CIS Microsoft Windows Server 2022 Benchmark

v5.1.0 - 07-28-2026

Terms of Use

Please see the below link for our current terms of use:

https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/

For information on referencing and/or citing CIS Benchmarks in 3rd party documentation (including using portions of Benchmark Recommendations) please contact CIS Legal (legalnotices@cisecurity.org) and request guidance on copyright usage.

NOTE: It is ***NEVER*** acceptable to host a CIS Benchmark in ***ANY*** format (PDF, etc.) on a 3rd party (non-CIS owned) site.

Table of Contents

Terms of Use 1

Table of Contents 2

Overview 23

Important Usage Information 23
- Key Stakeholders 23
- Apply the Correct Version of a Benchmark 24
- Exceptions 24
- Remediation 25
- Summary 25

Target Technology Details 26

Intended Audience 26

Consensus Guidance 27

Typographical Conventions 28

Recommendation Definitions 29

Title 29

Assessment Status 29
- Automated 29
- Manual 29

Profile 29

Description 29

Rationale Statement 29

Impact Statement 30

Audit Procedure 30

Remediation Procedure 30

Default Value 30

References 30

CIS Critical Security Controls® (CIS Controls®) 30

Additional Information 30

Profile Definitions 31

Acknowledgements 33

Recommendations 34

1 Account Policies 34
- 1.1 Password Policy 34
  - 1.1.1 Ensure 'Enforce password history' is set to '24 or more password(s)' (Automated) 35
  - 1.1.2 Ensure 'Maximum password age' is set to '365 or fewer days, but not 0' (Automated) 38
  - 1.1.3 Ensure 'Minimum password age' is set to '1 or more day(s)' (Automated) 40

1.1.4 Ensure 'Minimum password length' is set to '14 or more character(s)' (Automated) 43
1.1.5 Ensure 'Password must meet complexity requirements' is set to 'Enabled' (Automated) 46
1.1.6 Ensure 'Relax minimum password length limits' is set to 'Enabled' (Automated) 49
1.1.7 Ensure 'Store passwords using reversible encryption' is set to 'Disabled' (Automated) . 51
1.2 Account Lockout Policy 53
1.2.1 Ensure 'Account lockout duration' is set to '15 or more minute(s)' (Automated) 54
1.2.2 Ensure 'Account lockout threshold' is set to '5 or fewer invalid logon attempt(s), but not 0' (Automated) 56
1.2.3 Ensure 'Allow Administrator account lockout' is set to 'Enabled' (MS only) (Manual) 58
1.2.4 Ensure 'Reset account lockout counter after' is set to '15 or more minute(s)' (Automated) 60

