDrive for file storage' is set to 'Enabled'

This policy setting regulates whether users are allowed to install apps on their device from the Microsoft Store App on other devices or the web. The recommended state for this setting is enabled to ensure that in a high-security environment, application installations are controlled centrally by IT staff rather than by end users.

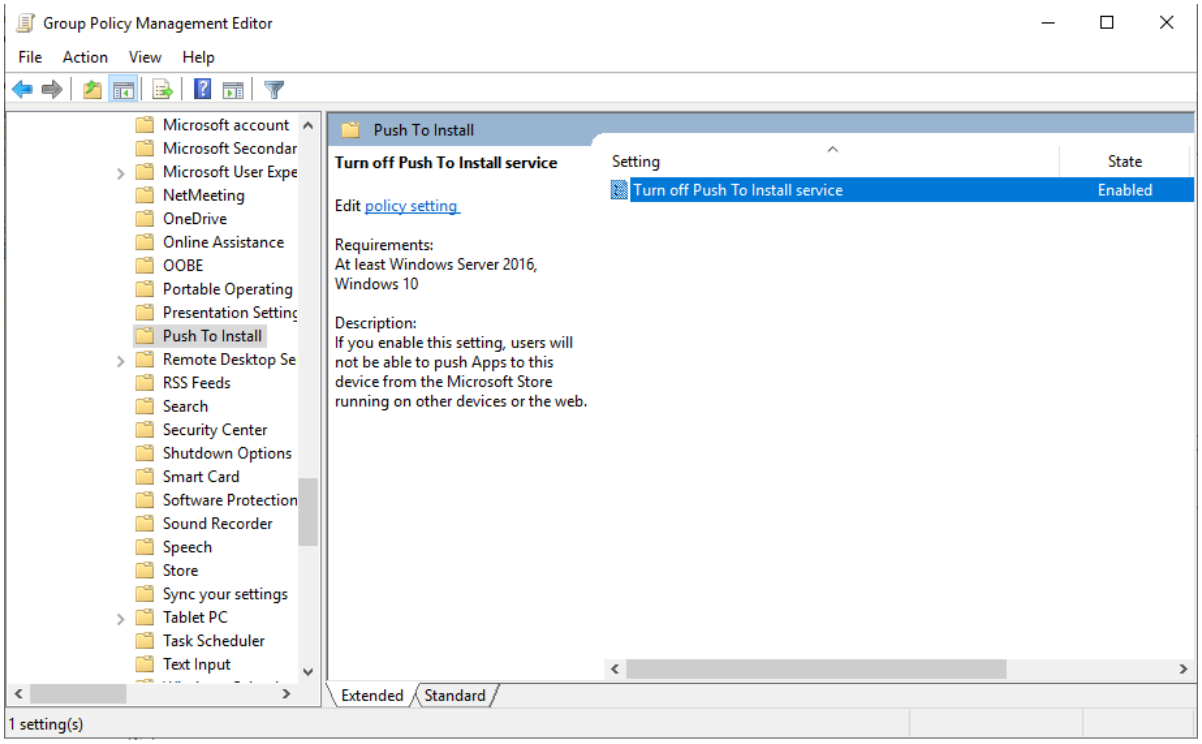


Image 282-Ensure 'Prevent the usage of OneDrive for file storage' is set to 'Enabled'

7.8.18 Remote Desktop Services (formerly Terminal Services)

7.8.18.1 Remote Desktop Connection Client

7.8.18.1.1 Ensure 'Do not allow passwords to be saved' is set to 'Enabled'

This policy setting prevents Remote Desktop clients from saving passwords on a computer. The recommended state for this setting is enabled. If this policy was previously set to disabled or not configured, any saved passwords will be deleted when the Remote Desktop client first disconnects from a server. This measure helps protect against the risk of an attacker gaining access to additional hosts if they have physical access to the computer or compromise a user's account.

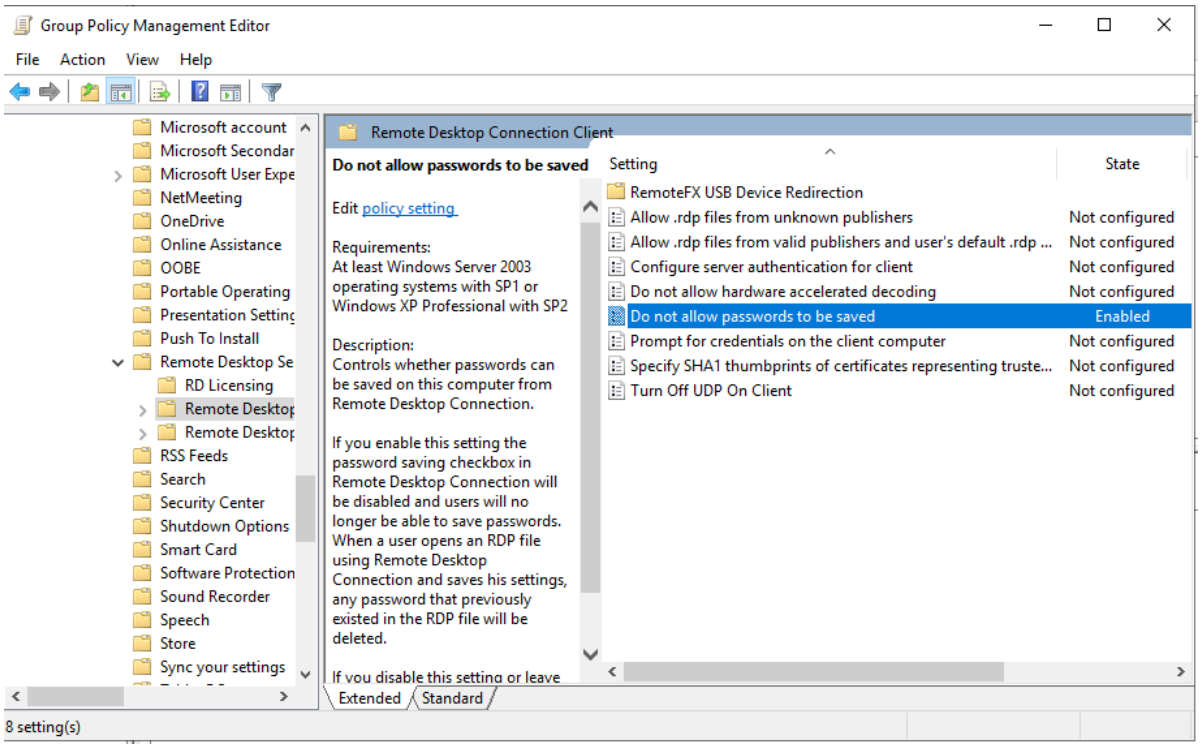


Image 283-Ensure 'Do not allow passwords to be saved' is set to 'Enabled'

7.8.18.2 Remote Desktop Session Host (formerly Terminal Server)

7.8.18.2.1 Connections

7.8.18.2.1.1 Ensure 'Restrict Remote Desktop Services users to a single Remote Desktop Services session' is set to 'Enabled'

This policy setting restricts users to a single Remote Desktop Services session. The recommended state for this setting is enabled. This ensures that users and administrators reconnect to the same session if they disconnect, rather than creating a new session. This approach helps prevent excessive resource usage on the server and maintains a consistent user experience by avoiding unnecessary additional sessions.

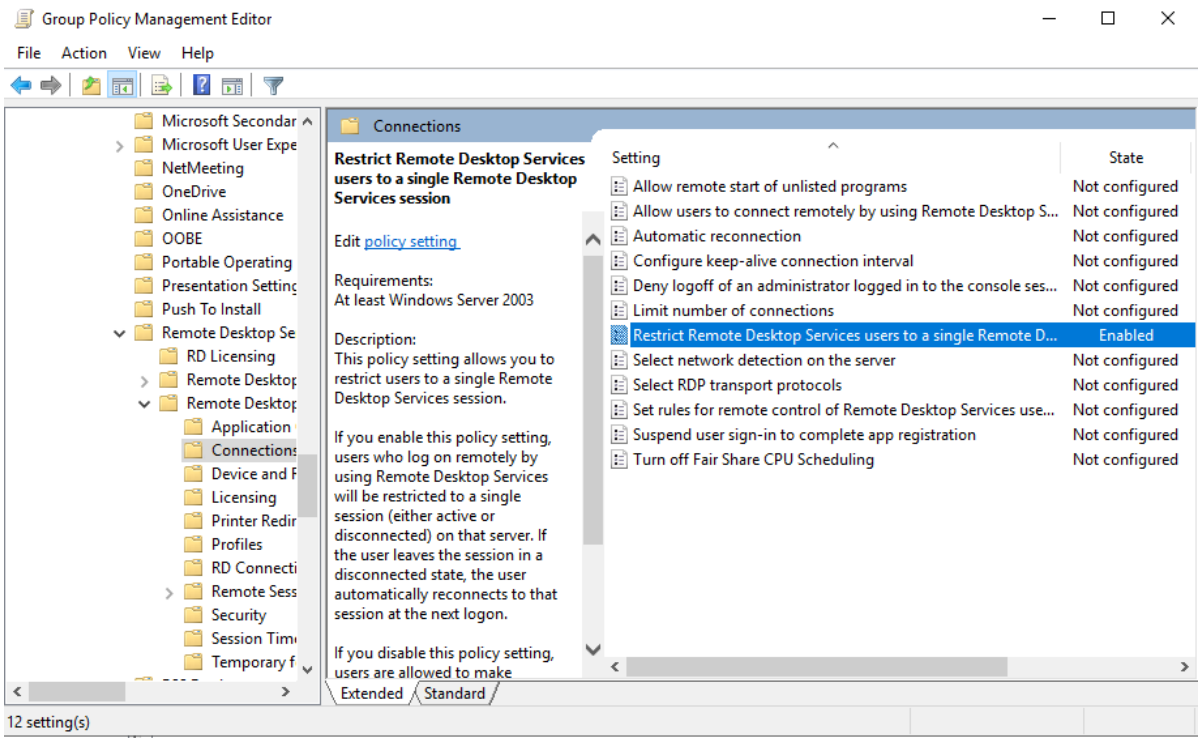


Image 284-Ensure 'Restrict Remote Desktop Services users to a single Remote Desktop Services session' is set to 'Enabled'

7.8.18.2.2 Device and Resource Redirection

7.8.18.2.2.1 Ensure 'Do not allow COM port redirection' is set to 'Enabled'

This policy setting determines whether to block data redirection to client COM ports from a remote computer during a Remote Desktop Services session. The recommended state for this setting is enabled. In a security-focused environment, minimizing potential attack vectors is crucial. Since COM port redirection is seldom necessary, disabling it helps reduce opportunities for data exfiltration and the transfer of malicious code.

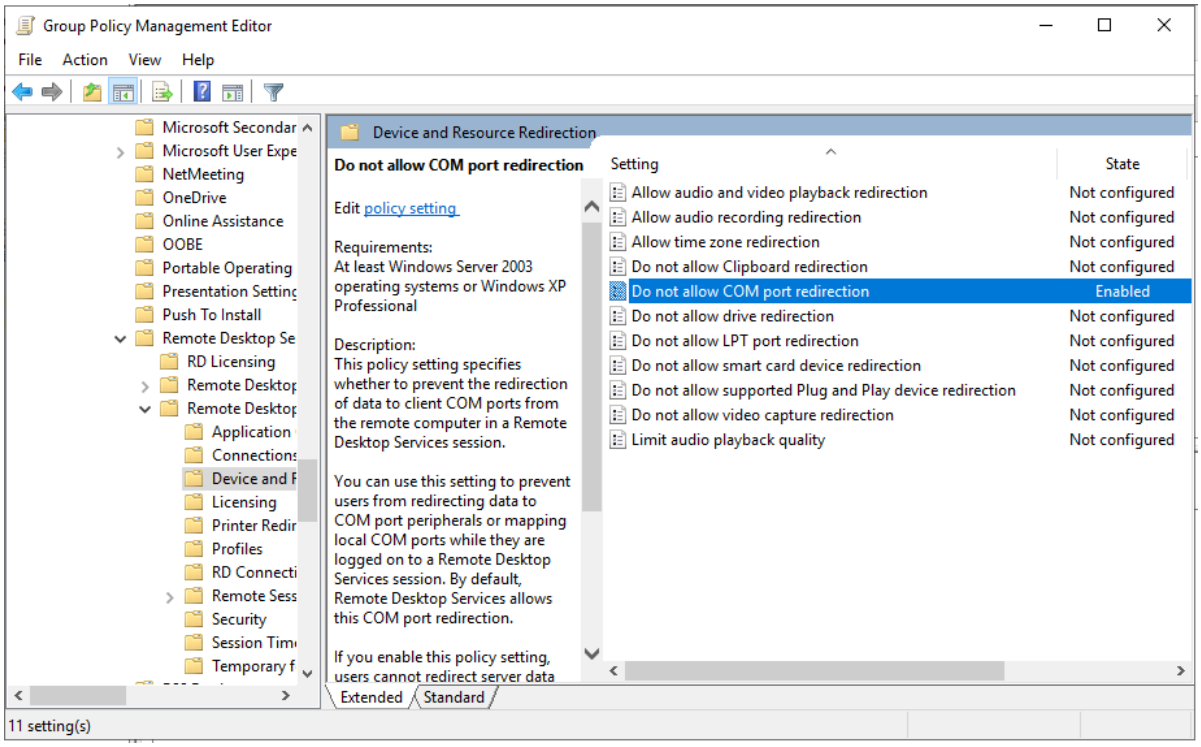


Image 285-Ensure 'Do not allow COM port redirection' is set to 'Enabled'

7.8.18.2.2.2 Ensure 'Do not allow drive redirection' is set to 'Enabled'

This policy setting blocks users from sharing their local drives with Remote Desktop Servers they connect to. Shared drives would appear in the session folder tree in Windows Explorer as \TSClient<driveletter>$, but keeping these drives shared exposes them to potential threats. The recommended state for this setting is enabled. By preventing local drive sharing, the risk of data being transferred from the Remote Desktop session to the local computer without direct user action is reduced. This helps protect against malicious software on a compromised server accessing the user's local drives stealthily during the session.

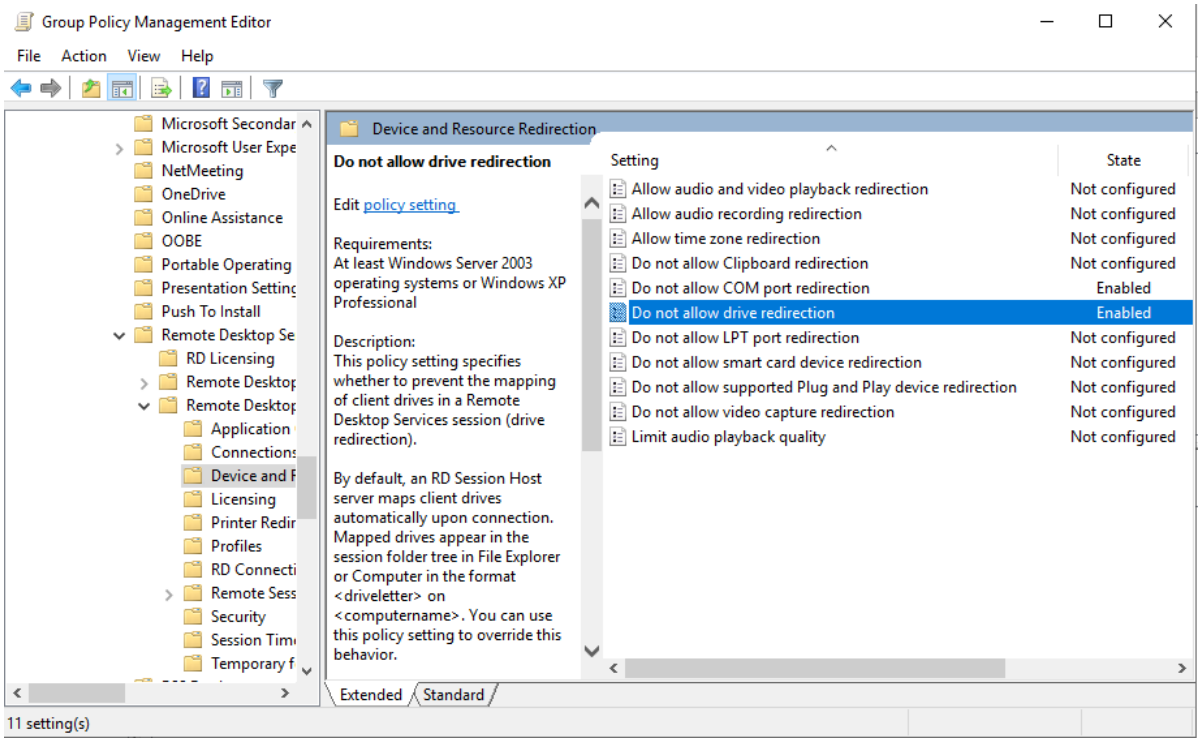


Image 286-Ensure 'Do not allow drive redirection' is set to 'Enabled'

7.8.18.2.2.3 Ensure 'Do not allow LPT port redirection' is set to 'Enabled'

This policy setting determines whether to block the redirection of data to client LPT ports during a Remote Desktop Services session. The recommended state for this setting is enabled. This approach helps minimize the potential attack surface in high-security environments, as LPT port redirection is rarely needed. Disabling it reduces the risk of unexpected data exfiltration or malicious code transfer.

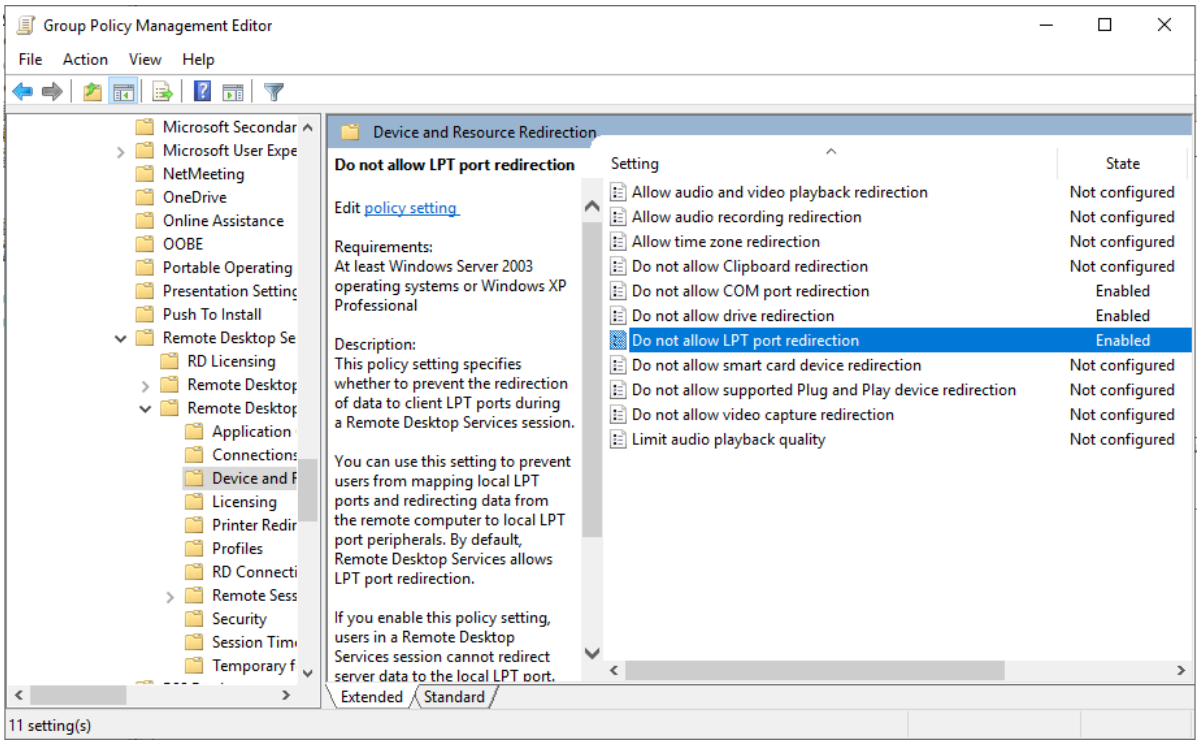


Image 287-Ensure 'Do not allow LPT port redirection' is set to 'Enabled'

7.8.18.2.2.4 Ensure 'Do not allow supported Plug and Play device redirection' is set to 'Enabled'

This policy setting manages the redirection of supported Plug and Play devices, like Windows Portable Devices, to the remote computer during a Remote Desktop Services session. The recommended configuration for this setting is enabled. In high-security environments, it's important to minimize the attack surface, and since Plug and Play device redirection is infrequently needed, disabling it reduces the risk of data exfiltration or malicious code transfer.

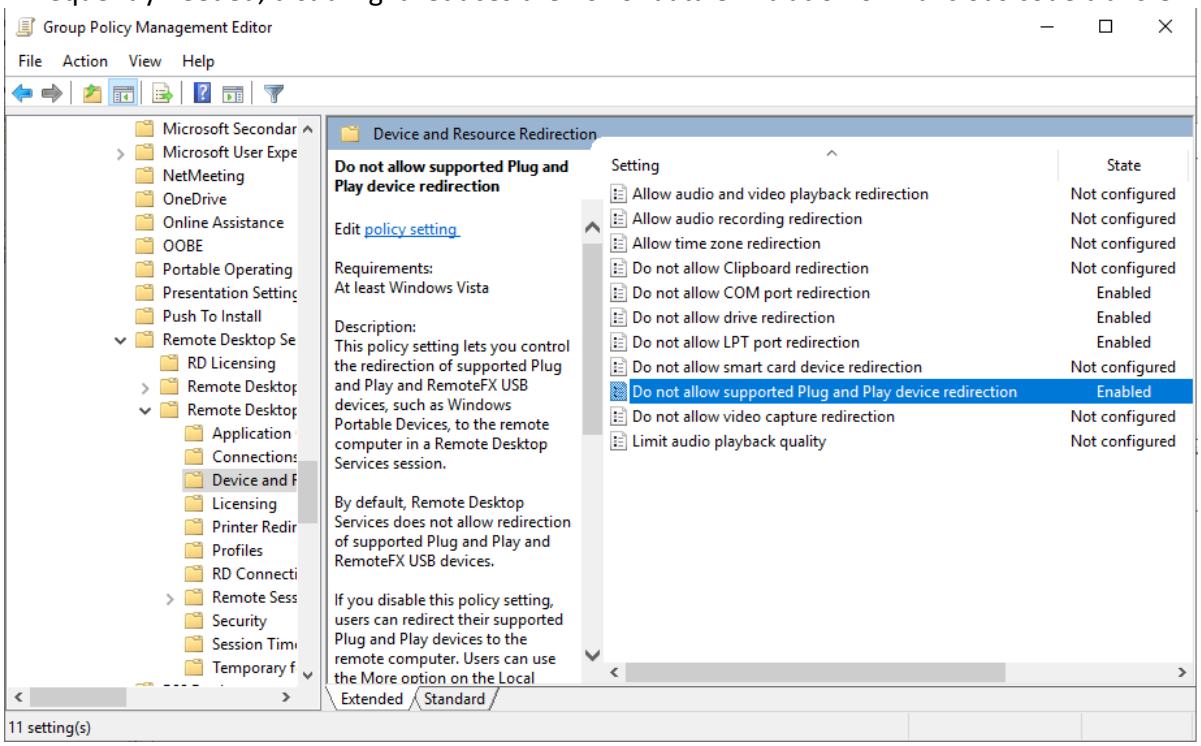


Image 288-Ensure 'Do not allow supported Plug and Play device redirection' is set to 'Enabled'

7.8.18.2.3 Security

7.8.18.2.3.1 Ensure 'Always prompt for password upon connection' is set to 'Enabled'

This policy setting controls whether Remote Desktop Services requires the client computer to prompt for a password upon connection, even if the password has already been entered in the Remote Desktop Connection client. The recommended configuration for this setting is enabled. This ensures that users must provide their password each time they connect, preventing unauthorized access by individuals who might gain physical access to the user's computer and attempt to connect to the Remote Desktop Server using saved credentials.