2 Local Policies 62
2.1 Audit Policy 62
2.2 User Rights Assignment 62
2.2.1 Ensure 'Access Credential Manager as a trusted caller' is set to 'No One' (Automated) 63
2.2.2 Ensure 'Access this computer from the network' is set to 'Administrators, Authenticated Users, ENTERPRISE DOMAIN CONTROLLERS' (DC only) (Automated) 65
2.2.3 Ensure 'Access this computer from the network' is set to 'Administrators, Authenticated Users' (MS only) (Automated) 68
2.2.4 Ensure 'Act as part of the operating system' is set to 'No One' (Automated) 70
2.2.5 Ensure 'Add workstations to domain' is set to 'Administrators' (DC only) (Automated) .. 72
2.2.6 Ensure 'Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE' (Automated) 74
2.2.7 Ensure 'Allow log on locally' is set to 'Administrators, ENTERPRISE DOMAIN CONTROLLERS' (DC only) (Automated) 76
2.2.8 Ensure 'Allow log on locally' is set to 'Administrators' (MS only) (Automated) 78
2.2.9 Ensure 'Allow log on through Remote Desktop Services' is set to 'Administrators' (DC only) (Automated) 80
2.2.10 Ensure 'Allow log on through Remote Desktop Services' is set to 'Administrators, Remote Desktop Users' (MS only) (Automated) 82
2.2.11 Ensure 'Back up files and directories' is set to 'Administrators' (Automated) 84
2.2.12 Ensure 'Change the system time' is set to 'Administrators, LOCAL SERVICE' (Automated) 86
2.2.13 Ensure 'Create a pagefile' is set to 'Administrators' (Automated) 89
2.2.14 Ensure 'Create a token object' is set to 'No One' (Automated) 91
2.2.15 Ensure 'Create global objects' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' (Automated) 93
2.2.16 Ensure 'Create permanent shared objects' is set to 'No One' (Automated) 95
2.2.17 Ensure 'Create symbolic links' is set to 'Administrators' (DC only) (Automated) 97
2.2.18 Ensure 'Create symbolic links' is set to 'Administrators, NT VIRTUAL MACHINE\Virtual Machines' (MS only) (Automated) 99
2.2.19 Ensure 'Debug programs' is set to 'Administrators' (Automated) 101
2.2.20 Ensure 'Deny access to this computer from the network' to include 'Guests' (DC only) (Automated) 103
2.2.21 Ensure 'Deny access to this computer from the network' to include 'Guests, Local account and member of Administrators group' (MS only) (Automated) 105
2.2.22 Ensure 'Deny log on as a batch job' to include 'Guests' (Automated) 107
2.2.23 Ensure 'Deny log on as a service' to include 'Guests' (Automated) 109
2.2.24 Ensure 'Deny log on locally' to include 'Guests' (Automated) 111
2.2.25 Ensure 'Deny log on through Remote Desktop Services' to include 'Guests' (DC only) (Automated) 113
2.2.26 Ensure 'Deny log on through Remote Desktop Services' is set to 'Guests, Local account' (MS only) (Automated) 115
2.2.27 Ensure 'Enable computer and user accounts to be trusted for delegation' is set to 'Administrators' (DC only) (Automated) 117

2.2.28 Ensure 'Enable computer and user accounts to be trusted for delegation' is set to 'No One' (MS only) (Automated) 119
2.2.29 Ensure 'Force shutdown from a remote system' is set to 'Administrators' (Automated) 121
2.2.30 Ensure 'Generate security audits' is set to 'LOCAL SERVICE, NETWORK SERVICE' (Automated) 123
2.2.31 Ensure 'Impersonate a client after authentication' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' (DC only) (Automated) 125
2.2.32 Ensure 'Impersonate a client after authentication' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' (MS only) (Automated) 127
2.2.33 Ensure 'Increase scheduling priority' is set to 'Administrators, Window Manager\Window Manager Group' (Automated) 129
2.2.34 Ensure 'Load and unload device drivers' is set to 'Administrators' (Automated) 131
2.2.35 Ensure 'Lock pages in memory' is set to 'No One' (Automated) 133
2.2.36 Ensure 'Log on as a batch job' is set to 'Administrators' (DC Only) (Automated) 135
2.2.37 Ensure 'Manage auditing and security log' is set to 'Administrators' (DC only) (Automated) 137
2.2.38 Ensure 'Manage auditing and security log' is set to 'Administrators' (MS only) (Automated) 139
2.2.39 Ensure 'Modify an object label' is set to 'No One' (Automated) 141
2.2.40 Ensure 'Modify firmware environment values' is set to 'Administrators' (Automated) . 143
2.2.41 Ensure 'Perform volume maintenance tasks' is set to 'Administrators' (Automated) .. 145
2.2.42 Ensure 'Profile single process' is set to 'Administrators' (Automated) 147
2.2.43 Ensure 'Profile system performance' is set to 'Administrators, NT SERVICE\WdiServiceHost' (Automated) 149
2.2.44 Ensure 'Replace a process level token' is set to 'LOCAL SERVICE, NETWORK SERVICE' (Automated) 151
2.2.45 Ensure 'Restore files and directories' is set to 'Administrators' (Automated) 153
2.2.46 Ensure 'Shut down the system' is set to 'Administrators' (Automated) 155
2.2.47 Ensure 'Synchronize directory service data' is set to 'No One' (DC only) (Automated) 157
2.2.48 Ensure 'Take ownership of files or other objects' is set to 'Administrators' (Automated) 159
2.3 Security Options 161
2.3.1 Accounts 161
2.3.1.1 Ensure 'Accounts: Guest account status' is set to 'Disabled' (MS only) (Automated) 162
2.3.1.2 Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled' (Automated) 164
2.3.1.3 Configure 'Accounts: Rename administrator account' (Automated) 166
2.3.1.4 Configure 'Accounts: Rename guest account' (Automated) 168
2.3.2 Audit 170
2.3.2.1 Ensure 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' is set to 'Enabled' (Automated) 171
2.3.2.2 Ensure 'Audit: Shut down system immediately if unable to log security audits' is set to 'Disabled' (Automated) 173
2.3.3 DCOM 174
2.3.4 Devices 175
2.3.4.1 Ensure 'Devices: Prevent users from installing printer drivers' is set to 'Enabled' (Automated) 176
2.3.5 Domain controller 178
2.3.5.1 Ensure 'Domain controller: Allow server operators to schedule tasks' is set to 'Disabled' (DC only) (Automated) 179
2.3.5.2 Ensure 'Domain controller: Allow vulnerable Netlogon secure channel connections' is set to 'Not Configured' (DC Only) (Automated) 181
2.3.5.3 Ensure 'Domain controller: LDAP server channel binding token requirements' is set to 'Always' (DC Only) (Automated) 183