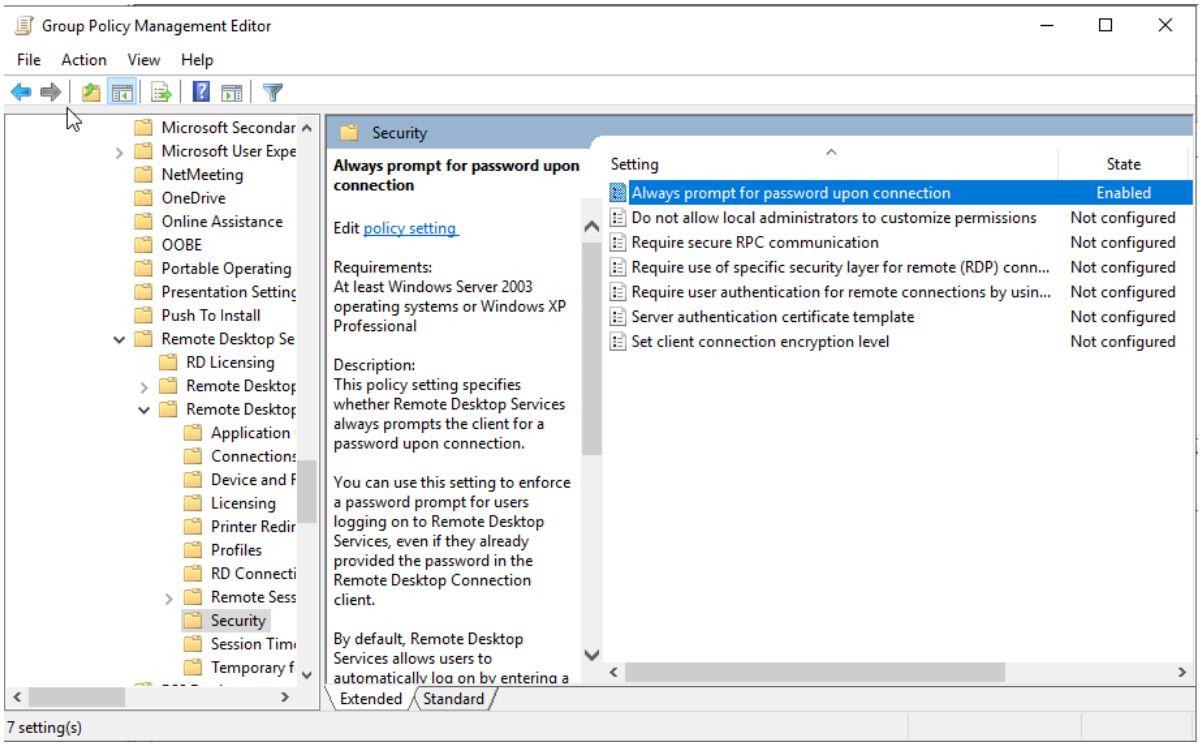


Image 289-Ensure 'Always prompt for password upon connection' is set to 'Enabled'

7.8.18.2.3.2 Ensure 'Require secure RPC communication' is set to 'Enabled'

This policy setting determines whether Remote Desktop Services mandates secure Remote Procedure Call (RPC) communication with clients or permits unsecured communication. Enabling this setting ensures that RPC communication is authenticated and encrypted, enhancing security by preventing potential man-in-the-middle attacks and protecting against data disclosure. The recommended configuration for this setting is enabled.

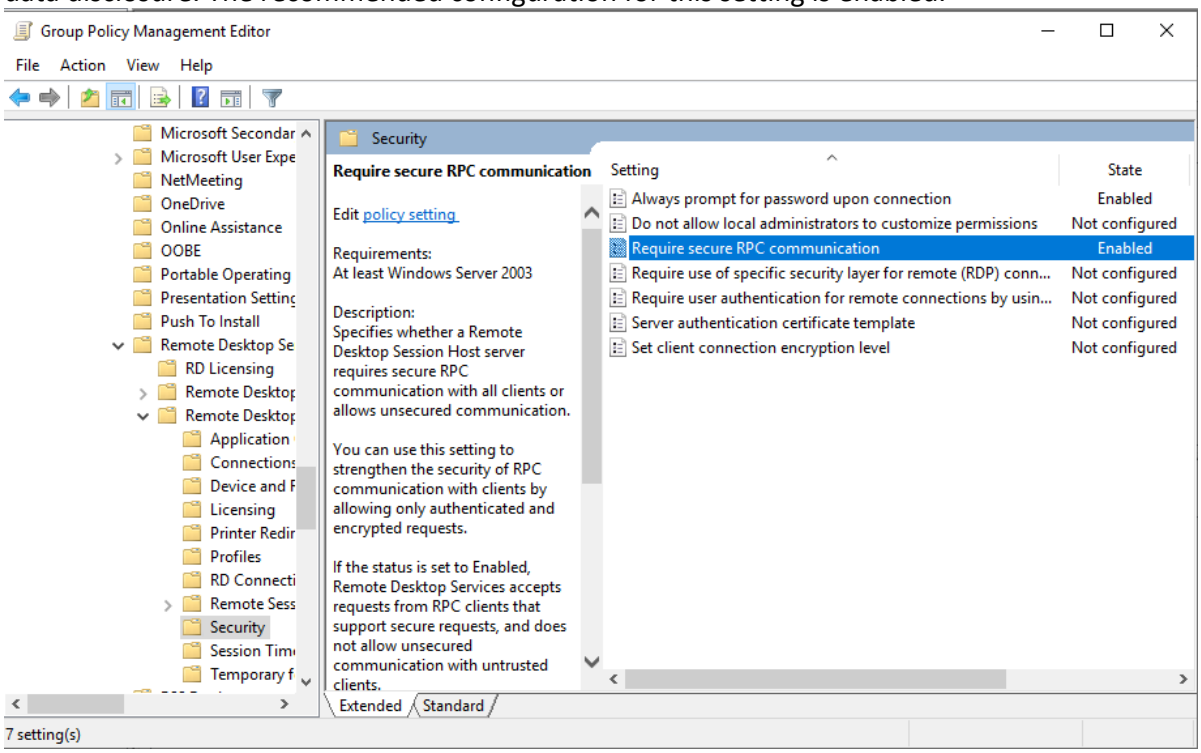


Image 290-Ensure 'Require secure RPC communication' is set to 'Enabled'

7.8.18.2.3.3 Ensure 'Require use of specific security layer for remote (RDP) connections' is set to 'Enabled: SSL'

This policy setting determines whether a specific security layer must be used to protect communications between clients and RD Session Host servers during Remote Desktop Protocol (RDP) connections. The recommended configuration for this setting is Enabled: SSL, which actually enforces Transport Layer Security (TLS) version 1.0 rather than the older and less secure SSL protocol. The rationale for this setting is that the native RDP encryption is considered weak, so enforcing the use of stronger TLS encryption enhances security for RDP communications.

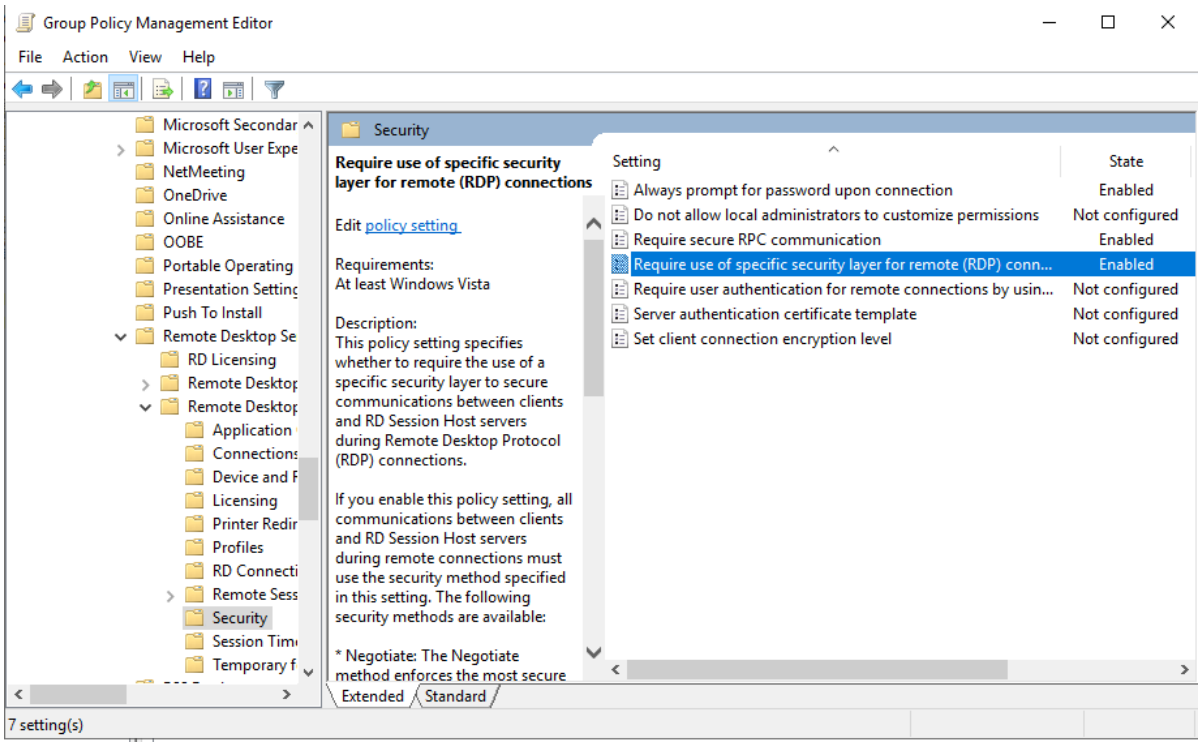


Image 291-Ensure 'Require use of specific security layer for remote (RDP) connections' is set to 'Enabled: SSL'

7.8.18.2.3.4 Ensure 'Require user authentication for remote connections by using Network Level Authentication' is set to 'Enabled'

This policy setting determines whether Network Level Authentication (NLA) is required for user authentication before establishing remote connections to the RD Session Host server. The recommended configuration is Enabled. Requiring authentication early in the remote connection process strengthens security by ensuring users are verified before the connection is fully established.

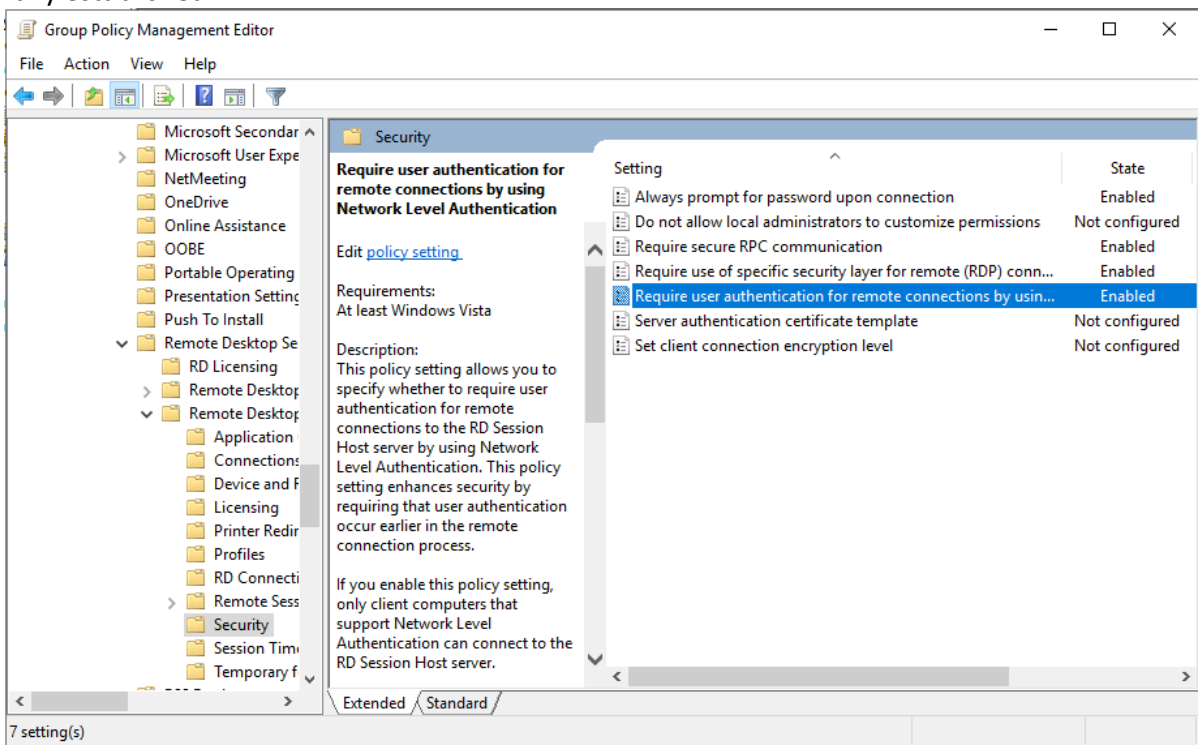


Image 292-Ensure 'Require user authentication for remote connections by using Network Level Authentication' is set to 'Enabled'

7.8.18.2.3.5 Ensure 'Set client connection encryption level' is set to 'Enabled: High Level'

This policy setting determines whether a specific level of encryption must be used to secure communications between client computers and RD Session Host servers during Remote Desktop Protocol (RDP) connections. It applies only to native RDP encryption, which is generally less secure compared to SSL encryption. The recommended configuration is Enabled: High Level. Allowing connections with low-level encryption increases the risk of decryption and potential exposure of network traffic to attackers.

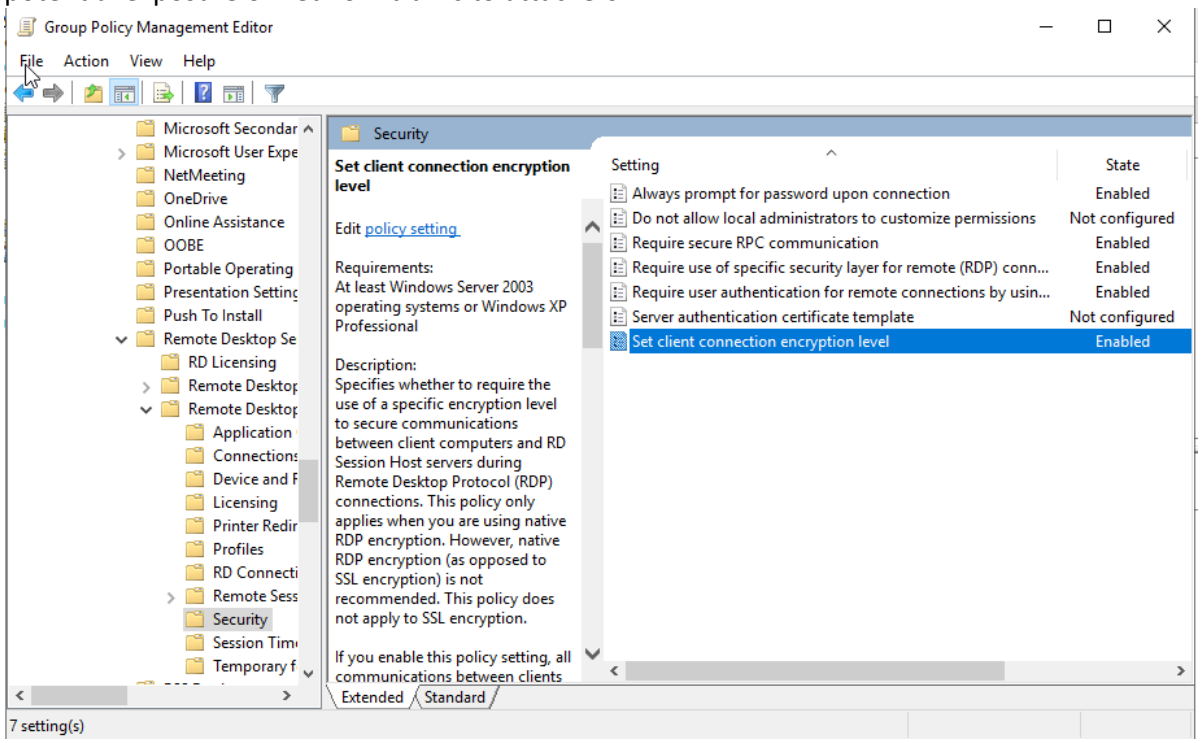


Image 293-Ensure 'Set client connection encryption level' is set to 'Enabled: High Level'

7.8.18.2.4 Session Time Limits

7.8.18.2.4.1 Ensure 'Set client connection encryption level' is set to 'Enabled: High Level'

This policy setting defines the maximum idle time allowed for an active Remote Desktop Services session before it is automatically disconnected. The recommended configuration is Enabled: 15 minutes or less, and not set to Never (0). This setting helps prevent computing resources from being consumed by inactive sessions and reduces the risk of issues such as password lockouts if a user's password changes while an old session remains active. For systems with a limited number of concurrent connections, like servers with a default limit of two administrative sessions, lingering sessions can block new connections, leading to potential denial of service. Additionally, improperly configured or extended session timeouts can increase the risk of session hijacking by attackers.

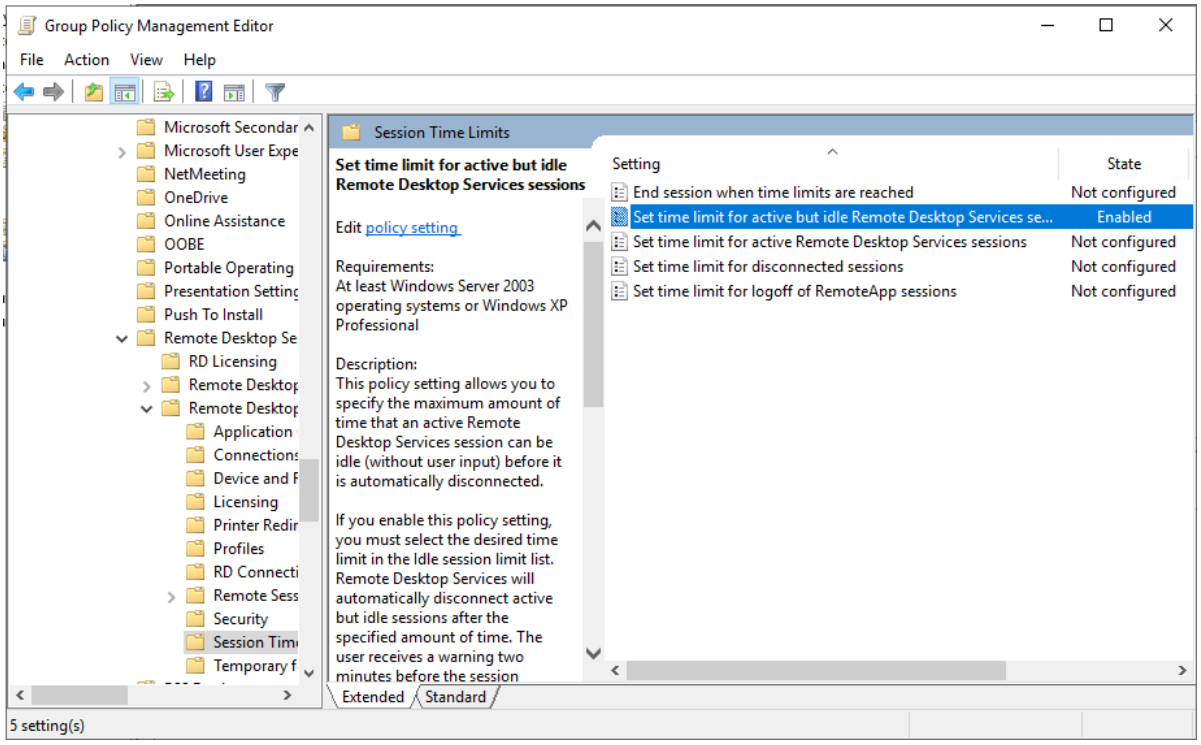


Image 294-Ensure 'Set client connection encryption level' is set to 'Enabled: High Level'

7.8.18.2.4.2 Ensure 'Set time limit for disconnected sessions' is set to 'Enabled: 1 minute'

This policy setting configures a time limit for disconnected Remote Desktop Services sessions, with the recommended state set to Enabled: 1 minute. This configuration helps to ensure that disconnected sessions do not remain active for extended periods, thereby conserving computing resources and preventing issues such as password lockouts if a user's password has changed while an old session remains active. For systems with limited concurrent connections, such as servers with a default limit of two administrative sessions, lingering sessions can block new users from connecting, leading to potential service denial. Properly terminating disconnected sessions with this setting is crucial to prevent resource wastage and reduce the risk of session hijacking by attackers.

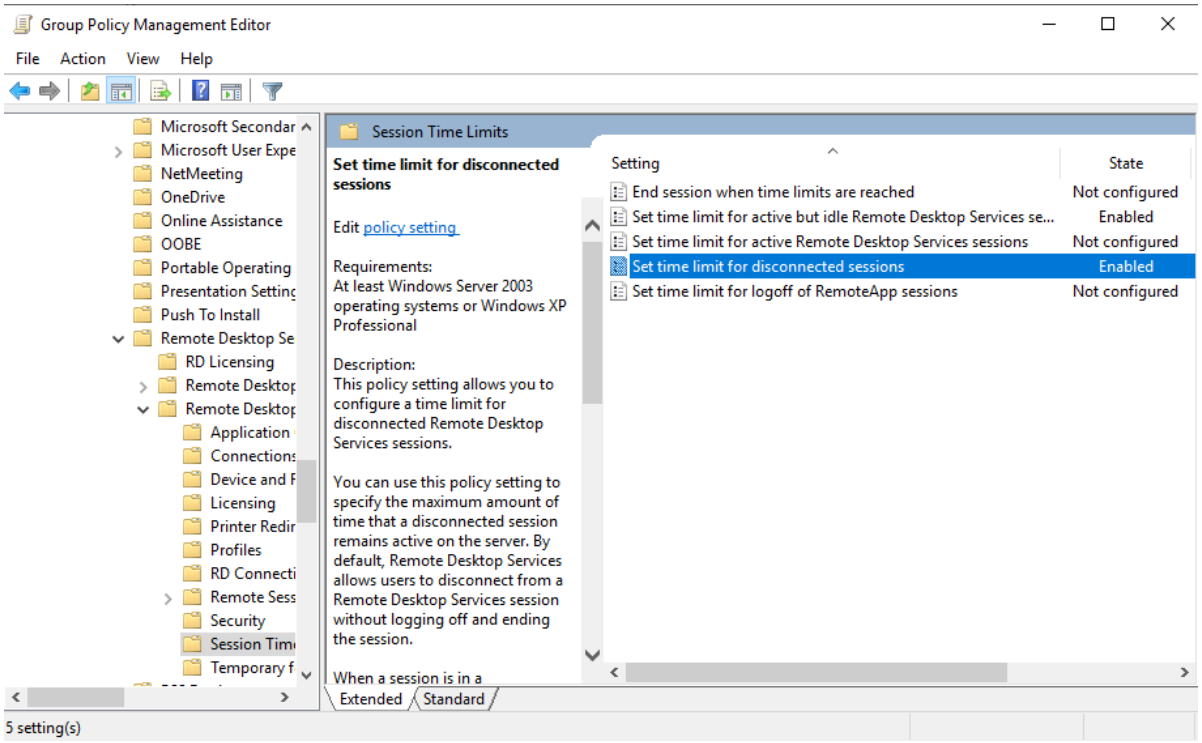


Image 295-Ensure 'Set time limit for disconnected sessions' is set to 'Enabled: 1 minute'

7.8.18.2.5 Temporary folders

7.8.18.2.5.1 Ensure 'Do not delete temp folders upon exit' is set to 'Disabled'

This policy setting determines if Remote Desktop Services retains a user's per-session temporary folders after logoff. The recommended state for this setting is: Disabled. Retaining these folders could expose sensitive information to other administrators who log into the system.

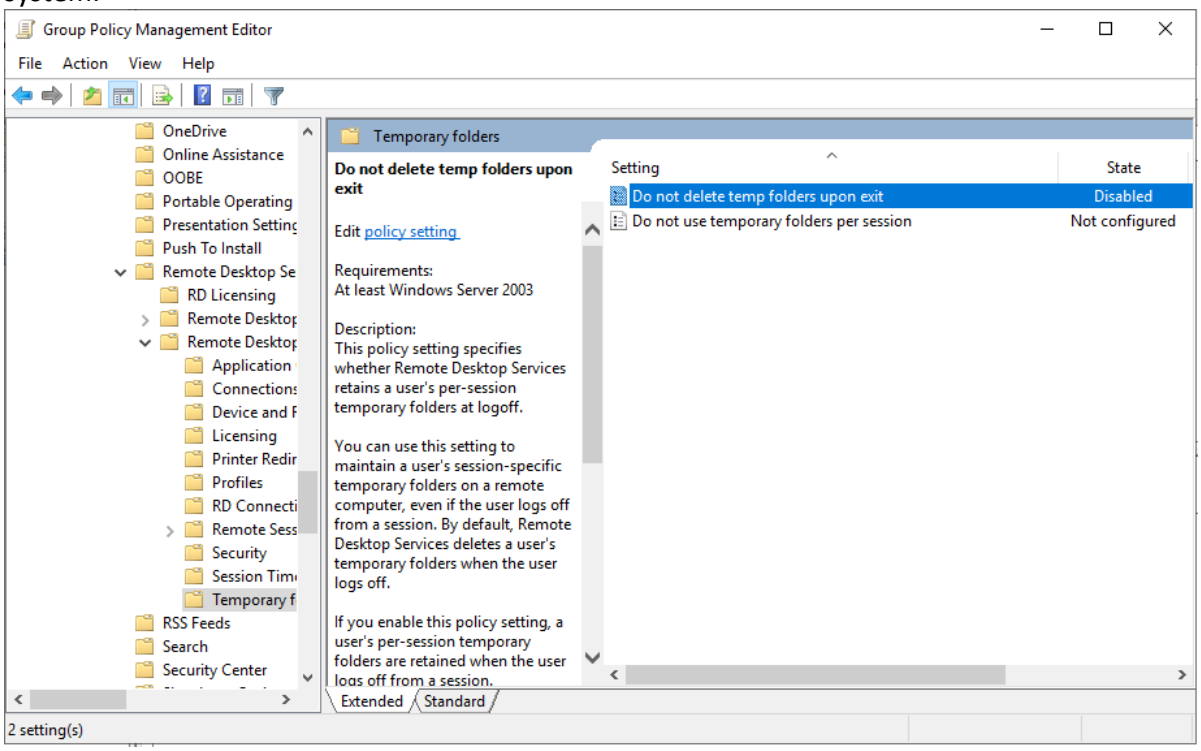


Image 296-Ensure 'Do not delete temp folders upon exit' is set to 'Disabled'

7.8.18.2.5.2 Ensure 'Do not use temporary folders per session' is set to 'Disabled'

By default, Remote Desktop Services generates a unique temporary folder on the RD Session Host server for each active user session. This folder, located in a Temp directory under the user's profile and named with the session ID, stores temporary files specific to that session. To free up disk space, this temporary folder is deleted when the user logs off. The recommended state for this setting is: Disabled. Disabling this setting ensures that cached data remains isolated between sessions, reducing issues related to shared cached data and maintaining the separation of potentially sensitive information across different user sessions.

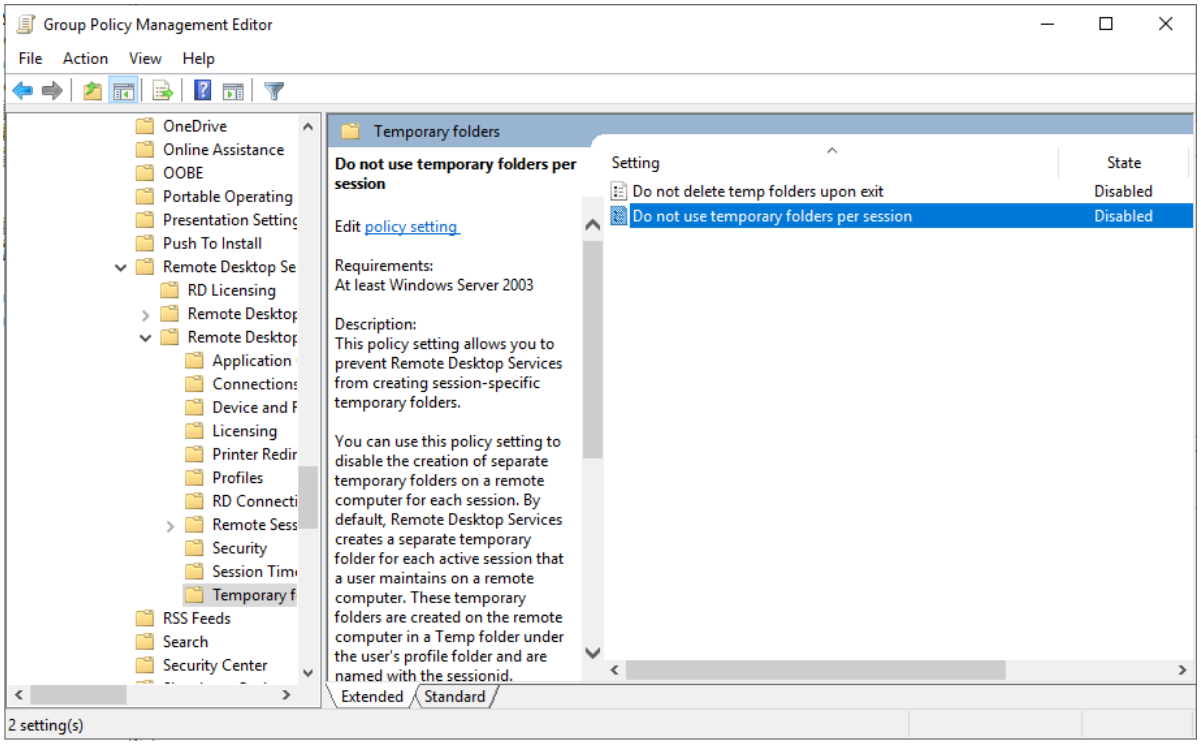


Image 297-Ensure 'Do not use temporary folders per session' is set to 'Disabled'

7.8.19 RSS Feeds

7.8.19.1 Ensure 'Prevent downloading of enclosures' is set to 'Enabled'

This policy setting restricts the downloading of file attachments from RSS feeds to the user's computer. The recommended state for this setting is: Enabled. Disabling the download of attachments via RSS feeds helps prevent potentially malicious files from being introduced to the system.

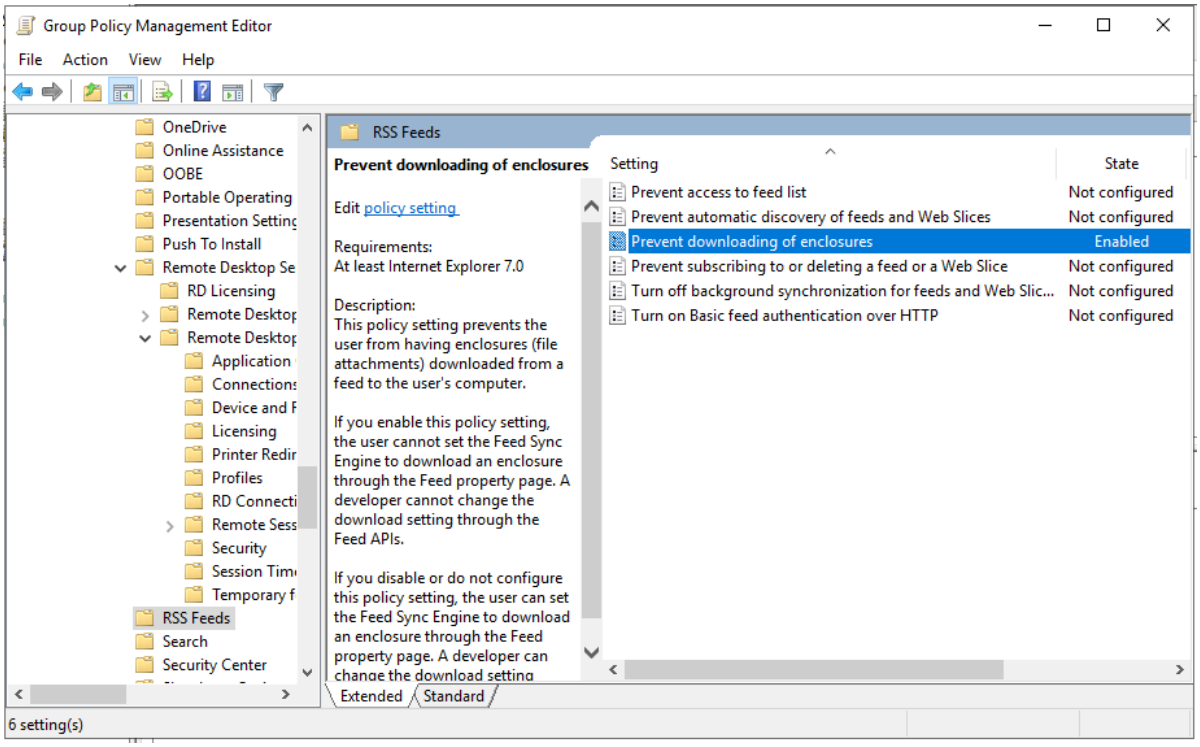


Image 298-Ensure 'Prevent downloading of enclosures' is set to 'Enabled'

7.8.20 Search

7.8.20.1 Ensure 'Allow Cloud Search' is set to 'Enabled: Disable Cloud Search'

This policy setting controls whether search and Cortana can access cloud sources such as OneDrive and SharePoint. The recommended state for this setting is: Enabled: Disable Cloud Search. This approach is recommended to address privacy concerns, as sending data to third-party cloud services can potentially expose sensitive information.

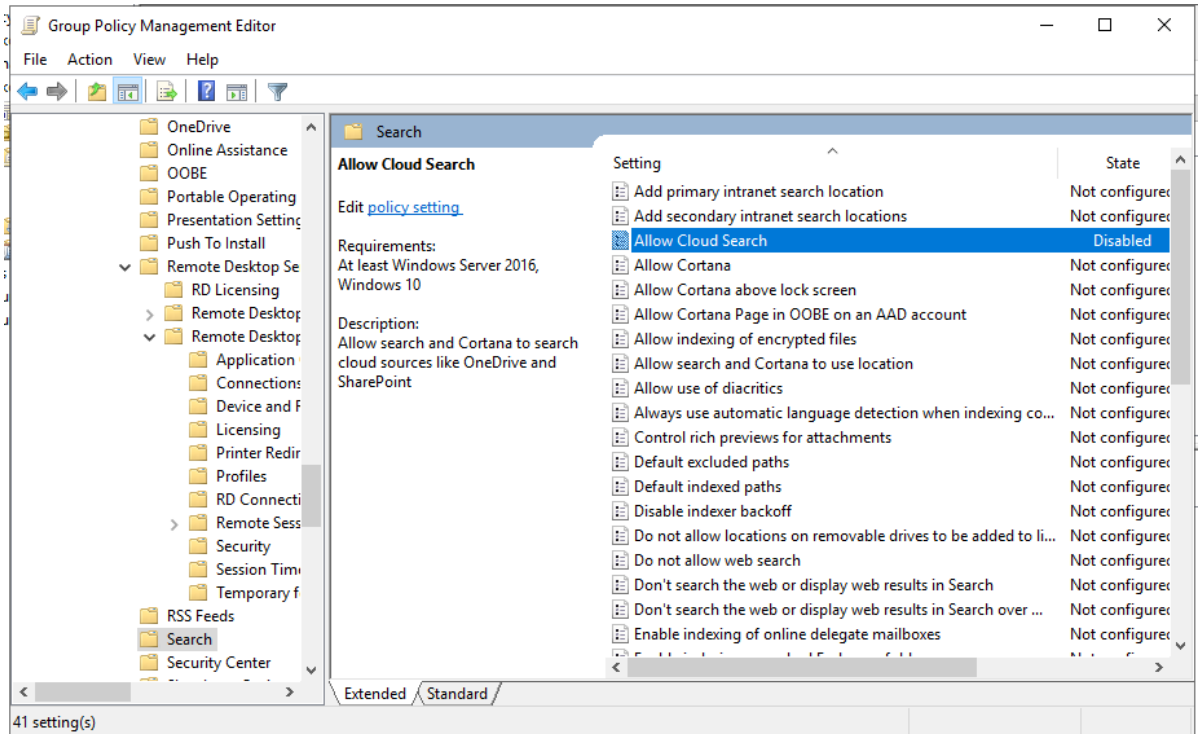


Image 299-Ensure 'Allow Cloud Search' is set to 'Enabled: Disable Cloud Search'

7.8.20.2 Ensure 'Allow indexing of encrypted files' is set to 'Disabled'

This policy setting determines whether encrypted items can be indexed. Changing this setting triggers a complete rebuild of the index. To ensure the security of encrypted files, full volume encryption, such as BitLocker or another solution, must be employed for the index location. The recommended state for this setting is: Disabled. Allowing the indexing and searching of encrypted files could potentially expose confidential information contained within them.

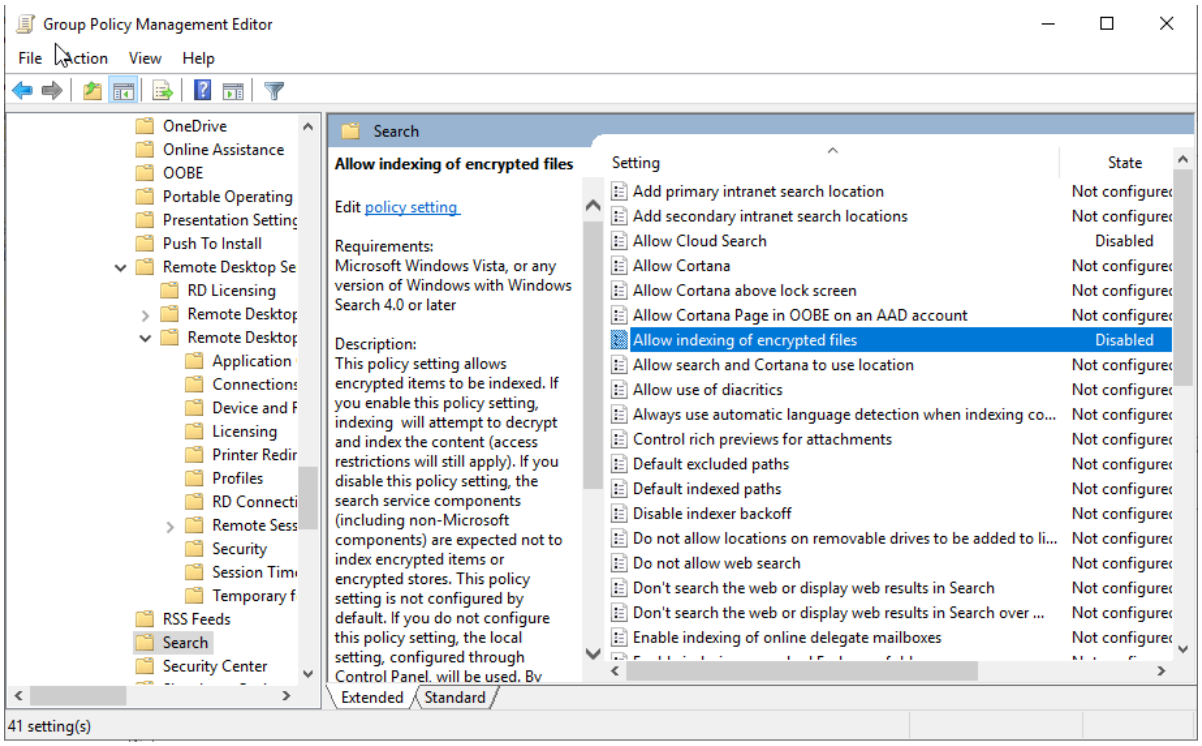


Image 300-Ensure 'Allow indexing of encrypted files' is set to 'Disabled'

7.8.21 Software Protection Platform

7.8.21.1 Ensure 'Turn off KMS Client Online AVS Validation' is set to 'Enabled'

The Key Management Service (KMS) allows local server-based activation of Microsoft licenses without direct client connections to Microsoft. This policy setting enables opting out of automatically sending KMS client activation data to Microsoft. The recommended state for this setting is: Enabled. Preventing the automatic transmission of KMS client activation data to Microsoft helps address privacy concerns, particularly in high-security environments.

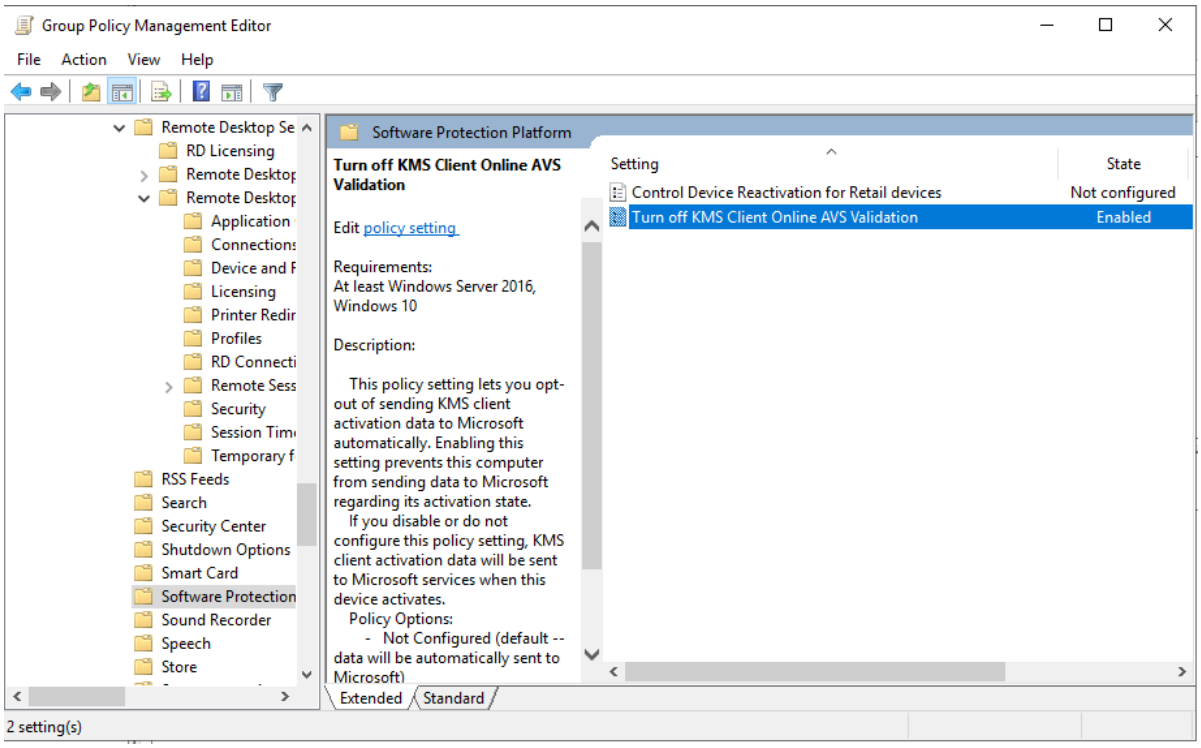


Image 301-Ensure 'Turn off KMS Client Online AVS Validation' is set to 'Enabled'

7.8.22 Windows Defender SmartScreen

7.8.22.1 Explorer

7.8.22.1.1 Ensure 'Configure Windows Defender SmartScreen' is set to 'Enabled: Warn and prevent bypass'

This policy setting controls the behavior of Windows SmartScreen, which helps protect PCs by warning users before running unrecognized programs downloaded from the Internet. Some data is sent to Microsoft about the files and programs run when this feature is enabled. The recommended state for this setting is: Enabled: Warn and prevent bypass. While Windows SmartScreen enhances security by warning users about potentially unsafe programs, some organizations may opt to disable it due to concerns about information being sent to Microsoft.

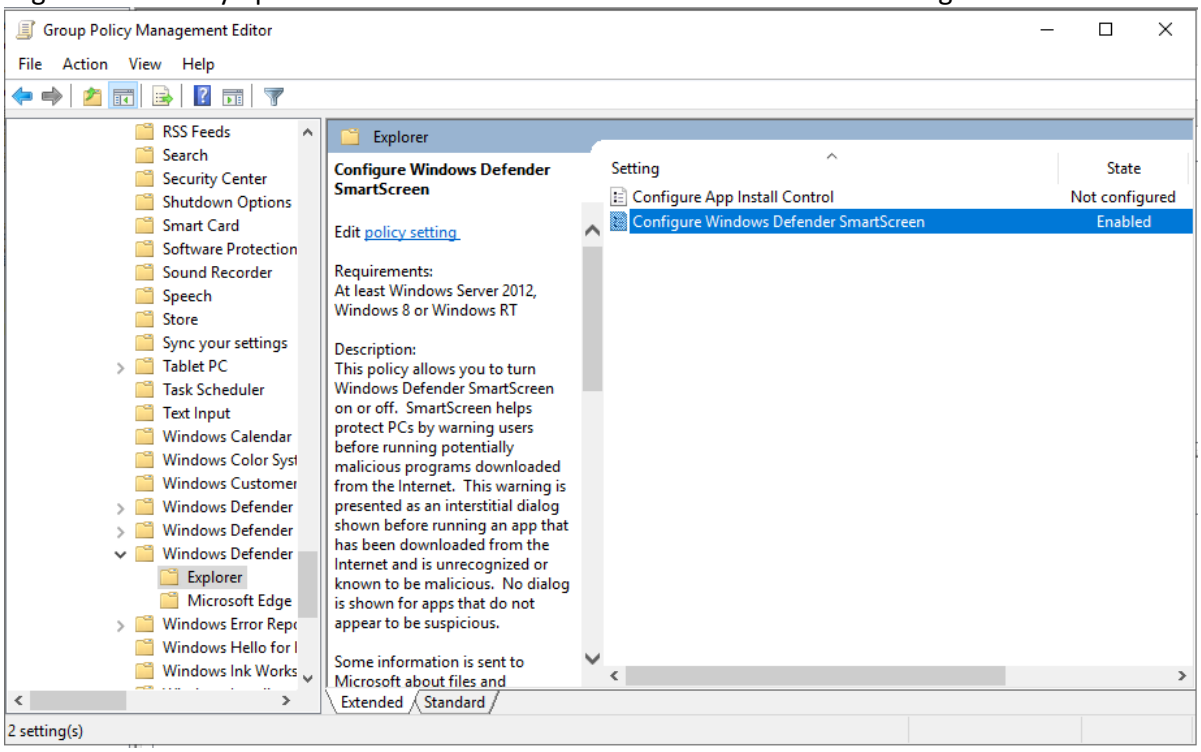


Image 302-Ensure 'Configure Windows Defender SmartScreen' is set to 'Enabled: Warn and prevent bypass'

7.8.23 Windows Ink Workspace

7.8.23.1 Ensure 'Allow suggested apps in Windows Ink Workspace' is set to 'Disabled'

This policy setting controls whether suggested apps in Windows Ink Workspace are allowed. The recommended state for this setting is: Disabled. Disabling this feature prevents data collection and sharing with third parties, enhancing privacy.