2.3.5.4 Ensure 'Domain controller: LDAP server signing requirements' is set to 'Require signing' (DC only) (Automated) 186
2.3.5.5 Ensure 'Domain controller: Refuse machine account password changes' is set to 'Disabled' (DC only) (Automated) 189
2.3.6 Domain member 191
2.3.6.1 Ensure 'Domain member: Digitally encrypt or sign secure channel data (always)' is set to 'Enabled' (Automated) 192
2.3.6.2 Ensure 'Domain member: Digitally encrypt secure channel data (when possible)' is set to 'Enabled' (Automated) 194
2.3.6.3 Ensure 'Domain member: Digitally sign secure channel data (when possible)' is set to 'Enabled' (Automated) 196
2.3.6.4 Ensure 'Domain member: Disable machine account password changes' is set to 'Disabled' (Automated) 198
2.3.6.5 Ensure 'Domain member: Maximum machine account password age' is set to '30 or fewer days, but not 0' (Automated) 200
2.3.6.6 Ensure 'Domain member: Require strong (Windows 2000 or later) session key' is set to 'Enabled' (Automated) 202
2.3.7 Interactive logon 204
2.3.7.1 Ensure 'Interactive logon: Do not require CTRL+ALT+DEL' is set to 'Disabled' (Automated) 205
2.3.7.2 Ensure 'Interactive logon: Don't display last signed-in' is set to 'Enabled' (Automated) 207
2.3.7.3 Ensure 'Interactive logon: Machine inactivity limit' is set to '900 or fewer second(s), but not 0' (Automated) 209
2.3.7.4 Configure 'Interactive logon: Message text for users attempting to log on' (Automated) 211
2.3.7.5 Configure 'Interactive logon: Message title for users attempting to log on' (Automated) 213
2.3.7.6 Ensure 'Interactive logon: Number of previous logons to cache (in case domain controller is not available)' is set to '4 or fewer logon(s)' (MS only) (Automated) 215
2.3.7.7 Ensure 'Interactive logon: Prompt user to change password before expiration' is set to 'between 5 and 14 days' (Automated) 217
2.3.7.8 Ensure 'Interactive logon: Require Domain Controller Authentication to unlock workstation' is set to 'Enabled' (MS only) (Automated) 219
2.3.7.9 Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or higher (Automated) 221
2.3.8 Microsoft network client 223
2.3.8.1 Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled' (Automated) 224
2.3.8.2 Ensure 'Microsoft network client: Send unencrypted password to third-party SMB servers' is set to 'Disabled' (Automated) 226
2.3.9 Microsoft network server 228
2.3.9.1 Ensure 'Microsoft network server: Amount of idle time required before suspending session' is set to '15 or fewer minute(s)' (Automated) 229
2.3.9.2 Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled' (Automated) 231
2.3.9.3 Ensure 'Microsoft network server: Disconnect clients when logon hours expire' is set to 'Enabled' (Automated) 233
2.3.9.4 Ensure 'Microsoft network server: Server SPN target name validation level' is set to 'Accept if provided by client' or higher (MS only) (Automated) 235
2.3.10 Network access 237
2.3.10.1 Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled' (Automated) 238
2.3.10.2 Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts' is set to 'Enabled' (MS only) (Automated) 240