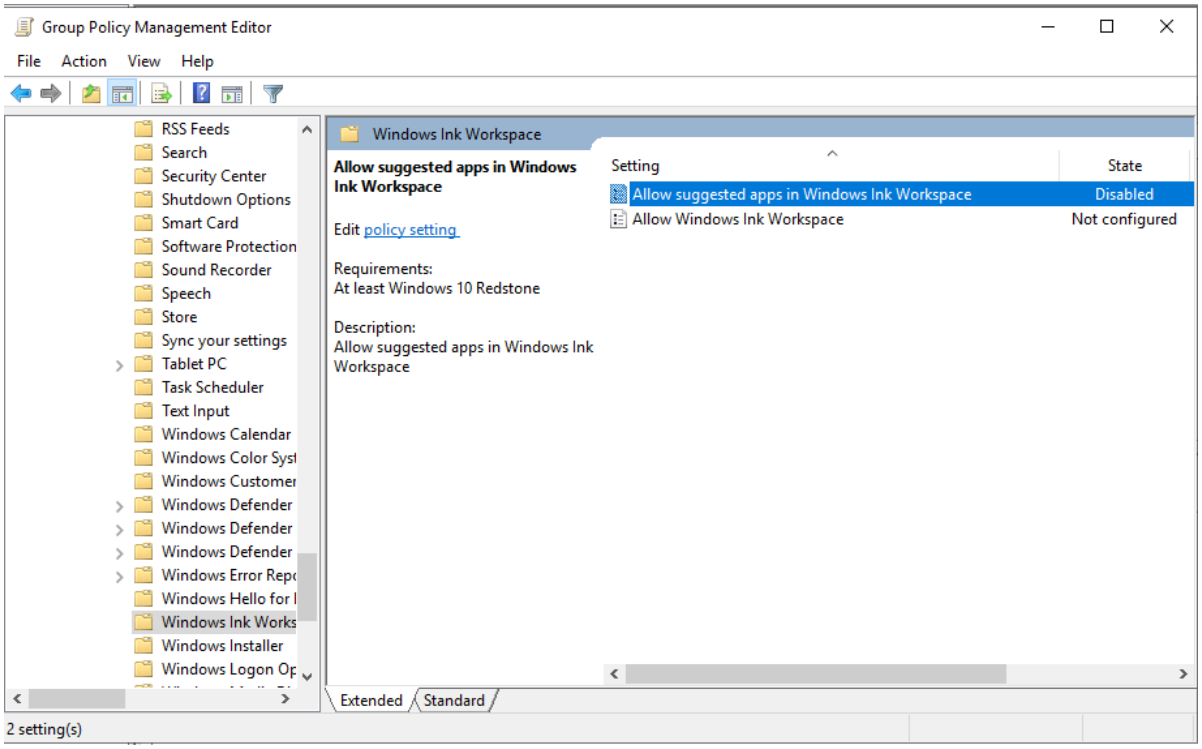


Image 303-Ensure 'Allow suggested apps in Windows Ink Workspace' is set to 'Disabled'

7.8.23.2 Ensure 'Allow Windows Ink Workspace' is set to 'Enabled: On, but disallow access above lock' OR 'Enabled: Disabled'

This policy setting controls whether Windows Ink items are accessible above the lock screen. The recommended state is: Enabled, but disallow access above lock or Disabled. Allowing access to apps while the system is locked is not recommended; such features should only be accessible after proper user authentication.

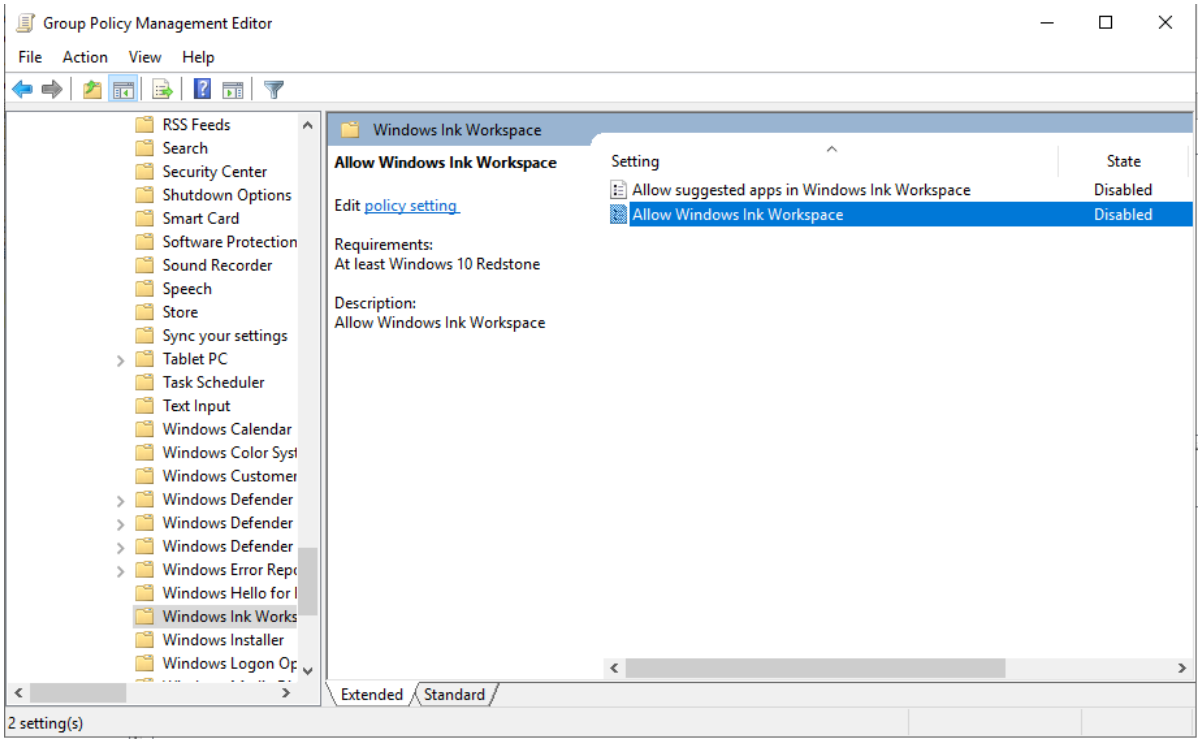


Image 304-Ensure 'Allow Windows Ink Workspace' is set to 'Enabled: On, but disallow access above lock' OR 'Enabled: Disabled'

7.8.24 Windows Installer

7.8.24.1 Ensure 'Allow user control over installs' is set to 'Disabled'

This setting controls whether users can change installation options typically reserved for system administrators. Windows Installer's security features prevent users from modifying protected options, and if detected, the installation is halted with a warning. These protections are active only when the installer runs with elevated privileges. The recommended state for this setting is: Disabled. In an enterprise environment, only IT staff should have administrative rights to install or modify software, as allowing users control over installations could lead to unapproved software and potential system vulnerabilities.

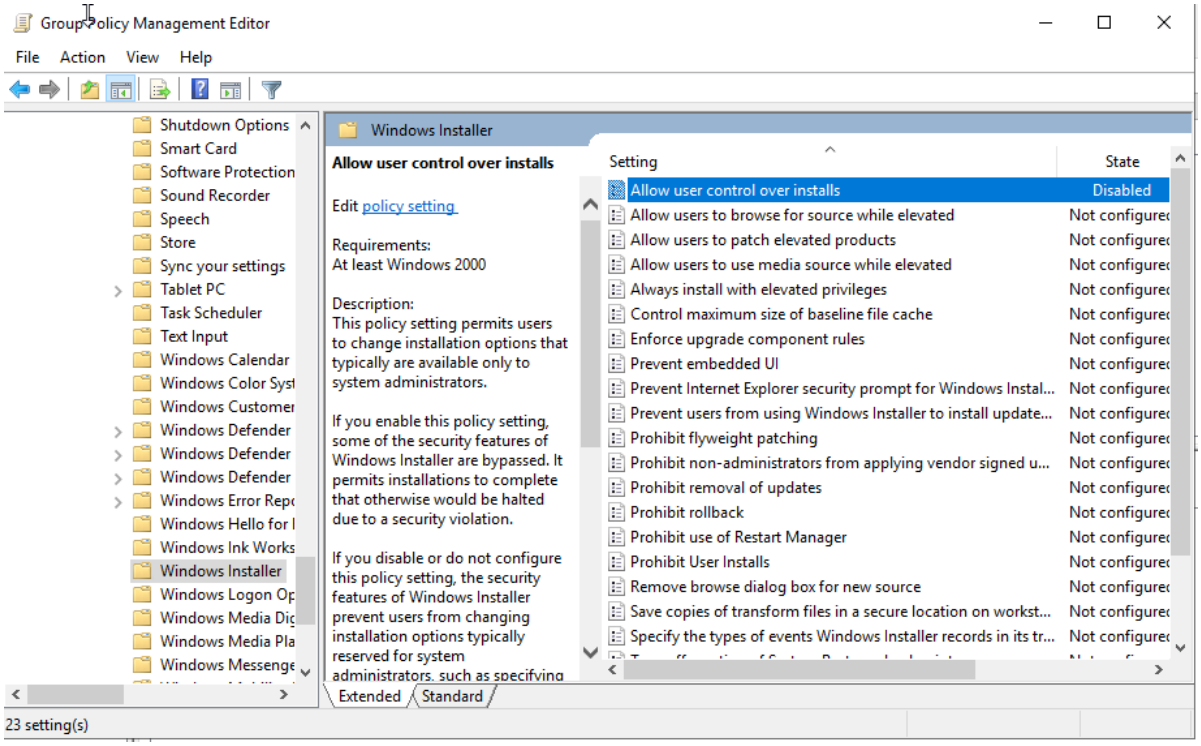


Image 305-Ensure 'Allow user control over installs' is set to 'Disabled'

7.8.24.2 Ensure 'Always install with elevated privileges' is set to 'Disabled'

This setting controls whether Windows Installer should use system permissions during program installations. It appears in both Computer Configuration and User Configuration folders and must be enabled in both to take effect. Caution: If enabled, skilled users could exploit this setting to elevate their privileges and access restricted files and folders. The User Configuration version is not fully secure. The recommended state for this setting is: Disabled. Users with limited privileges could misuse this feature to gain administrative access, install malicious software, or perform unauthorized activities.

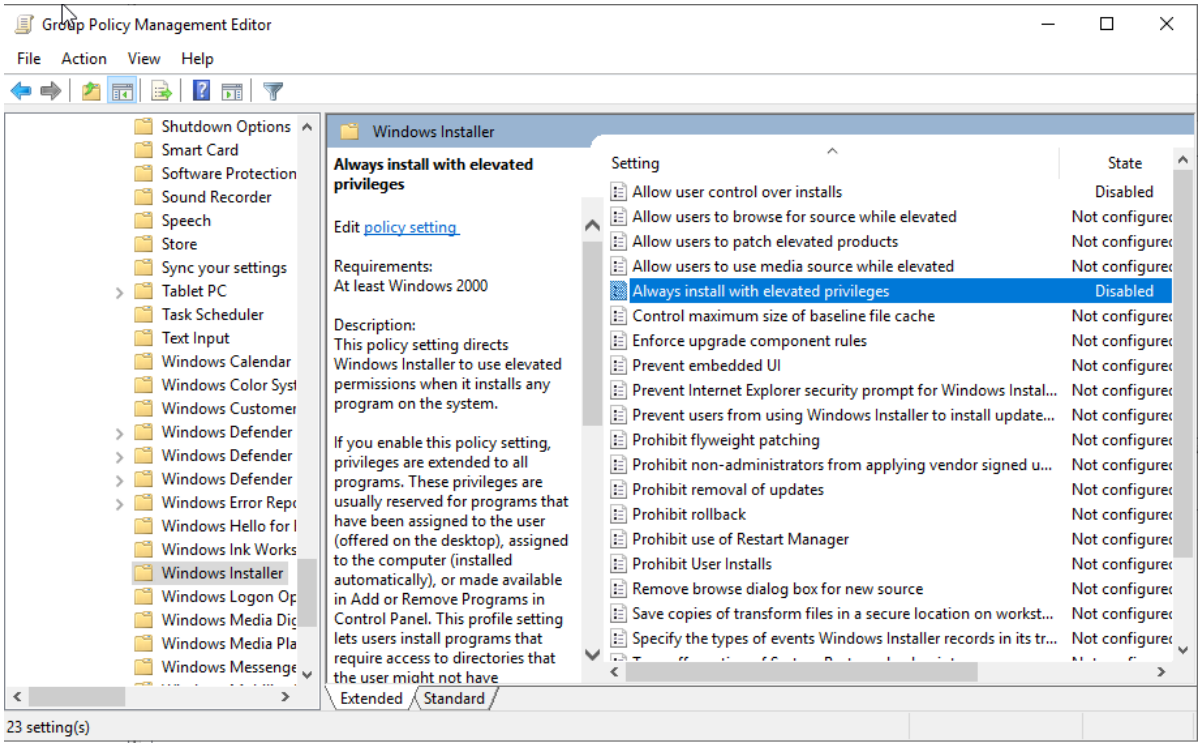


Image 306-Ensure 'Always install with elevated privileges' is set to 'Disabled'

7.8.24.3 Ensure 'Prevent Internet Explorer security prompt for Windows Installer scripts' is set to 'Disabled'

This policy setting determines if Web-based programs can install software without user notification. The recommended state for this setting is: Disabled. Disabling system warnings can increase security risks and expand the system's attack surface.

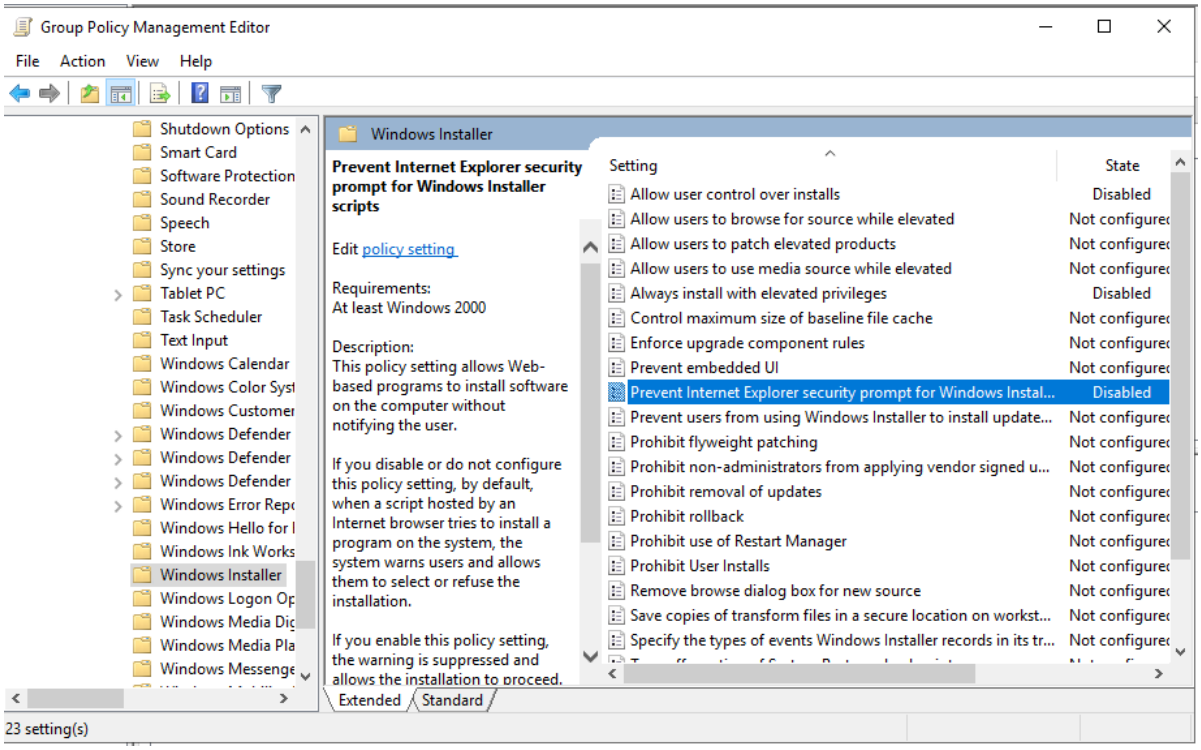


Image 307-Ensure 'Prevent Internet Explorer security prompt for Windows Installer scripts' is set to 'Disabled'

7.8.25 Windows Logon Options

7.8.25.1 Ensure 'Sign-in and lock last interactive user automatically after a restart' is set to 'Disabled'

This policy setting determines if a device automatically signs in the last user after a Windows Update restart. The recommended state for this setting is: Disabled. Disabling this feature prevents credential caching, unauthorized access, and ensures the user is aware of the restart.

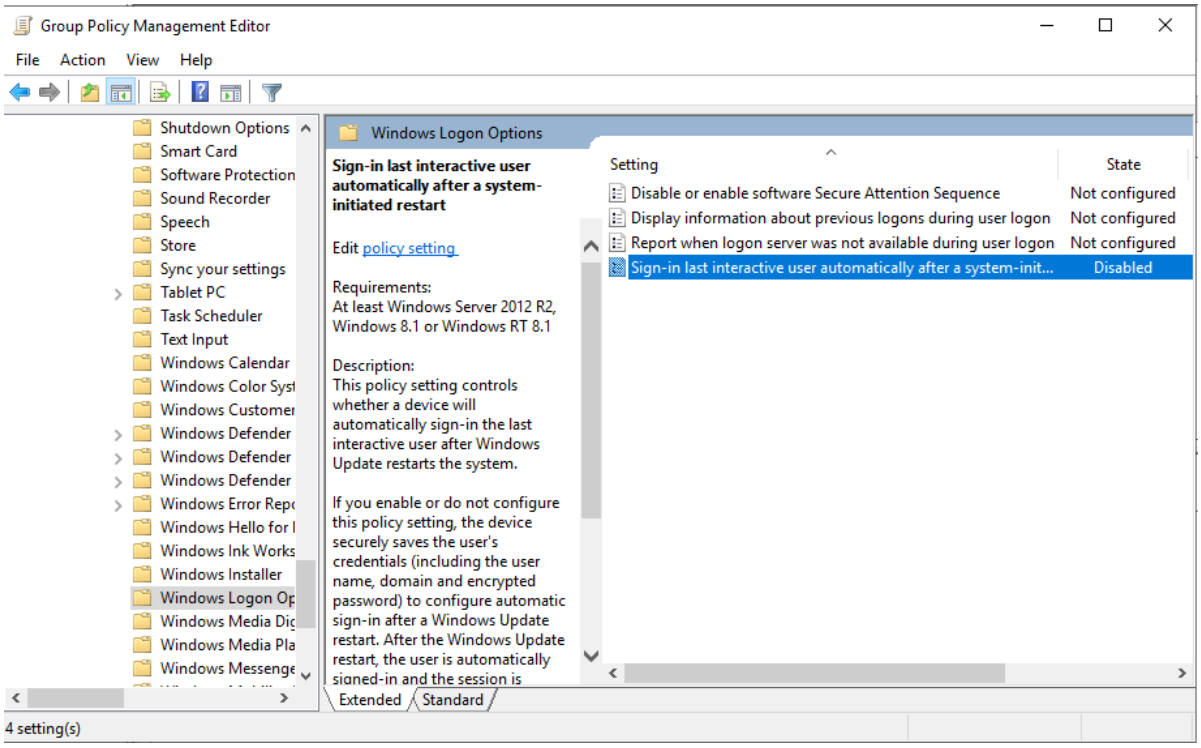


Image 308-Ensure 'Sign-in and lock last interactive user automatically after a restart' is set to 'Disabled'

7.8.26 Windows PowerShell

7.8.26.1 Ensure 'Turn on PowerShell Script Block Logging' is set to 'Enabled'

This policy setting enables logging of all PowerShell script input to the PowerShell Operational Event Log. The recommended state is: Enabled. Enabling logging of Script Block Invocation Start/Stop Events generates a high volume of logs, and while CIS does not specifically recommend this option, it is considered compliant if chosen. PowerShell script input logs are valuable for forensic investigations of PowerShell attack incidents

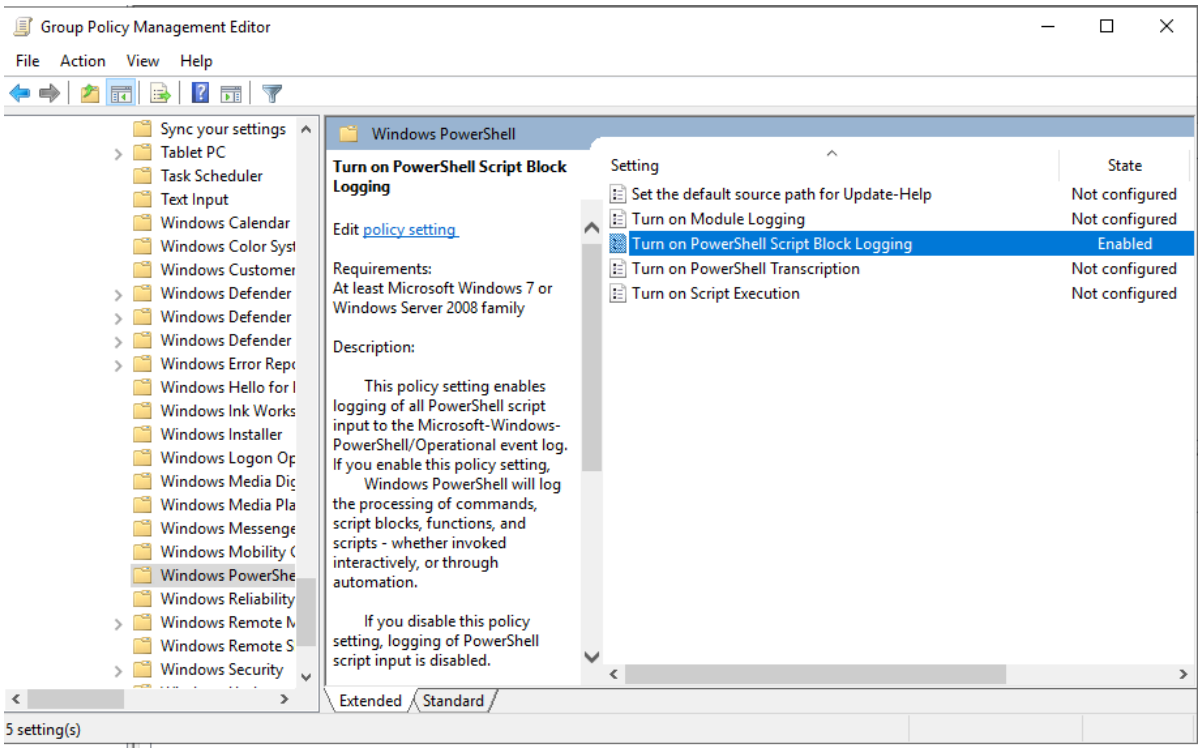


Image 309-Ensure 'Turn on PowerShell Script Block Logging' is set to 'Enabled'

7.8.26.2 Ensure 'Turn on PowerShell Transcription' is set to 'Enabled'

This policy setting enables the capture of input and output from Windows PowerShell commands into text-based transcripts. The recommended state is: Enabled. Capturing PowerShell transcripts is highly beneficial for forensic investigations into PowerShell attacks, as it helps in understanding what transpired.