2.3.10.3 Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled' (MS only) (Automated) 242
2.3.10.4 Ensure 'Network access: Do not allow storage of passwords and credentials for network authentication' is set to 'Enabled' (Automated) 244
2.3.10.5 Ensure 'Network access: Let Everyone permissions apply to anonymous users' is set to 'Disabled' (Automated) 246
2.3.10.6 Ensure 'Network access: Named Pipes that can be accessed anonymously' is configured (DC only) (Automated) 248
2.3.10.7 Ensure 'Network access: Named Pipes that can be accessed anonymously' is configured (MS only) (Automated) 250
2.3.10.8 Ensure 'Network access: Remotely accessible registry paths' is configured (Automated) 252
2.3.10.9 Ensure 'Network access: Remotely accessible registry paths and sub-paths' is configured (Automated) 254
2.3.10.10 Ensure 'Network access: Restrict anonymous access to Named Pipes and Shares' is set to 'Enabled' (Automated) 257
2.3.10.11 Ensure 'Network access: Restrict clients allowed to make remote calls to SAM' is set to 'Administrators: Remote Access: Allow' (MS only) (Automated) 259
2.3.10.12 Ensure 'Network access: Shares that can be accessed anonymously' is set to 'None' (Automated) 261
2.3.10.13 Ensure 'Network access: Sharing and security model for local accounts' is set to 'Classic - local users authenticate as themselves' (Automated) 263
2.3.11 Network security 265
2.3.11.1 Ensure 'Network security: Allow Local System to use computer identity for NTLM' is set to 'Enabled' (Automated) 266
2.3.11.2 Ensure 'Network security: Allow LocalSystem NULL session fallback' is set to 'Disabled' (Automated) 268
2.3.11.3 Ensure 'Network Security: Allow PKU2U authentication requests to this computer to use online identities' is set to 'Disabled' (Automated) 270
2.3.11.4 Ensure 'Network security: Configure encryption types allowed for Kerberos' is set to 'AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types' (Automated) 272
2.3.11.5 Ensure 'Network security: Do not store LAN Manager hash value on next password change' is set to 'Enabled' (Automated) 274
2.3.11.6 Ensure 'Network security: Force logoff when logon hours expire' is set to 'Enabled' (Manual) 276
2.3.11.7 Ensure 'Network security: LAN Manager authentication level' is set to 'Send NTLMv2 response only. Refuse LM & NTLM' (Automated) 278
2.3.11.8 Ensure 'Network security: LDAP client signing requirements' is set to 'Negotiate signing' or higher (Automated) 281
2.3.11.9 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' (Automated) 283
2.3.11.10 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' (Automated) 285
2.3.11.11 Ensure 'Network security: Restrict NTLM: Audit Incoming NTLM Traffic' is set to 'Enable auditing for all accounts' (Automated) 287
2.3.11.12 Ensure 'Network security: Restrict NTLM: Audit NTLM authentication in this domain' is set to 'Enable all' (DC only) (Automated) 289
2.3.11.13 Ensure 'Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers' is set to 'Audit all' or higher (Automated) 291
2.3.12 Recovery console 292
2.3.13 Shutdown 293
2.3.13.1 Ensure 'Shutdown: Allow system to be shut down without having to log on' is set to 'Disabled' (Automated) 294
2.3.14 System cryptography 295