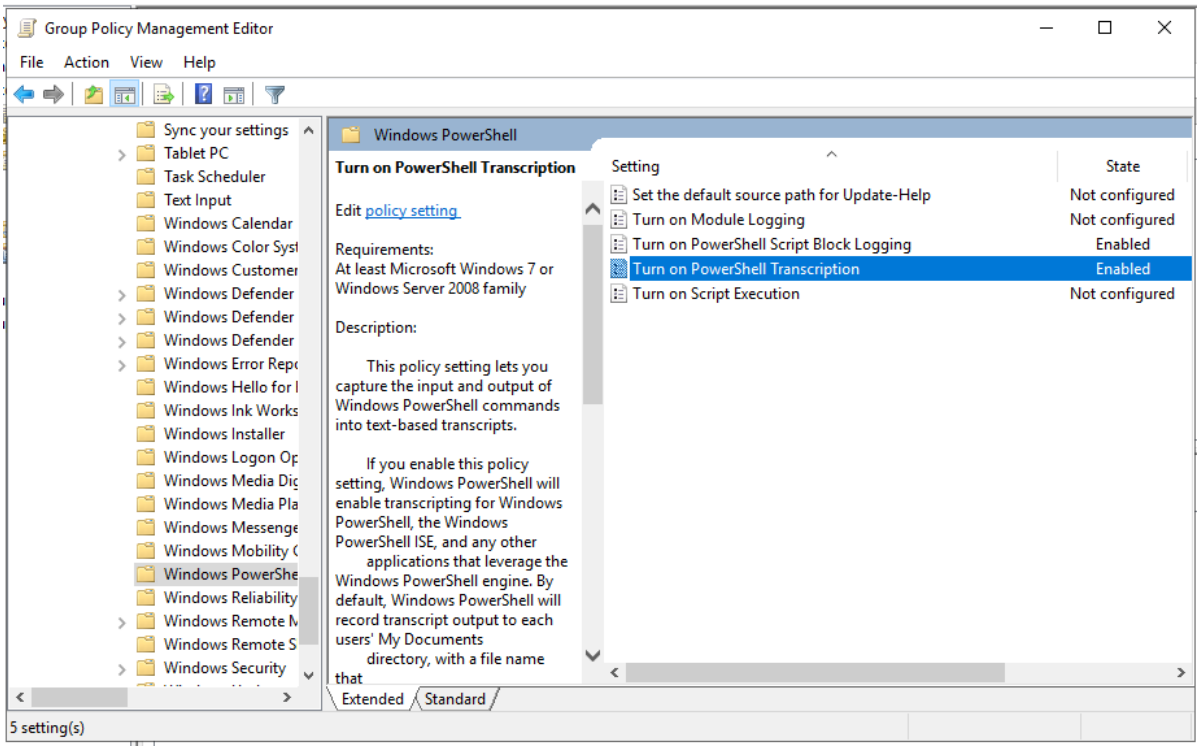


Image 310-Ensure 'Turn on PowerShell Transcription' is set to 'Enabled'

7.8.27 Windows Remote Management (WinRM)

7.8.27.1 WinRM Client

7.8.27.1.1 Ensure 'Allow Basic authentication' is set to 'Disabled'

This policy setting controls whether the Windows Remote Management (WinRM) client can use Basic authentication. The recommended state is: Disabled. Basic authentication is less secure compared to other available methods because it transmits credentials, including passwords, in plain text. An attacker who intercepts network packets where WinRM is active could potentially obtain these credentials and compromise remote host access.

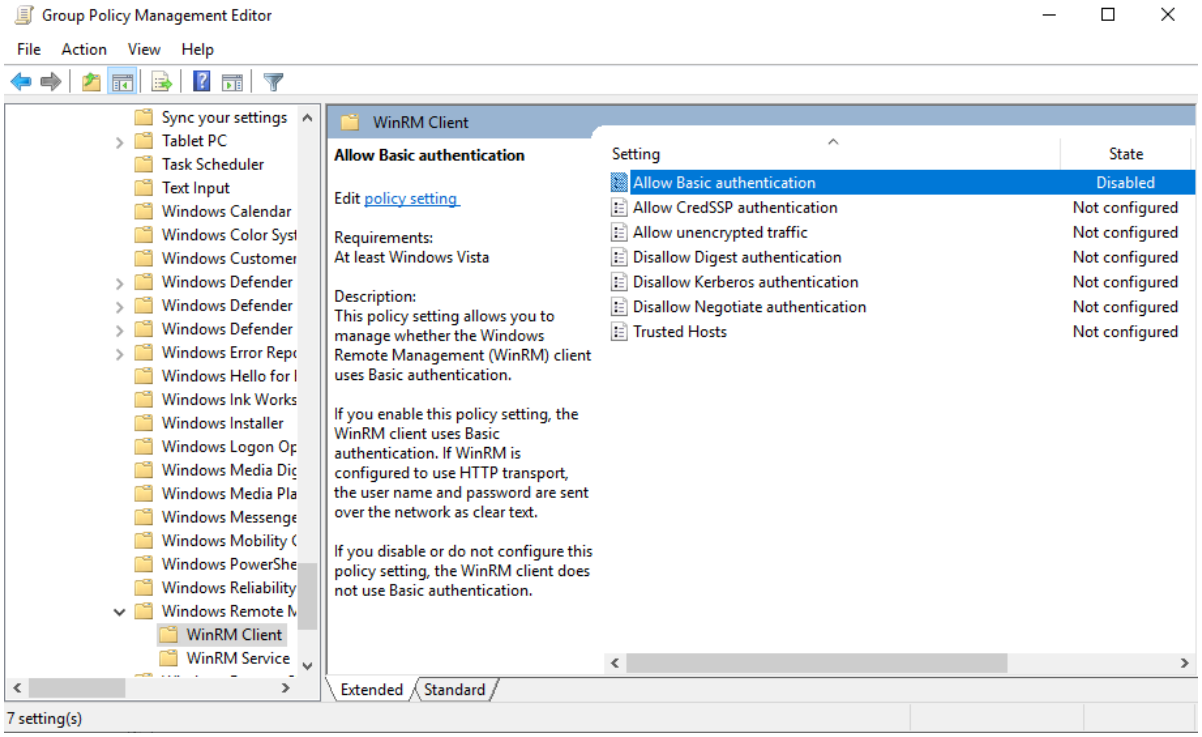


Image 311-Ensure 'Allow Basic authentication' is set to 'Disabled'

7.8.27.1.2 Ensure 'Allow unencrypted traffic' is set to 'Disabled'

This policy setting controls whether the Windows Remote Management (WinRM) client transmits and receives unencrypted messages over the network. The recommended state is: Disabled. Encrypting WinRM network traffic helps mitigate the risk of attackers intercepting or altering WinRM messages as they travel across the network.

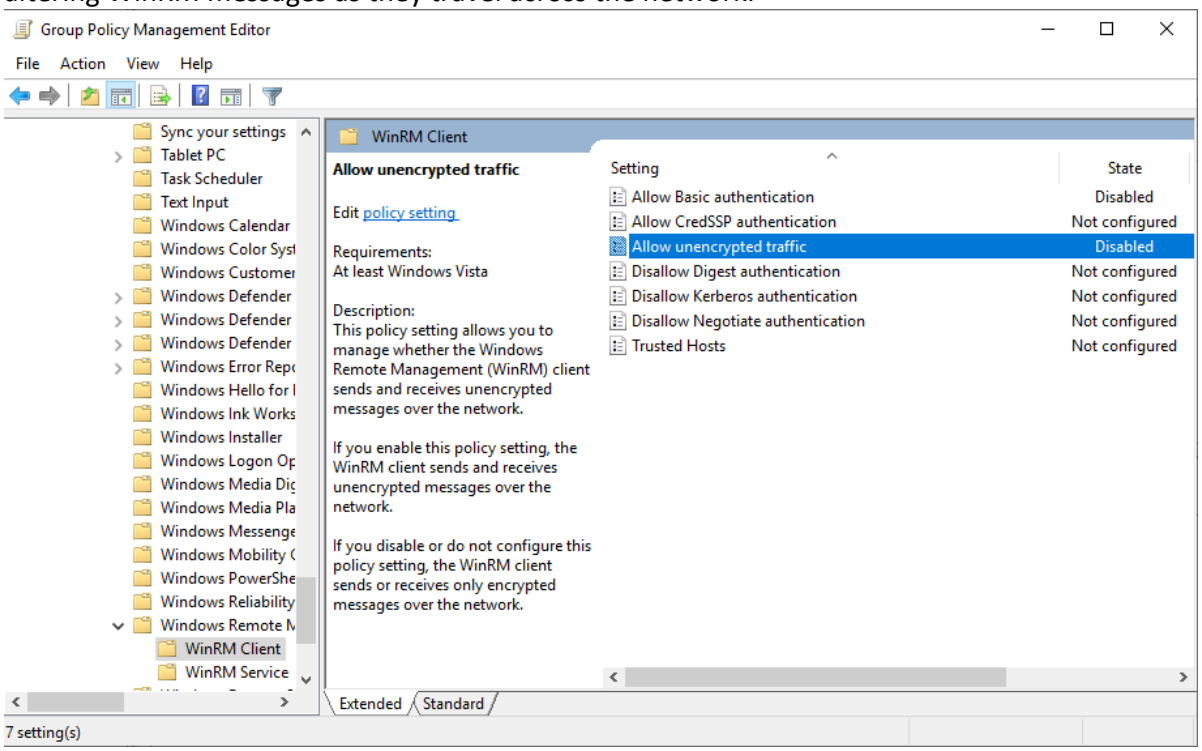


Image 312-Ensure 'Allow unencrypted traffic' is set to 'Disabled'

7.8.27.1.3 Ensure 'Disallow Digest authentication' is set to 'Enabled'

This policy setting controls whether the Windows Remote Management (WinRM) client should avoid using Digest authentication. The recommended state is: Enabled. Digest authentication is less secure compared to other available authentication methods in WinRM. If an attacker captures packets on the network where WinRM is operating, they could potentially uncover the credentials used for accessing remote hosts via WinRM.

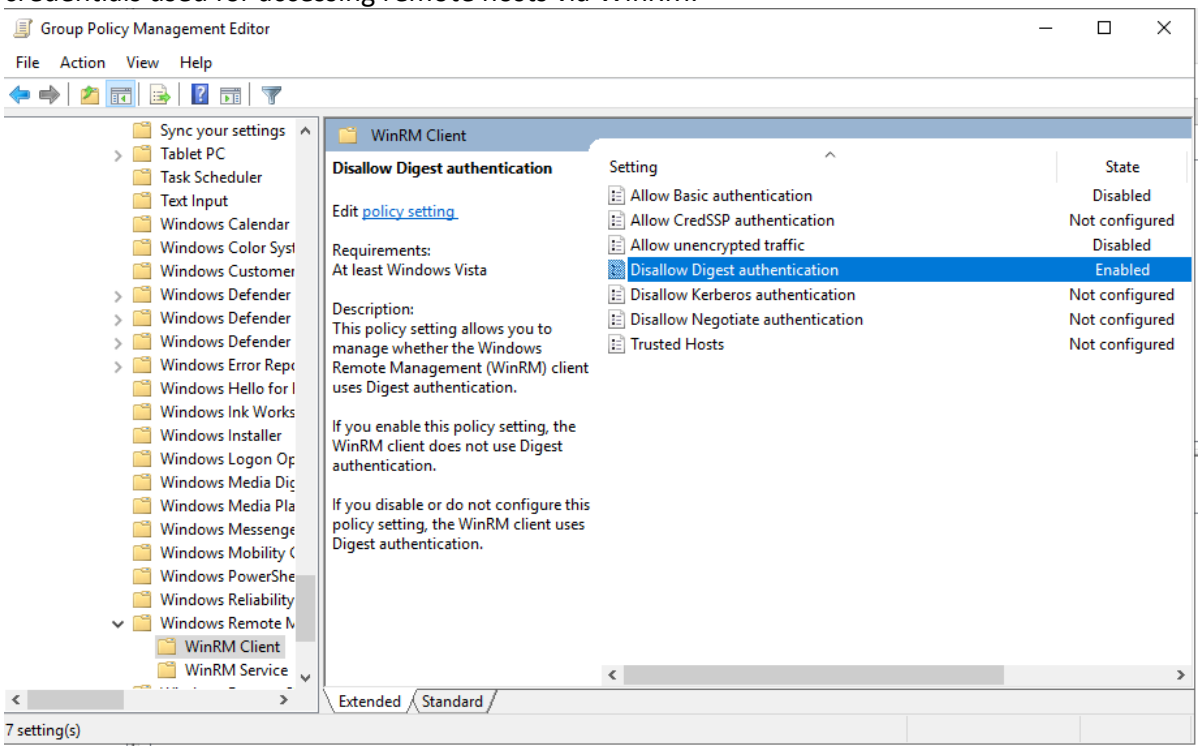


Image 313-Ensure 'Disallow Digest authentication' is set to 'Enabled'

7.8.27.2 WinRM Service

7.8.27.2.1 Ensure 'Allow Basic authentication' is set to 'Disabled'

This policy setting controls whether the Windows Remote Management (WinRM) service will accept Basic authentication from remote clients. The recommended state is: Disabled. Basic authentication is less secure compared to other available authentication methods in WinRM because it transmits credentials, including passwords, in plain text. If an attacker captures network packets where WinRM is active, they might be able to obtain the credentials used to access remote hosts via WinRM.

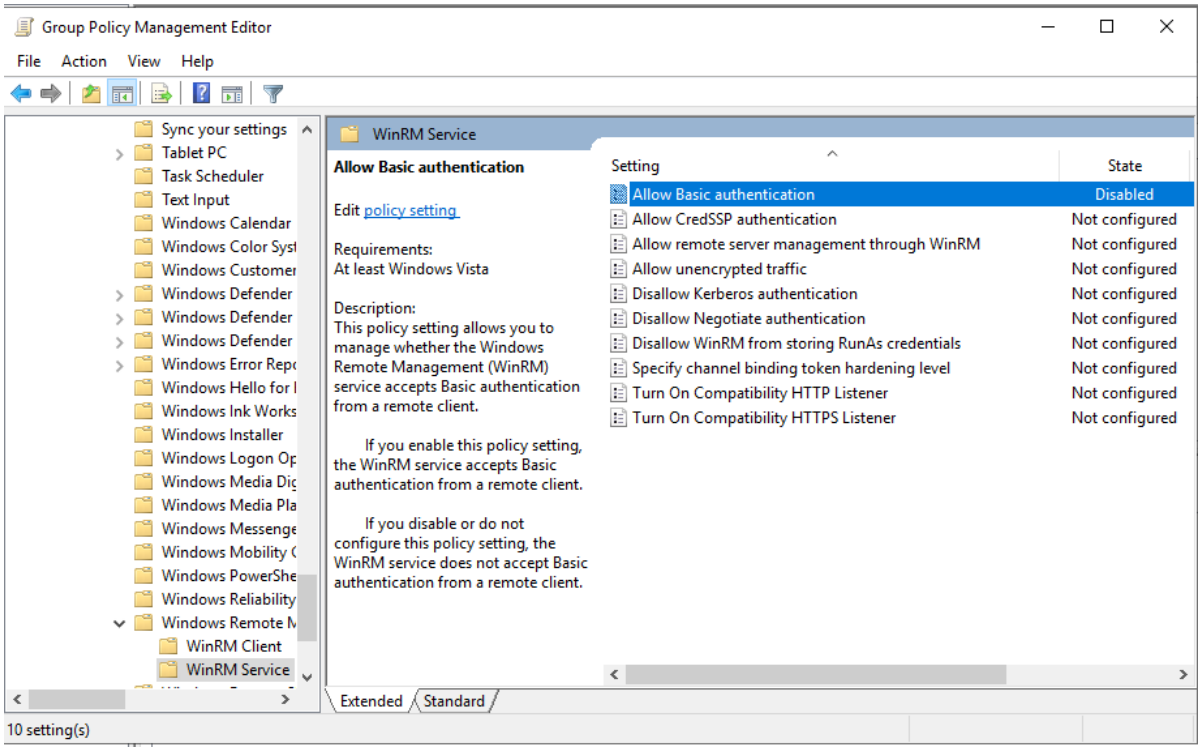


Image 314-Ensure 'Allow Basic authentication' is set to 'Disabled'

7.8.27.2.2 Ensure 'Allow remote server management through WinRM' is set to 'Disabled'

This policy setting controls whether the Windows Remote Management (WinRM) service automatically listens for requests over HTTP on the default port. The recommended state is: Disabled. Features that allow inbound network connections can be potential security risks. To minimize this risk, enable the WinRM service only on trusted networks and consider using additional security measures such as IPsec where possible.

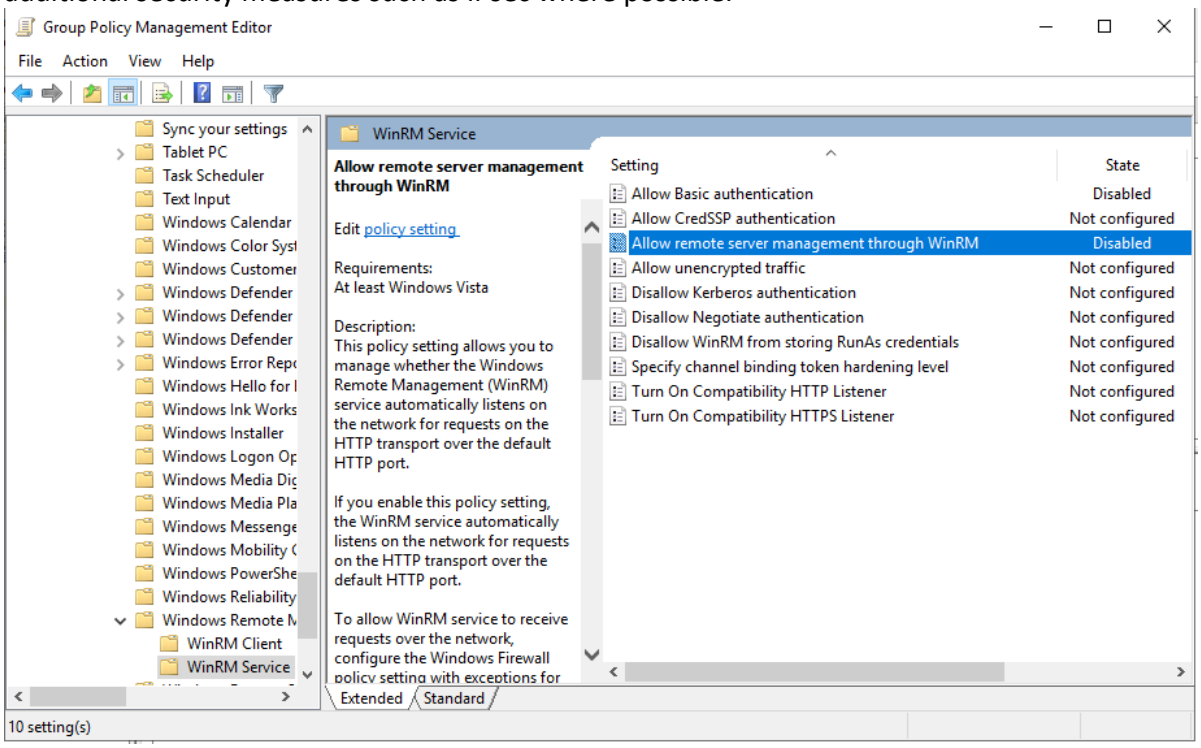


Image 315-Ensure 'Allow remote server management through WinRM' is set to 'Disabled'

7.8.27.2.3 Ensure 'Allow unencrypted traffic' is set to 'Disabled'

This policy setting controls whether the Windows Remote Management (WinRM) service transmits and receives unencrypted messages over the network. The recommended state is: Disabled. Encrypting WinRM network traffic helps to protect against unauthorized viewing or tampering of messages while they are in transit.

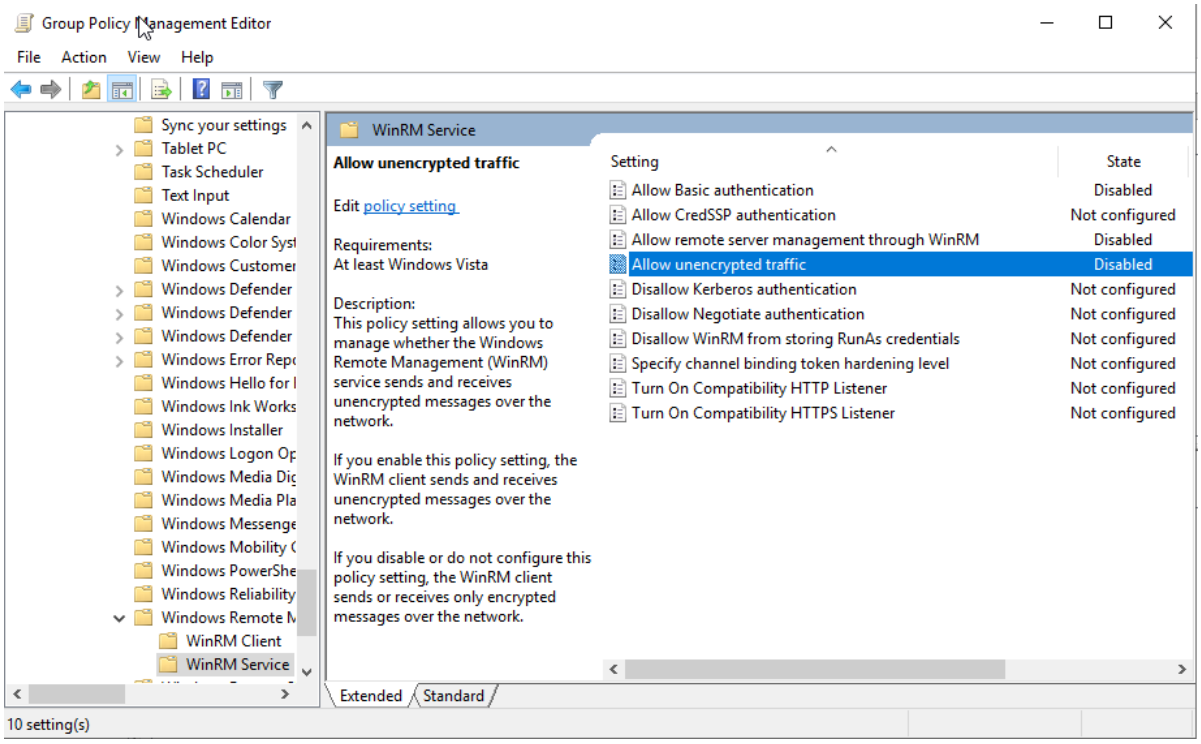


Image 316-Ensure 'Allow unencrypted traffic' is set to 'Disabled'

7.8.27.2.4 Ensure 'Disallow WinRM from storing RunAs credentials' is set to 'Enabled'

This policy setting manages whether the Windows Remote Management (WinRM) service allows the storage of RunAs credentials for plug-ins. The recommended state is: Enabled. Enabling and then disabling this policy will require you to reset any previously configured RunAsPassword values. While storing RunAs credentials offers convenience, it slightly increases the risk of account compromise. For instance, if you leave your desktop unattended without locking it, someone could potentially access both your computer and any managed hosts via WinRM using the cached RunAs credentials.

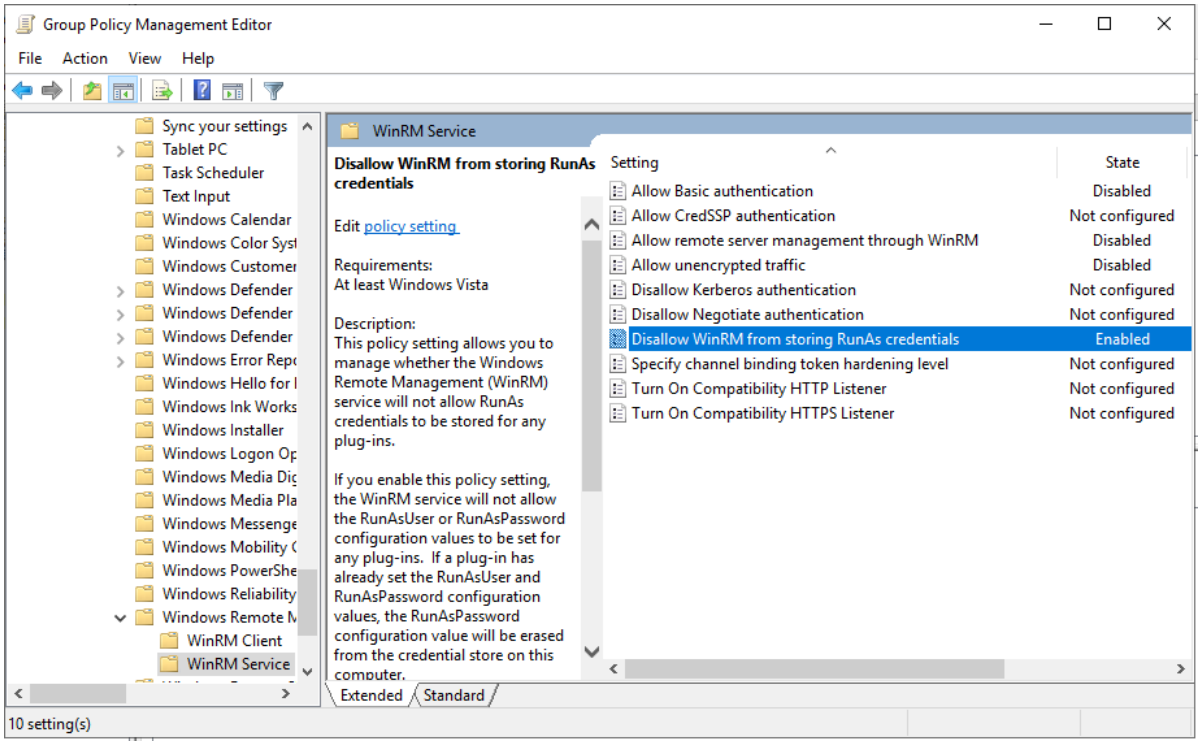


Image 317-Ensure 'Disallow WinRM from storing RunAs credentials' is set to 'Enabled'

7.8.28 Windows Remote Shell

7.8.28.1 Ensure 'Allow Remote Shell Access' is set to 'Disabled'

This policy setting controls the configuration of remote access to all supported shells for executing scripts and commands. The recommended state for this setting is: Disabled. The Group Policy Management Editor (GPME) help text incorrectly suggests that enabling this setting will reject new Remote Shell connections, while disabling it will allow them. In reality, enabling the setting will allow Remote Shell connections, and disabling it will reject them. This is a wording error by Microsoft in the Administrative Template. Features that enable inbound network connections, such as remote access, present potential security risks. It is advisable to enable Windows Remote Shell only on trusted networks and, when possible, use additional security measures like IPsec.

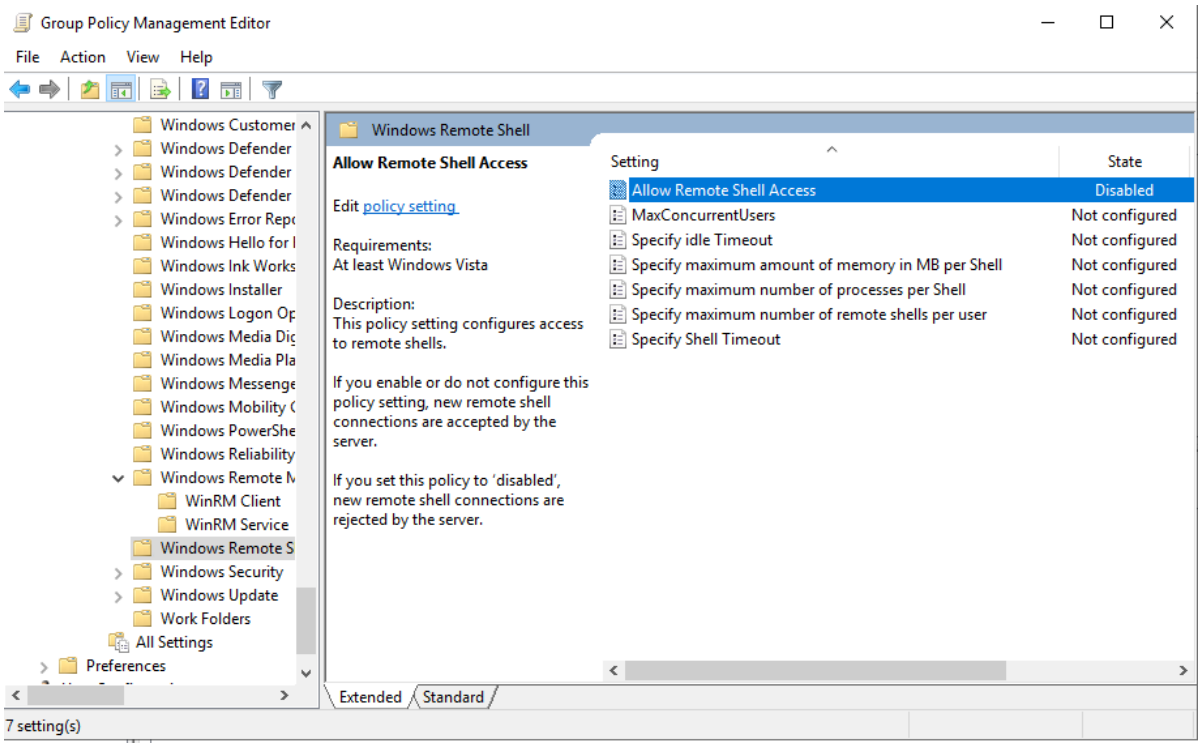


Image 318-Ensure 'Allow Remote Shell Access' is set to 'Disabled'

7.8.29 Windows Security (formerly Windows Defender Security Center)

7.8.29.1 App and browser protection

7.8.29.1.1 Ensure 'Prevent users from modifying settings' is set to 'Enabled'

This policy setting restricts users from altering the Exploit protection settings within Windows Security. The recommended state for this setting is: Enabled. To ensure that the organization's specific configuration remains intact, only authorized IT staff should be permitted to modify the exploit protection settings.

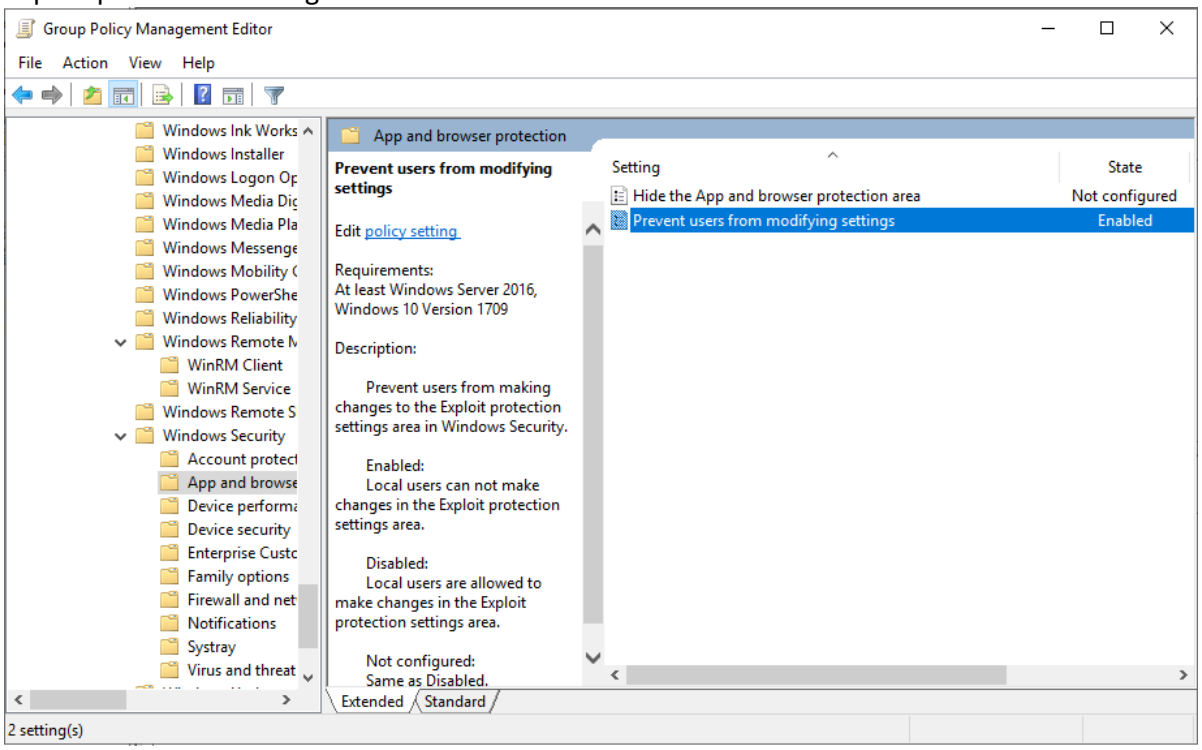


Image 319-Ensure 'Prevent users from modifying settings' is set to 'Enabled'

7.8.30 Windows Update

7.8.30.1 Legacy Policies

7.8.30.1.1 Ensure 'No auto-restart with logged on users for scheduled automatic updates installations' is set to 'Disabled'

This policy setting dictates that Automatic Updates will wait for users to manually restart their computers to complete a scheduled installation. The recommended state for this setting is: Disabled. This setting is applicable only if Automatic Updates is configured to perform scheduled installations. If Automatic Updates is set to Disabled, this setting will have no effect. Some security updates necessitate a restart to finalize the installation. Without automatic restarts, the computer may remain in an insecure state if users delay restarting, as no new updates will be downloaded until the restart occurs.

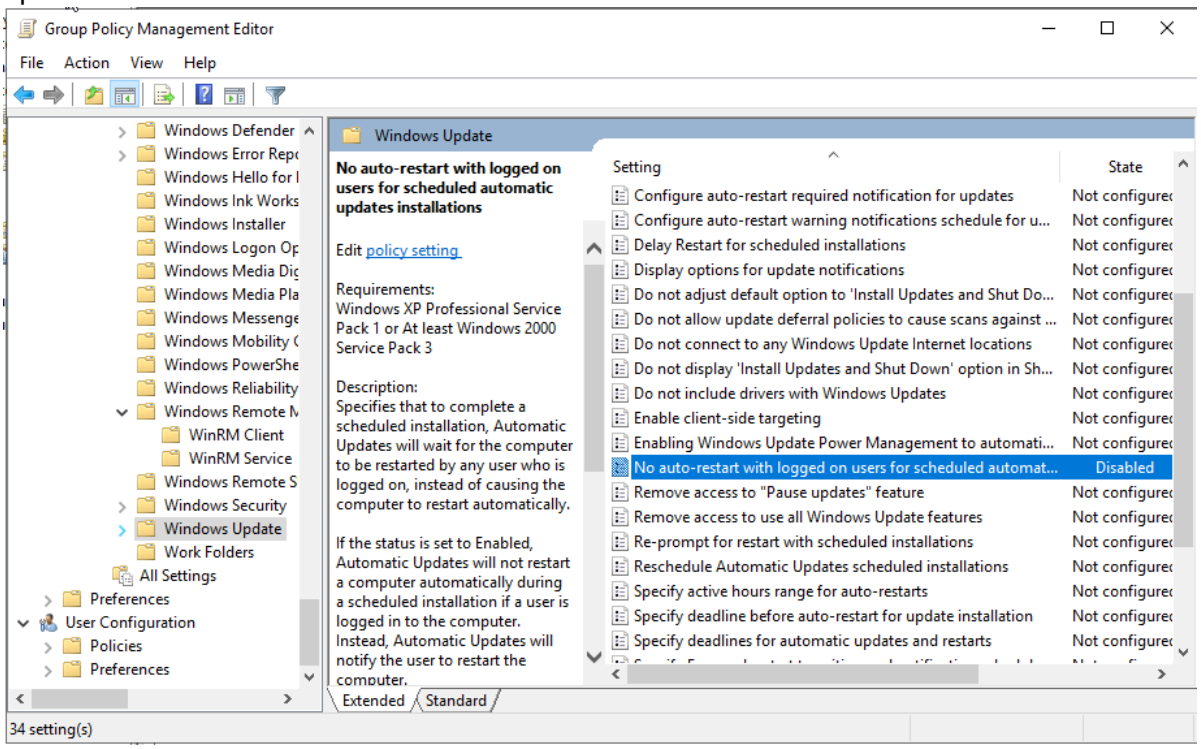


Image 320-Ensure 'No auto-restart with logged on users for scheduled automatic updates installations' is set to 'Disabled'

7.8.30.2 Manage end user experience

7.8.30.2.1 Ensure 'Configure Automatic Updates' is set to 'Enabled'

This policy setting determines whether computers in your network will receive security updates from Windows Update or WSUS. If you enable this setting, the operating system will automatically detect network connections and use them to search for updates on Windows Update or your designated intranet site. Once enabled, you must select one of the following options in the Configure Automatic Updates Properties dialog box to define the service's behavior:

- 2 - Notify for download and auto-install (Notifies before downloading updates)
- 3 - Auto-download and notify for install (Downloads updates automatically and notifies when they are ready to be installed) (Default setting)
- 4 - Auto-download and schedule the install (Automatically downloads updates and installs them on a specified schedule)
- 5 - Allow local admin to choose setting (Leaves the choice to local administrators, which is not recommended)

The recommended state for this setting is: Enabled. Note that the sub-setting "Configure automatic updating:" has four possible values, all valid depending on specific needs, but using a value of 4 - Auto-download and schedule the install is suggested if feasible. Organizations using third-party patching solutions may opt to set this policy to Disabled to prevent interference with their patching processes. Although Windows is rigorously tested before release, issues may arise post-release. Configuring Automatic Updates ensures that computers always have the latest critical updates and service packs installed.

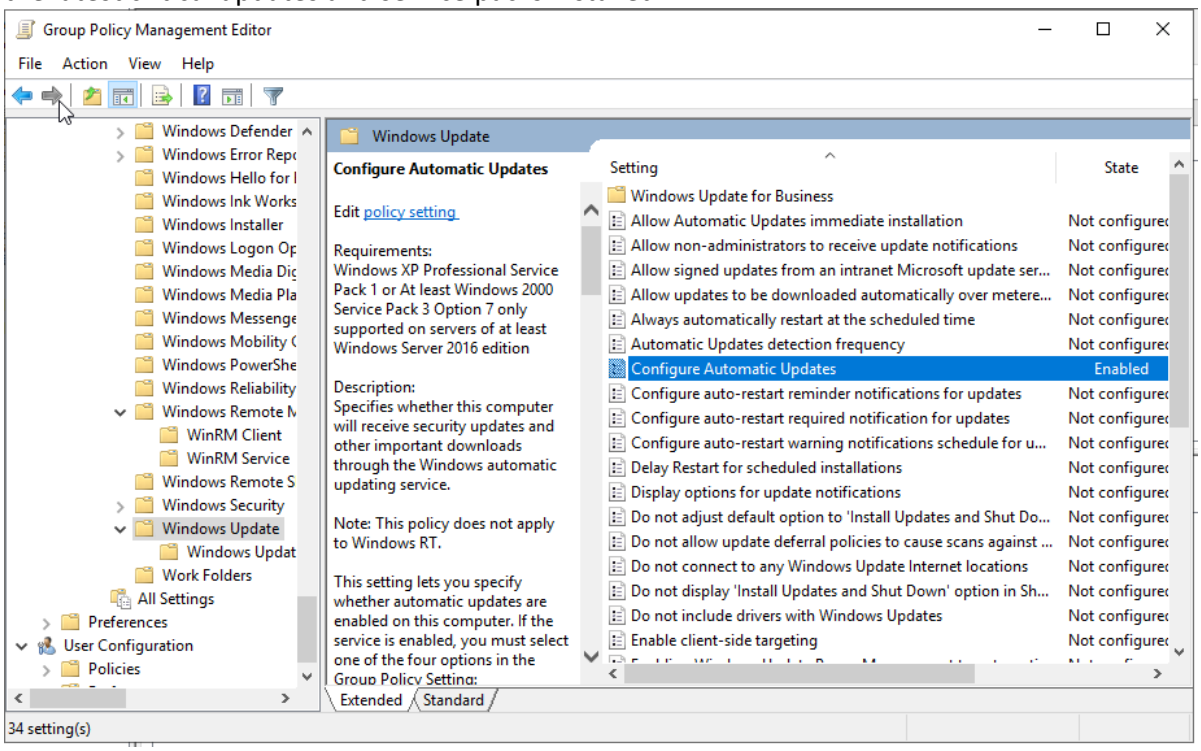


Image 321-Ensure 'Configure Automatic Updates' is set to 'Enabled'

7.8.30.3 Manage updates offered from Windows Update (formerly Defer Windows Updates and Windows Update for Business)

7.8.30.3.1 Ensure 'Manage preview builds' is set to 'Disabled'

This policy setting governs the reception of updates before their official release.

- Dev Channel: Suitable for highly technical users, offering builds from the earliest stage of development that are not tied to a specific Windows 10 release.
- Beta Channel: Ideal for those interested in upcoming features, where feedback helps fix issues before the major release.
- Release Preview Channel (default): Provides access to the next Windows 10 release before its public availability, supported by Microsoft. Recommended for companies to test upcoming releases before broad deployment.

The recommended state for this setting is: Disabled. Note that preview builds require a telemetry level of 2 or higher and domain registration on insider.windows.com.
Allowing experimental features in a managed environment can introduce bugs and security risks, making it preferable to use only production-ready builds.

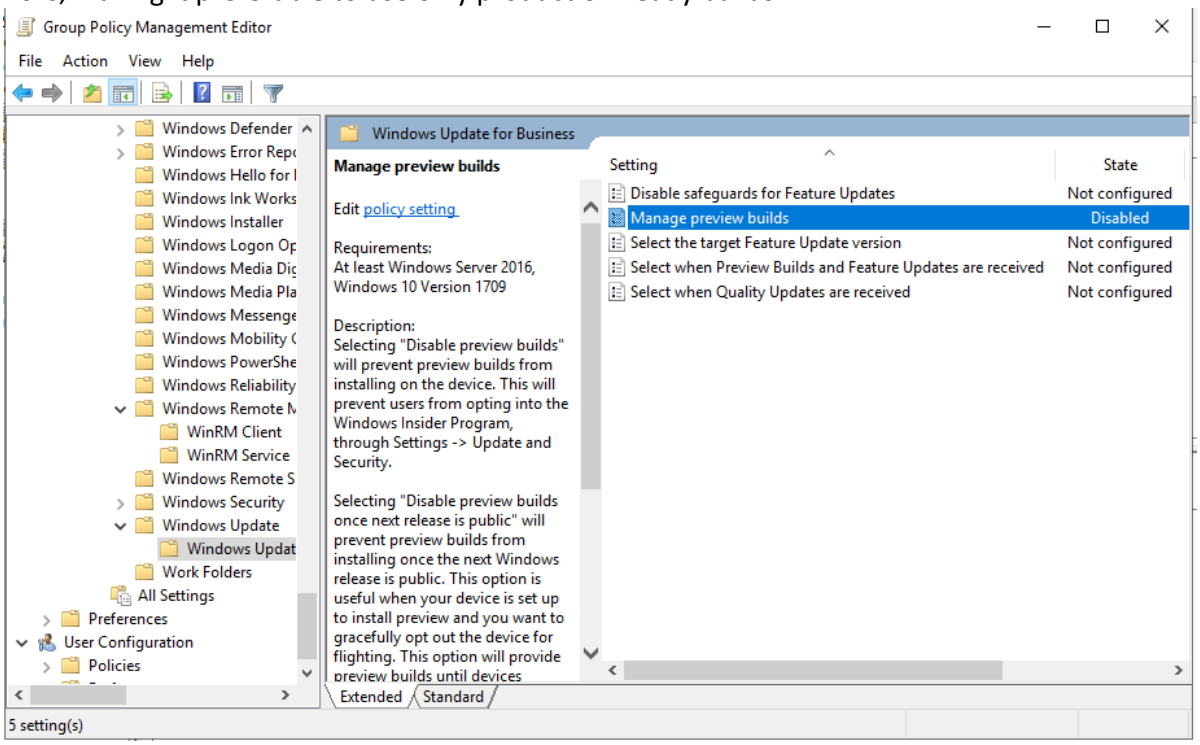


Image 322-Ensure 'Manage preview builds' is set to 'Disabled'

7.8.30.3.2 Ensure 'Select when Preview Builds and Feature Updates are received' is set to 'Enabled: 180 or more days'

This policy setting manages the timing for receiving Preview Builds or Feature Updates.

- Defer Updates: Allows devices to delay the next Feature Update for up to 14 days for pre-release channels and up to 365 days for the Semi-Annual Channel. If updating from the Semi-Annual Channel, you can specify a version for the device to remain on until the policy is updated or the device reaches end of service. If both policies are set, the specified version takes precedence over deferrals.
- Pause Updates: Temporarily halts Feature Updates for up to 35 days from the start date or until the pause is cleared, while still offering Quality Updates.

The policy has no effect if "Allow Diagnostic Data" is set to 0. Also, starting with Windows 10 R1607, the Dual Scan feature may conflict with WSUS updates, requiring adjustments to prevent interference. More details on Dual Scan can be found in related Microsoft blogs. Additionally, values over 180 days were not recognized before Windows 10 R1703; now, deferrals can be up to 365 days.

In a production environment, it's advisable to use only publicly available software and features that have undergone extensive beta testing.

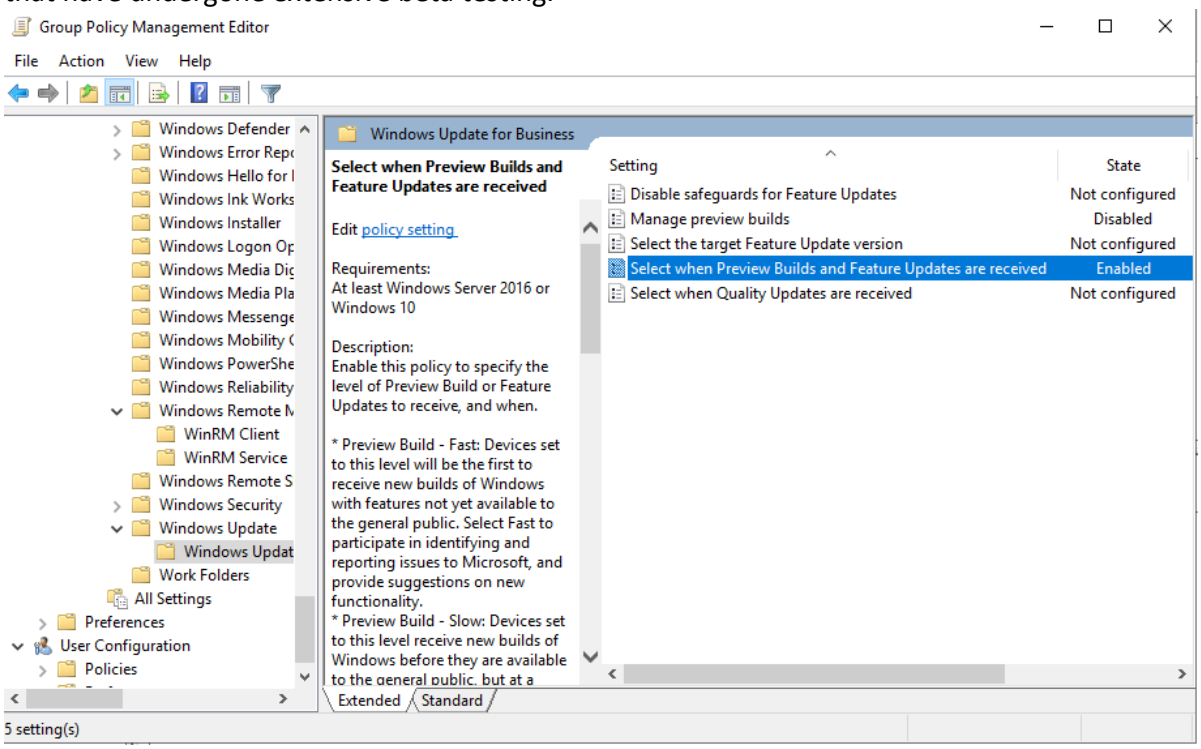


Image 323-Ensure 'Select when Preview Builds and Feature Updates are received' is set to 'Enabled: 180 or more days'

7.8.30.3.3 Ensure 'Select when Quality Updates are received' is set to 'Enabled: 0 days'

This setting determines the timing for receiving Quality Updates.