2.3.15 System objects **296**
2.3.15.1 Ensure 'System objects: Require case insensitivity for non-Windows subsystems' is set to 'Enabled' (Automated) 297
2.3.15.2 Ensure 'System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)' is set to 'Enabled' (Automated) 299
2.3.16 System settings **300**
2.3.17 User Account Control **301**
2.3.17.1 Ensure 'User Account Control: Admin Approval Mode for the Built-in Administrator account' is set to 'Enabled' (Automated) 302
2.3.17.2 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 (Automated) 304
2.3.17.3 Ensure 'User Account Control: Behavior of the elevation prompt for standard users' is set to 'Automatically deny elevation requests' (Automated) 306
2.3.17.4 Ensure 'User Account Control: Detect application installations and prompt for elevation' is set to 'Enabled' (Automated) 308
2.3.17.5 Ensure 'User Account Control: Only elevate UIAccess applications that are installed in secure locations' is set to 'Enabled' (Automated) 310
2.3.17.6 Ensure 'User Account Control: Run all administrators in Admin Approval Mode' is set to 'Enabled' (Automated) 312
2.3.17.7 Ensure 'User Account Control: Switch to the secure desktop when prompting for elevation' is set to 'Enabled' (Automated) 314
2.3.17.8 Ensure 'User Account Control: Virtualize file and registry write failures to per-user locations' is set to 'Enabled' (Automated) 316

3 Event Log **318**

4 Restricted Groups **318**

5 System Services **318**
5.1 Ensure 'Print Spooler (Spooler)' is set to 'Disabled' (DC only) (Automated) 319
5.2 Ensure 'Print Spooler (Spooler)' is set to 'Disabled' (MS only) (Automated) 321

6 Registry **323**

7 File System **323**

8 Wired Network (IEEE 802.3) Policies **323**

9 Windows Defender Firewall with Advanced Security (formerly Windows Firewall with Advanced Security) **323**
9.1 Domain Profile **323**
9.1.1 Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)' (Automated) 324
9.1.2 Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)' (Automated) 326
9.1.3 Ensure 'Windows Firewall: Domain: Settings: Display a notification' is set to 'No' (Automated) 328
9.1.4 Ensure 'Windows Firewall: Domain: Logging: Name' is configured (Automated) 330
9.1.5 Ensure 'Windows Firewall: Domain: Logging: Size limit (KB)' is set to '16,384 KB or greater' (Automated) 332
9.1.6 Ensure 'Windows Firewall: Domain: Logging: Log dropped packets' is set to 'Yes' (Automated) 334
9.1.7 Ensure 'Windows Firewall: Domain: Logging: Log successful connections' is set to 'Yes' (Automated) 336
9.2 Private Profile **338**
9.2.1 Ensure 'Windows Firewall: Private: Firewall state' is set to 'On (recommended)' (Automated) 339

9.2.2 Ensure 'Windows Firewall: Private: Inbound connections' is set to 'Block (default)' (Automated) 341
9.2.3 Ensure 'Windows Firewall: Private: Settings: Display a notification' is set to 'No' (Automated) 343
9.2.4 Ensure 'Windows Firewall: Private: Logging: Name' is configured (Automated) 345
9.2.5 Ensure 'Windows Firewall: Private: Logging: Size limit (KB)' is set to '16,384 KB or greater' (Automated) 347
9.2.6 Ensure 'Windows Firewall: Private: Logging: Log dropped packets' is set to 'Yes' (Automated) 349
9.2.7 Ensure 'Windows Firewall: Private: Logging: Log successful connections' is set to 'Yes' (Automated) 351
9.3 Public Profile 353
9.3.1 Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)' (Automated) 354
9.3.2 Ensure 'Windows Firewall: Public: Inbound connections' is set to 'Block (default)' (Automated) 356
9.3.3 Ensure 'Windows Firewall: Public: Settings: Display a notification' is set to 'No' (Automated) 358
9.3.4 Ensure 'Windows Firewall: Public: Settings: Apply local firewall rules' is set to 'No' (Automated) 360
9.3.5 Ensure 'Windows Firewall: Public: Settings: Apply local connection security rules' is set to 'No' (Automated) 362
9.3.6 Ensure 'Windows Firewall: Public: Logging: Name' is configured (Automated) 364
9.3.7 Ensure 'Windows Firewall: Public: Logging: Size limit (KB)' is set to '16,384 KB or greater' (Automated) 366
9.3.8 Ensure 'Windows Firewall: Public: Logging: Log dropped packets' is set to 'Yes' (Automated) 368
9.3.9 Ensure 'Windows Firewall: Public: Logging: Log successful connections' is set to 'Yes' (Automated) 370
10 Network List Manager Policies 372
11 Wireless Network (IEEE 802.11) Policies 372
12 Public Key Policies 372
13 Software Restriction Policies 372
14 Network Access Protection NAP Client Configuration 372
15 Application Control Policies 372
16 IP Security Policies 372
17 Advanced Audit Policy Configuration 373
17.1 Account Logon 373
17.1.1 Ensure 'Audit Credential Validation' is set to 'Success and Failure' (Automated) 374
17.1.2 Ensure 'Audit Kerberos Authentication Service' is set to 'Success and Failure' (DC Only) (Automated) 376
17.1.3 Ensure 'Audit Kerberos Service Ticket Operations' is set to 'Success and Failure' (DC Only) (Automated) 378
17.2 Account Management 380
17.2.1 Ensure 'Audit Application Group Management' is set to 'Success and Failure' (Automated) 381
17.2.2 Ensure 'Audit Computer Account Management' is set to include 'Success' (DC only) (Automated) 383
17.2.3 Ensure 'Audit Distribution Group Management' is set to include 'Success' (DC only) (Automated) 385

17.2.4 Ensure 'Audit Other Account Management Events' is set to include 'Success' (DC only) (Automated) 387
17.2.5 Ensure 'Audit Security Group Management' is set to include 'Success' (Automated) 389
17.2.6 Ensure 'Audit User Account Management' is set to 'Success and Failure' (Automated) 392
17.3 Detailed Tracking 394
17.3.1 Ensure 'Audit PNP Activity' is set to include 'Success' (Automated) 395
17.3.2 Ensure 'Audit Process Creation' is set to include 'Success' (Automated) 397
17.4 DS Access 399
17.4.1 Ensure 'Audit Directory Service Access' is set to include 'Failure' (DC only) (Automated) 400
17.4.2 Ensure 'Audit Directory Service Changes' is set to include 'Success' (DC only) (Automated) 402
17.5 Logon/Logoff 404
17.5.1 Ensure 'Audit Account Lockout' is set to include 'Failure' (Automated) 405
17.5.2 Ensure 'Audit Group Membership' is set to include 'Success' (Automated) 407
17.5.3 Ensure 'Audit Logoff' is set to include 'Success' (Automated) 409
17.5.4 Ensure 'Audit Logon' is set to 'Success and Failure' (Automated) 411
17.5.5 Ensure 'Audit Other Logon/Logoff Events' is set to 'Success and Failure' (Automated) 413
17.5.6 Ensure 'Audit Special Logon' is set to include 'Success' (Automated) 415
17.6 Object Access 417
17.6.1 Ensure 'Audit Detailed File Share' is set to include 'Failure' (Automated) 418
17.6.2 Ensure 'Audit File Share' is set to 'Success and Failure' (Automated) 421
17.6.3 Ensure 'Audit Other Object Access Events' is set to 'Success and Failure' (Automated) 423
17.6.4 Ensure 'Audit Removable Storage' is set to 'Success and Failure' (Automated) 425
17.7 Policy Change 427
17.7.1 Ensure 'Audit Audit Policy Change' is set to include 'Success' (Automated) 428
17.7.2 Ensure 'Audit Authentication Policy Change' is set to include 'Success' (Automated) 430
17.7.3 Ensure 'Audit Authorization Policy Change' is set to include 'Success' (Automated) . 432
17.7.4 Ensure 'Audit MPSSVC Rule-Level Policy Change' is set to 'Success and Failure' (Automated) 434
17.7.5 Ensure 'Audit Other Policy Change Events' is set to include 'Failure' (Automated) 437
17.8 Privilege Use 439
17.8.1 Ensure 'Audit Sensitive Privilege Use' is set to 'Success' (Automated) 440
17.9 System 442
17.9.1 Ensure 'Audit IPsec Driver' is set to 'Success and Failure' (Automated) 443
17.9.2 Ensure 'Audit Other System Events' is set to 'Success and Failure' (Automated) 446
17.9.3 Ensure 'Audit Security State Change' is set to include 'Success' (Automated) 448
17.9.4 Ensure 'Audit Security System Extension' is set to include 'Success' (Automated) 450
17.9.5 Ensure 'Audit System Integrity' is set to 'Success and Failure' (Automated) 452
18 Administrative Templates (Computer) 454
18.1 Control Panel 454
18.1.1 Personalization 454
18.1.1.1 Ensure 'Prevent enabling lock screen camera' is set to 'Enabled' (Automated) 455
18.1.1.2 Ensure 'Prevent enabling lock screen slide show' is set to 'Enabled' (Automated) .. 457
18.1.2 Regional and Language Options 459
18.1.2.1 Handwriting personalization 460
18.1.2.2 Ensure 'Allow users to enable online speech recognition services' is set to 'Disabled' (Automated) 461
18.1.3 Ensure 'Allow Online Tips' is set to 'Disabled' (Automated) 463
18.2 Desktop 465
18.3 LAPS (legacy) 465
18.4 MS Security Guide 465