The recommended configuration is: Enabled, with 0 days delay.

If the "Allow Diagnostic Data" policy is set to 0, this setting will not be effective. Additionally, starting with Windows Server 2016 RTM (Release 1607), the Dual Scan feature may conflict with updates from Windows Server Update Services (WSUS) or manual updates. In such cases, you might need to set this policy to Not Configured or use the "Do not allow update deferral policies to cause scans against Windows Update" setting, introduced in Windows 10 Release 1709, to avoid interference. Further information on Dual Scan can be found in related Microsoft blogs.

Installing Quality Updates promptly is crucial as they often include important bug fixes and security patches.

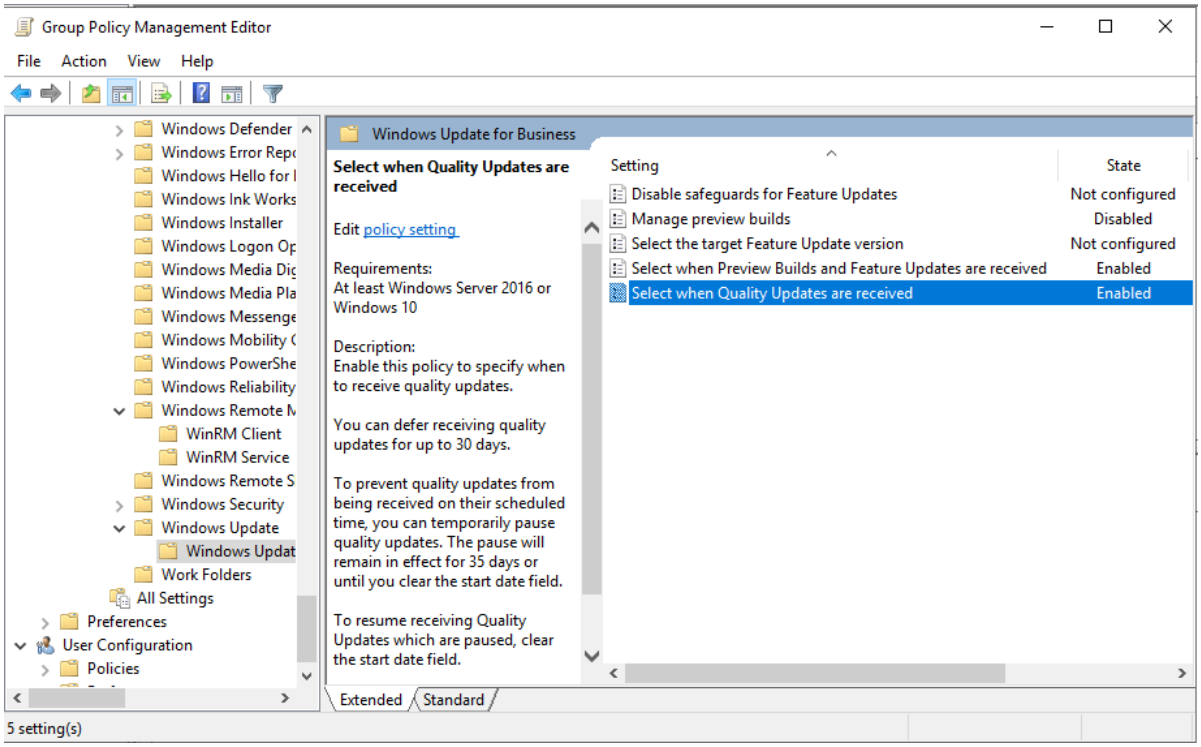


Image 324-Ensure 'Select when Quality Updates are received' is set to 'Enabled: 0 days'

8 Administrative Templates (User)

The Administrative Templates (User) section in Group Policy provides a set of policies for configuring user-specific settings in Windows. This includes controls over desktop environments, start menu options, and user interface elements. By defining these policies, administrators can tailor the user experience, enforce security settings, and manage application behavior to align with organizational standards.

8.1 Control Panel

The Control Panel section in Group Policy allows administrators to manage and restrict access to various Control Panel settings and applets. This includes controlling user access to specific configuration options, such as system settings, hardware configurations, and network settings. By applying these policies, administrators can streamline user interactions and maintain consistent system configurations across a network.

8.1.1 Personalization (formerly Desktop Themes)

8.1.1.1 Ensure 'Enable screen saver' is set to 'Enabled'

This policy setting controls whether desktop screen savers are enabled or disabled. The recommended configuration is: Enabled.

Enabling a timed screen saver with password protection helps prevent unauthorized access if a user forgets to lock their computer when stepping away, thereby enhancing security against potential hijacking.

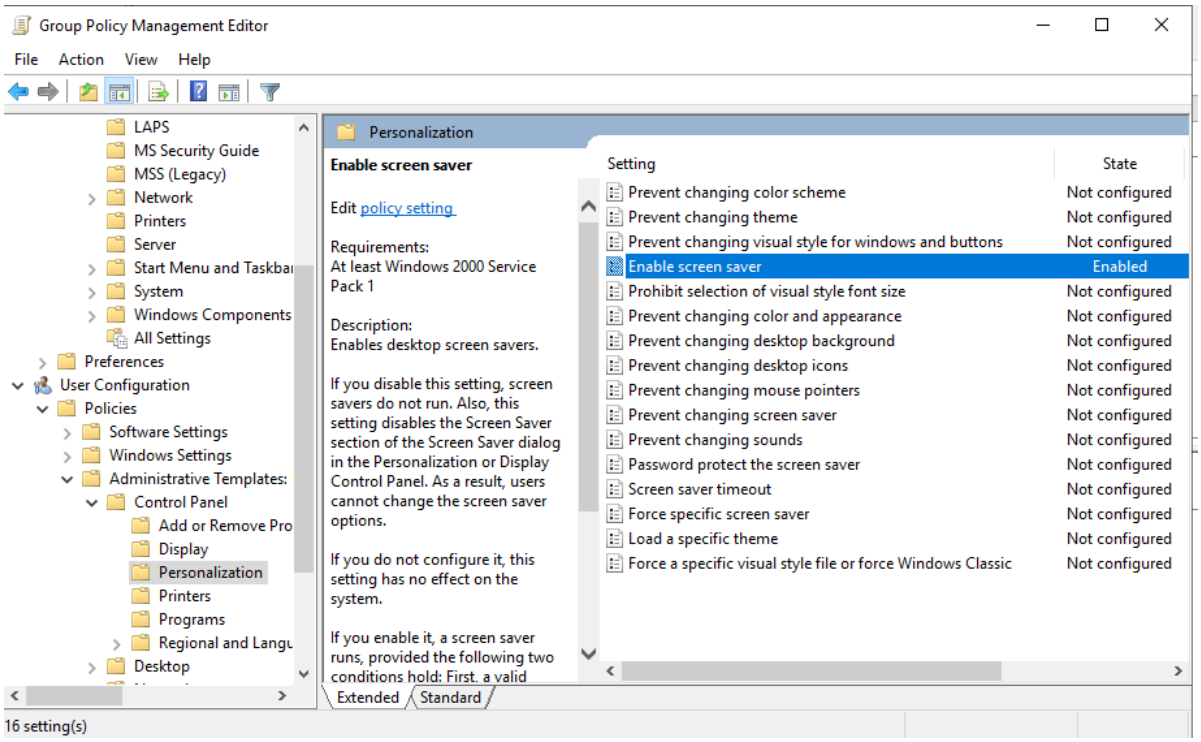


Image 325-Ensure 'Enable screen saver' is set to 'Enabled'

8.2 Start Menu and Taskbar

The Start Menu and Taskbar section in Group Policy enables administrators to customize and control the appearance and functionality of the Start Menu and Taskbar for users. This includes settings for pinning applications, hiding specific icons, and configuring the layout and behavior of these interfaces. By managing these options, administrators can ensure a consistent user experience and enhance productivity while aligning with organizational policies.

8.2.1 Notifications

8.2.1.1 Ensure 'Enable screen saver' is set to 'Enabled'

This policy setting disables toast notifications on the lock screen. The recommended configuration is: Enabled.

Although toast notifications can be useful, they may reveal sensitive personal or business information when the device is unattended. Disabling this feature helps protect against unauthorized viewing of such data.

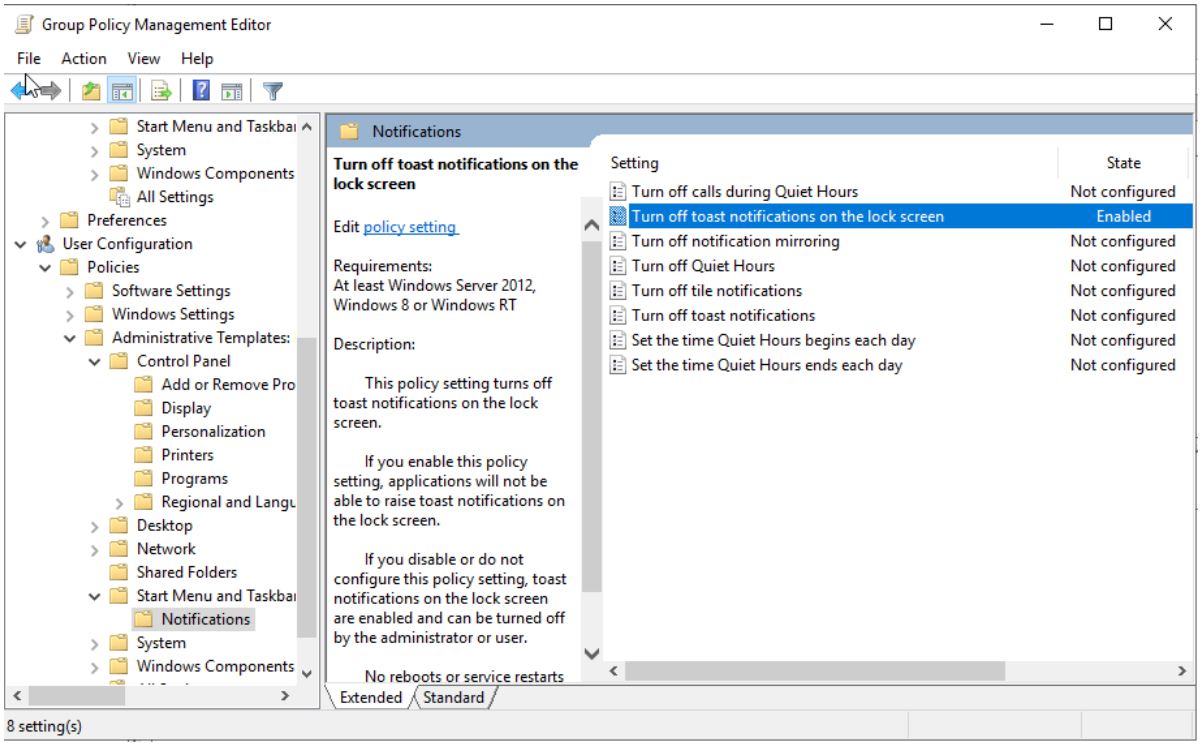


Image 326-Ensure 'Enable screen saver' is set to 'Enabled'

8.3 System

The System section in Group Policy provides administrators with the ability to manage and configure various system-level settings. This includes controls for system performance, power management, user logon and logoff behaviors, and security settings. By applying policies in this section, administrators can optimize system operations, enforce security measures, and ensure consistent configurations across all networked computers.

8.3.1 Internet Communication Management

8.3.1.1 Internet Communication settings

8.3.1.1.1 Ensure 'Turn off Help Experience Improvement Program' is set to 'Enabled'

This policy setting determines whether users are allowed to participate in the Help Experience Improvement program, which gathers data on how Windows Help is used to enhance its functionality. The recommended state for this setting is: Enabled.

In large, enterprise-managed environments, it may be preferable to avoid having information collected by Microsoft from managed client computers.

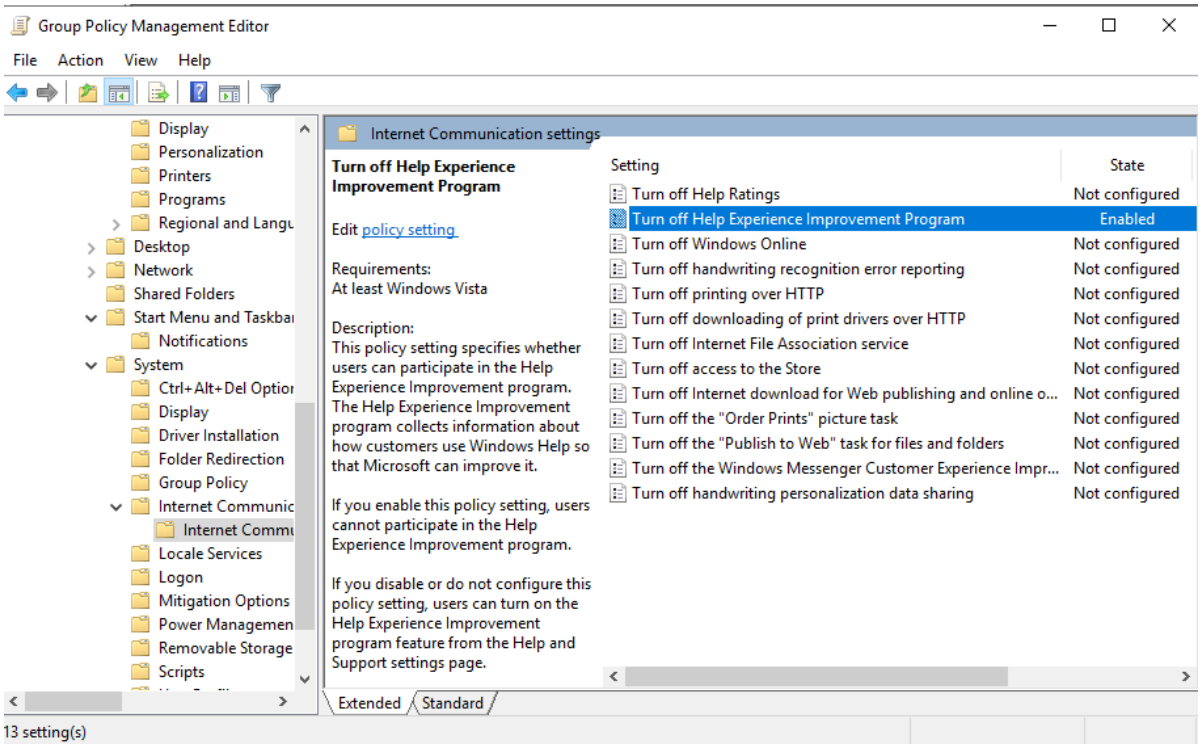


Image 327-Ensure 'Turn off Help Experience Improvement Program' is set to 'Enabled'

8.4 Windows Components

The Windows Components section in Group Policy allows administrators to configure and manage built-in Windows features and applications. This includes settings for components like Internet Explorer, Windows Defender, and Windows Update. Administrators can customize how these features operate and enforce policies to ensure that they meet organizational requirements and security standards.

8.4.1 Attachment Manager

8.4.1.1 Ensure 'Do not preserve zone information in file attachments' is set to 'Disabled'

This policy setting controls whether Windows assigns zone information (such as restricted, Internet, intranet, or local) to file attachments, a feature that requires NTFS and will not work on FAT32. Without this zone information, Windows cannot accurately assess the risk associated with the file. The recommended state for this setting is: Disabled.

The Attachment Manager warns users when opening or executing files marked as coming from an untrusted source, unless the file's zone information is removed using the "Unblock" button in the file's properties or a tool like Microsoft Sysinternals Streams.

Files downloaded from the Internet or restricted zones could be moved to seemingly safer locations, such as intranet file shares, and executed by users who may not recognize the potential risk. The Attachment Manager helps prevent this by warning users about files from untrusted sources, provided the zone information has not been removed.

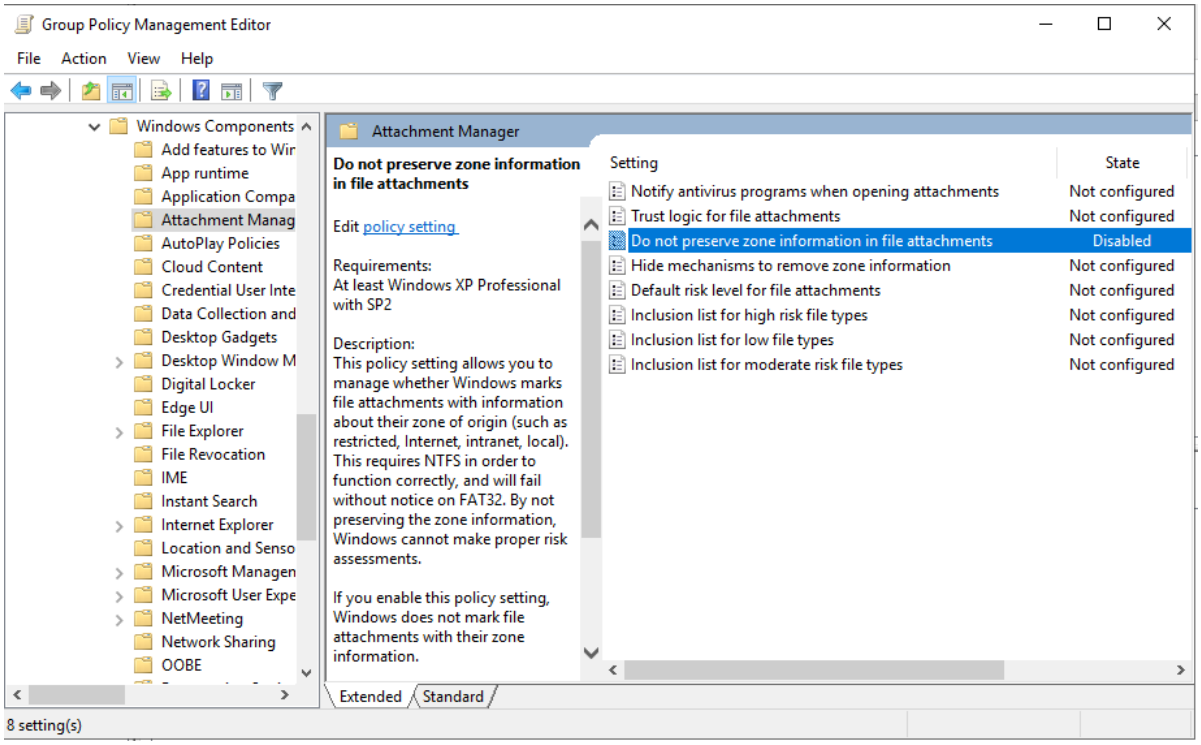


Image 328-Ensure 'Do not preserve zone information in file attachments' is set to 'Disabled'

8.4.1.2 Ensure 'Notify antivirus programs when opening attachments' is set to 'Enabled'

This policy setting controls how registered antivirus programs are notified, ensuring that all registered programs receive notifications. The recommended state for this setting is: Enabled.

To ensure proper functionality of this policy setting, an updated antivirus program must be installed.

Antivirus programs that do not conduct on-access scans might not be able to scan files that are downloaded, which could leave the system vulnerable.

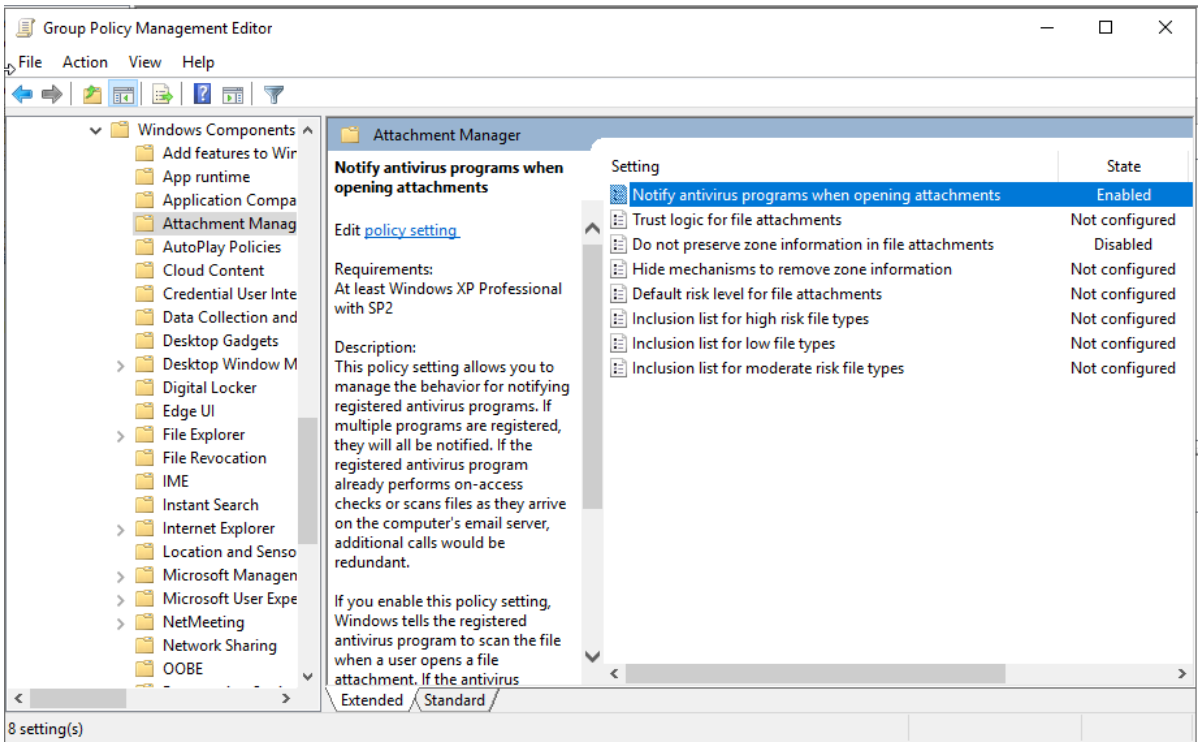


Image 329-Ensure 'Notify antivirus programs when opening attachments' is set to 'Enabled'

8.4.2 Cloud Content

8.4.2.1 Ensure 'Configure Windows spotlight on lock screen' is set to 'Disabled'

This policy setting allows you to configure Windows Spotlight for the lock screen. The recommended state for this setting is: Disabled.

According to Microsoft TechNet, this policy applies only to Windows 10 Enterprise and Windows 10 Education editions.

Disabling this setting helps protect your data from being shared with third parties. Windows Spotlight collects data to suggest apps and display images from the internet, which could raise privacy concerns.