18.4.1 Ensure 'Apply UAC restrictions to local accounts on network logons' is set to 'Enabled' (MS only) (Automated) 466
18.4.2 Ensure 'Configure SMB v1 client driver' is set to 'Enabled: Disable driver (recommended)' (Automated) 468
18.4.3 Ensure 'Configure SMB v1 server' is set to 'Disabled' (Automated) 471
18.4.4 Ensure 'Enable Certificate Padding' is set to 'Enabled' (Automated) 474
18.4.5 Ensure 'Enable Structured Exception Handling Overwrite Protection (SEHOP)' is set to 'Enabled' (Automated) 476
18.4.6 Ensure 'NetBT NodeType configuration' is set to 'Enabled: P-node (recommended)' (Automated) 478
18.5 MSS (Legacy) 481
18.5.1 Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon' is set to 'Disabled' (Automated) 482
18.5.2 Ensure 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level' is set to 'Enabled: Highest protection, source routing is completely disabled' (Automated) 484
18.5.3 Ensure 'MSS: (DisableIPSourceRouting) IP source routing protection level' is set to 'Enabled: Highest protection, source routing is completely disabled' (Automated) 486
18.5.4 Ensure 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' is set to 'Disabled' (Automated) 488
18.5.5 Ensure 'MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds' is set to 'Enabled: 300,000 or 5 minutes' (Automated) 490
18.5.6 Ensure 'MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers' is set to 'Enabled' (Automated) 492
18.5.7 Ensure 'MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses' is set to 'Disabled' (Automated) 494
18.5.8 Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode' is set to 'Enabled' (Automated) 496
18.5.9 Ensure 'MSS: (TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted' is set to 'Enabled: 3' (Automated) 498
18.5.10 Ensure 'MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted' is set to 'Enabled: 3' (Automated) 500
18.5.11 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' (Automated) 502
18.6 Network 504
18.6.1 Background Intelligent Transfer Service (BITS) 504
18.6.2 BranchCache 504
18.6.3 DirectAccess Client Experience Settings 504
18.6.4 DNS Client 504
18.6.4.1 Ensure 'Configure multicast DNS (mDNS) protocol' is set to 'Disabled' (Automated) 505
18.6.4.2 Ensure 'Configure NetBIOS settings' is set to 'Enabled: Disable NetBIOS name resolution on public networks' (Automated) 507
18.6.4.3 Ensure 'Turn off default IPv6 DNS Servers' is set to 'Enabled' (Automated) 509
18.6.4.4 Ensure 'Turn off multicast name resolution' is set to 'Enabled' (Automated) 511
18.6.5 Fonts 513
18.6.5.1 Ensure 'Enable Font Providers' is set to 'Disabled' (Automated) 514
18.6.6 Hotspot Authentication 516
18.6.7 Lanman Server 517
18.6.7.1 Ensure 'Mandate the minimum version of SMB' is set to 'Enabled: 3.1.1' (Automated) 518
18.6.8 Lanman Workstation 520
18.6.8.1 Ensure 'Enable insecure guest logons' is set to 'Disabled' (Automated) 521
18.6.8.2 Ensure 'Require Encryption' is set to 'Enabled' (Automated) 523
18.6.9 Link-Layer Topology Discovery 525
18.6.9.1 Ensure 'Turn on Mapper I/O (LLTDIO) driver' is set to 'Disabled' (Automated) 526
18.6.9.2 Ensure 'Turn on Responder (RSPNDR) driver' is set to 'Disabled' (Automated) 528