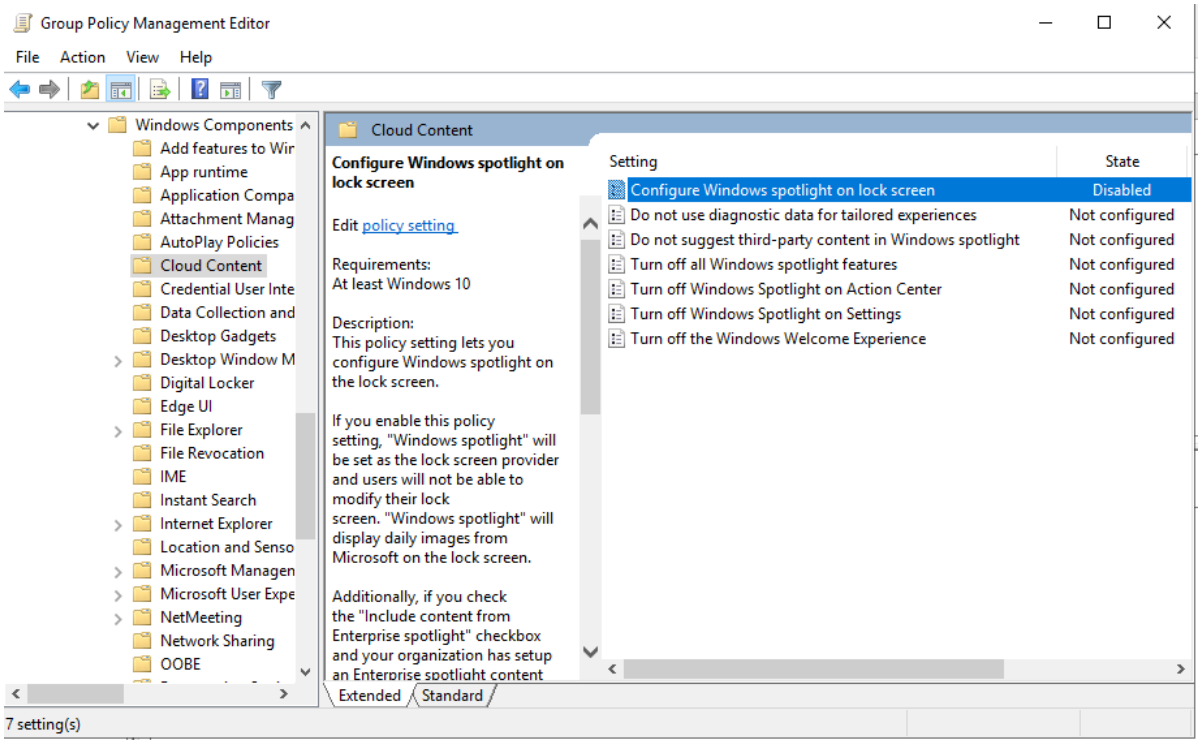


Image 330-Ensure 'Configure Windows spotlight on lock screen' is set to 'Disabled'

8.4.2.2 Ensure 'Do not suggest third-party content in Windows spotlight' is set to 'Enabled'

This policy setting controls whether Windows suggests apps and content from third-party publishers. The recommended state for this setting is: Enabled.

Enabling this setting helps ensure that your data is not shared with third parties. Windows Spotlight collects data to recommend apps and display images from the internet, which could pose privacy risks.

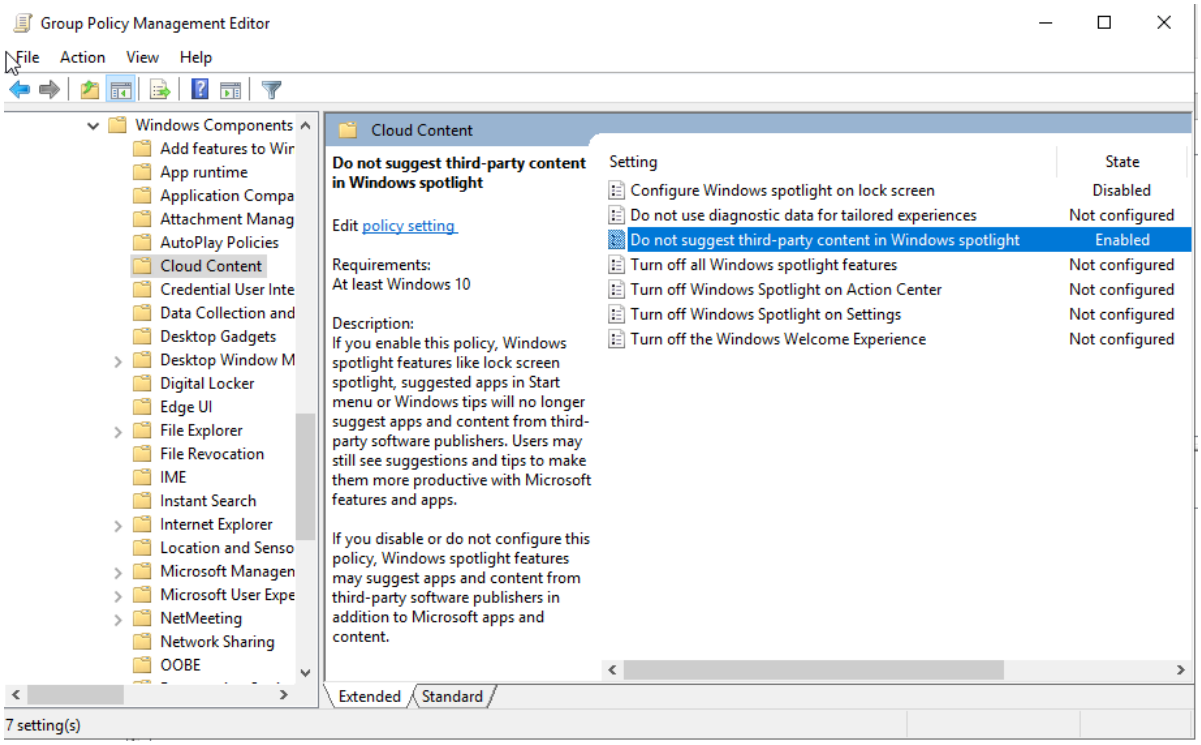


Image 331-Ensure 'Do not suggest third-party content in Windows spotlight' is set to 'Enabled'

8.4.2.3 Ensure 'Do not use diagnostic data for tailored experiences' is set to 'Enabled'

This setting controls whether Windows can use diagnostic data to offer personalized experiences to the user. The recommended state for this setting is: Enabled.

The collection and use of personalized data raise privacy and security concerns for many organizations.

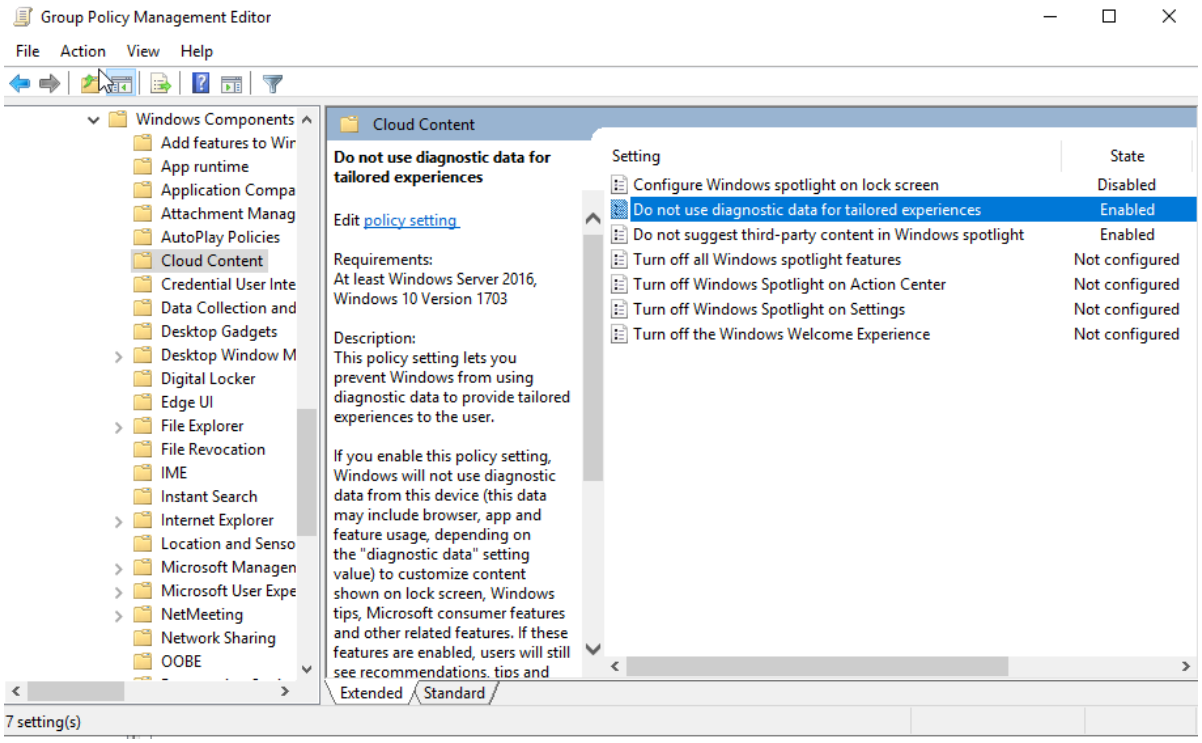


Image 332-Ensure 'Do not use diagnostic data for tailored experiences' is set to 'Enabled'

8.4.2.4 Ensure 'Turn off all Windows spotlight features' is set to 'Enabled'

This policy setting allows you to disable all Windows Spotlight features simultaneously. The recommended state for this setting is: Enabled.

According to Microsoft TechNet, this setting applies only to Windows 10 Enterprise and Windows 10 Education editions.

Enabling this setting helps prevent your data from being shared with third parties, as Windows Spotlight collects data to suggest apps and display images from the internet.

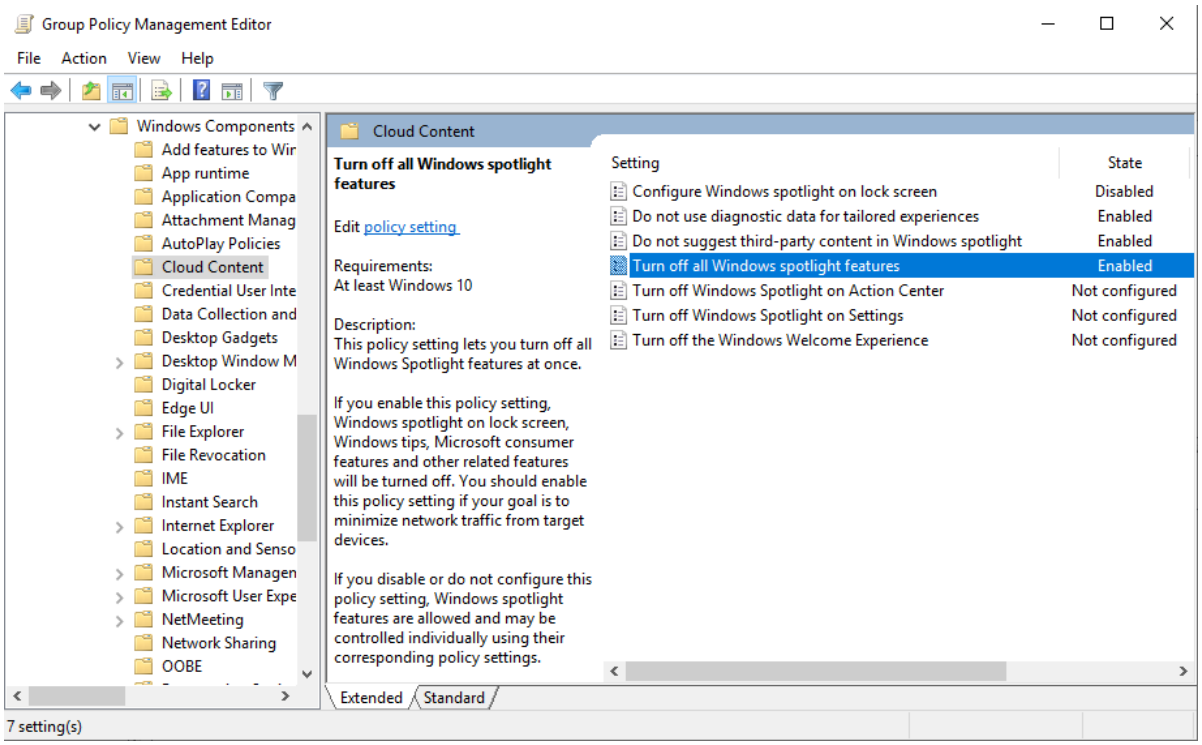


Image 333-Ensure 'Turn off all Windows spotlight features' is set to 'Enabled'

8.4.3 Network Sharing

8.4.3.1 Ensure 'Prevent users from sharing files within their profile.' is set to 'Enabled'

This policy setting controls whether users can share files within their profile. By default, users can share files from their profile with others on their network, provided an administrator has opted in the computer using the sharing wizard. The recommended state for this setting is: Enabled.

Improper configuration could lead to accidental sharing of sensitive data with unauthorized users. In a managed enterprise environment, the company should use a centralized file-sharing solution, such as a file server or SharePoint, rather than allowing users to share files directly from their profiles.

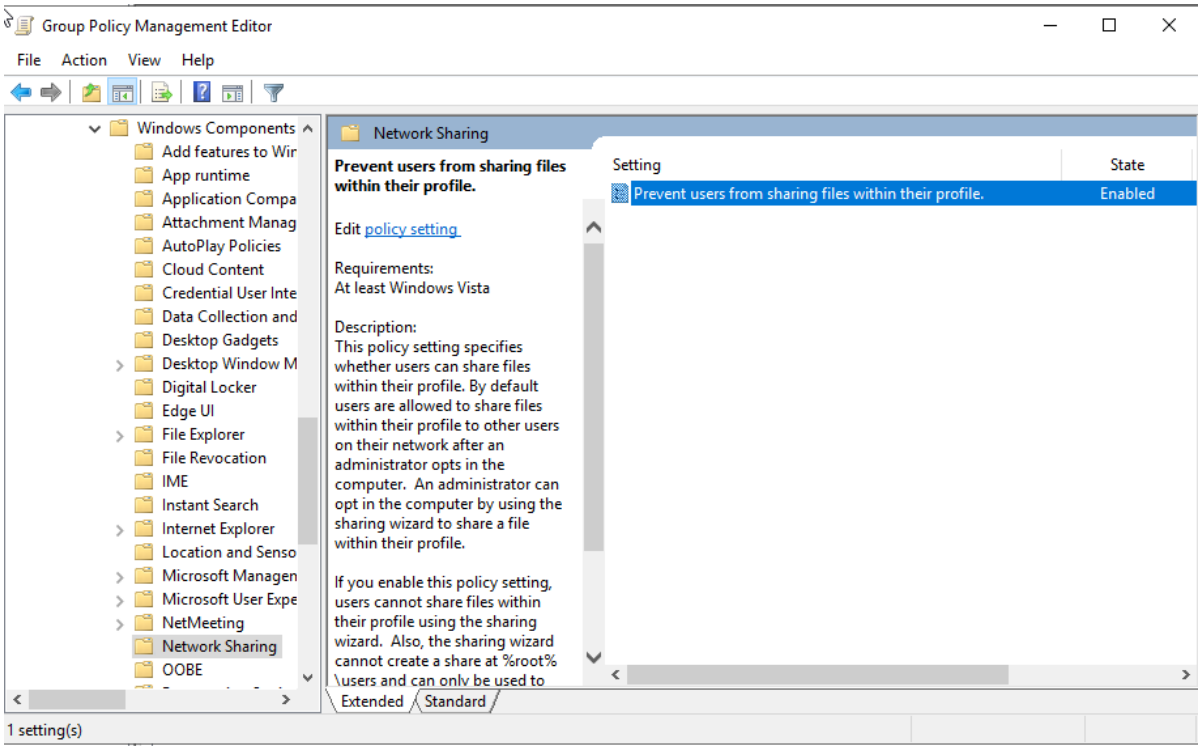


Image 334-Ensure 'Prevent users from sharing files within their profile.' is set to 'Enabled'

8.4.4 Windows Installer

8.4.4.1 Ensure 'Always install with elevated privileges' is set to 'Disabled'

This setting controls whether Windows Installer should use system permissions for installing programs. It must be enabled in both the Computer Configuration and User Configuration folders to be effective.

Caution: Enabling this setting could allow skilled users to exploit the permissions to alter their access levels, potentially gaining permanent access to restricted files and folders. The User Configuration aspect of this setting may not be secure.

The recommended state for this setting is: Disabled.

Users with limited privileges might exploit this feature to create an installation package that grants themselves administrative access or performs other unauthorized actions, such as installing malicious software.

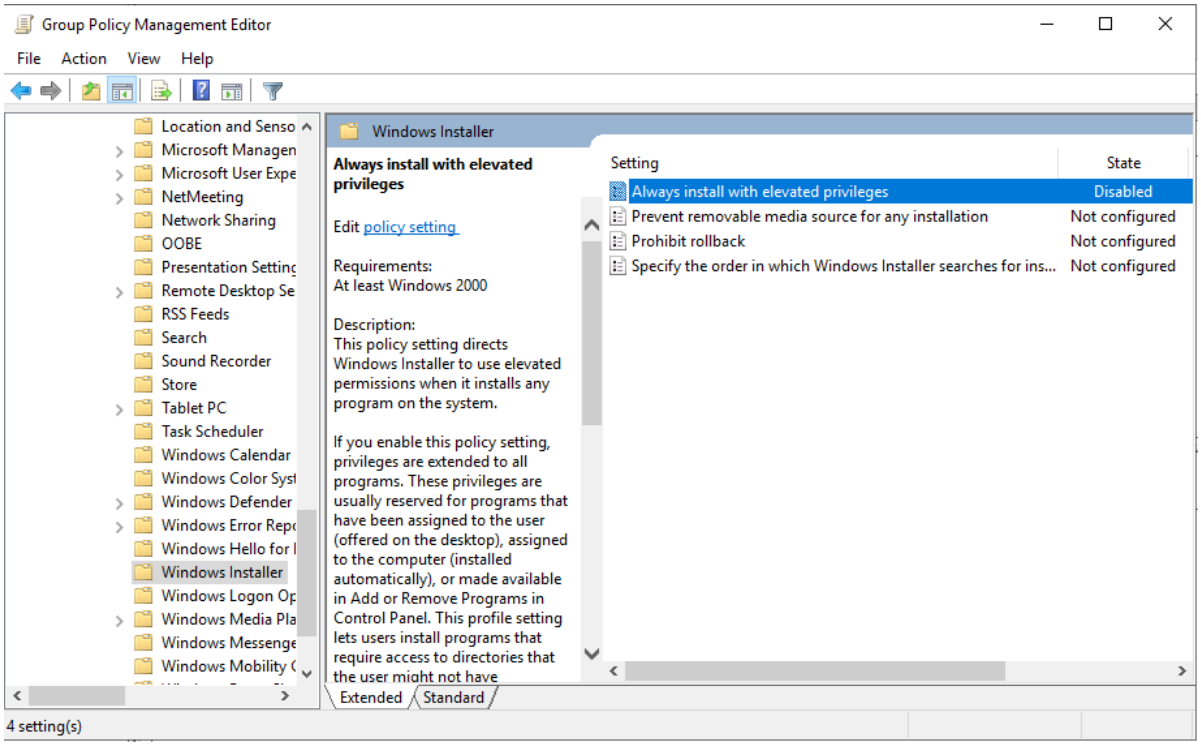


Image 335-Ensure 'Always install with elevated privileges' is set to 'Disabled'

8.4.5 Windows Media Player

8.4.5.1 Playback

8.4.5.1.1 Ensure 'Prevent Codec Download' is set to 'Enabled'

This setting manages whether Windows Media Player is permitted to download extra codecs needed to decode unfamiliar media files.

The recommended state for this setting is: Enabled.

Allowing Media Player to download additional codecs poses a risk if a malicious file triggers the installation of a harmful codec. Any codec required for essential tasks should be thoroughly tested for legitimacy and provided by the IT department to mitigate potential security risks.

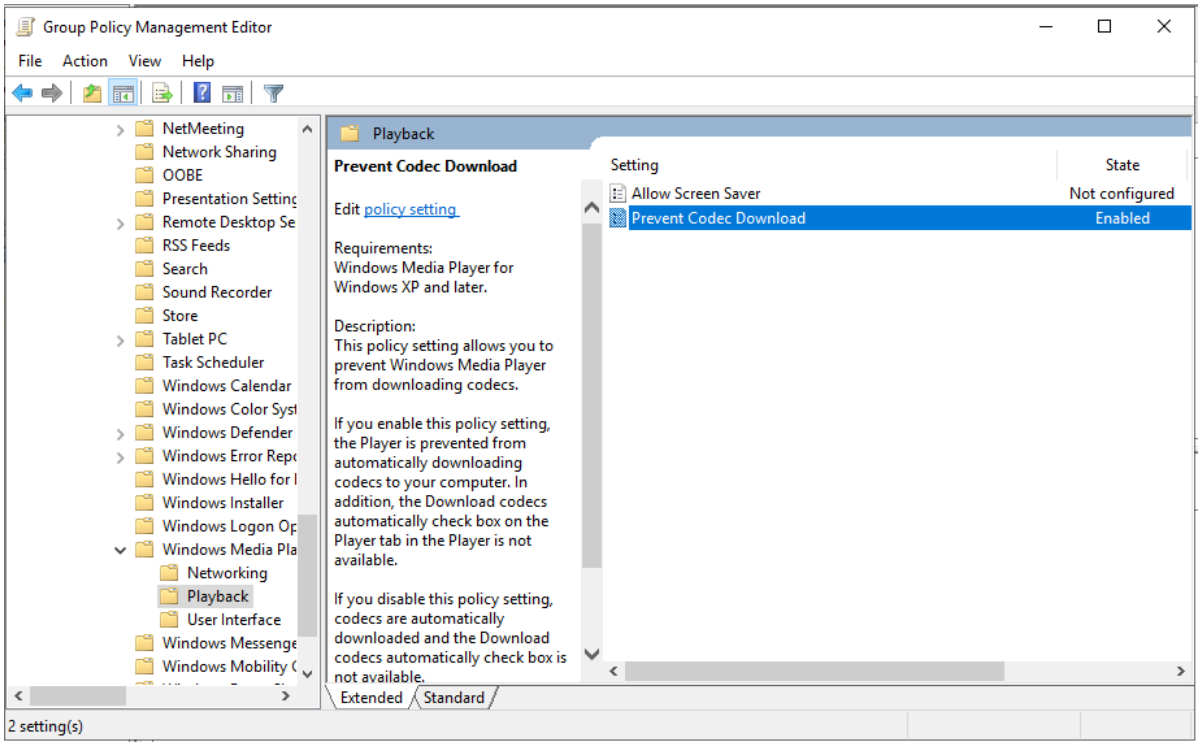


Image 336-Ensure 'Prevent Codec Download' is set to 'Enabled'

9 Conclusion

In conclusion, the application of CIS Benchmark hardening measures and the remediation of vulnerabilities on the Windows Server 2019 environment are crucial steps toward strengthening system security. By adhering to these rigorous standards and addressing identified weaknesses, the defense against cyber threats will be significantly enhanced.

Using the Wazuh security tool the initial security score provided at the outset has served as a benchmark for the current security posture. Following the comprehensive hardening and remediation process, the final security score will be presented. This final score will not only reflect the improvements made but also validate the effectiveness of the implemented security measures. Through this comparative analysis, the progress achieved and the strengthened security stance of the server will be clearly demonstrated.