18.6.10 Microsoft Peer-to-Peer Networking Services 529
18.6.10.1 Peer Name Resolution Protocol 530
18.6.10.2 Ensure 'Turn off Microsoft Peer-to-Peer Networking Services' is set to 'Enabled' (Automated) 531
18.6.11 Network Connections 533
18.6.11.1 Windows Defender Firewall (formerly Windows Firewall) 534
18.6.11.2 Ensure 'Prohibit installation and configuration of Network Bridge on your DNS domain network' is set to 'Enabled' (Automated) 535
18.6.11.3 Ensure 'Prohibit use of Internet Connection Sharing on your DNS domain network' is set to 'Enabled' (Automated) 537
18.6.11.4 Ensure 'Require domain users to elevate when setting a network's location' is set to 'Enabled' (Automated) 539
18.6.12 Network Connectivity Status Indicator 541
18.6.13 Network Isolation 541
18.6.14 Network Provider 542
18.6.14.1 Ensure 'Hardened UNC Paths' is set to 'Enabled, with "Require Mutual Authentication", "Require Integrity", and "Require Privacy" set for all NETLOGON and SYSVOL shares' (Automated) 543
18.6.15 Offline Files 546
18.6.16 QoS Packet Scheduler 546
18.6.17 SNMP 546
18.6.18 SSL Configuration Settings 546
18.6.19 TCPIP Settings 546
18.6.19.1 IPv6 Transition Technologies 547
18.6.19.2 Parameters 548
18.6.19.2.1 Disable IPv6 (Ensure TCPIP6 Parameter 'DisabledComponents' is set to '0xff (255)') (Automated) 549
18.6.20 Windows Connect Now 552
18.6.20.1 Ensure 'Configuration of wireless settings using Windows Connect Now' is set to 'Disabled' (Automated) 553
18.6.20.2 Ensure 'Prohibit access of the Windows Connect Now wizards' is set to 'Enabled' (Automated) 555
18.6.21 Windows Connection Manager 557
18.6.21.1 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' (Automated) 558
18.6.21.2 Ensure 'Prohibit connection to non-domain networks when connected to domain authenticated network' is set to 'Enabled' (MS only) (Automated) 560
18.7 Printers 562
18.7.1 Ensure 'Allow Print Spooler to accept client connections' is set to 'Disabled' (Automated) 563
18.7.2 Ensure 'Configure Redirection Guard' is set to 'Enabled: Redirection Guard Enabled' (Automated) 565
18.7.3 Ensure 'Configure RPC connection settings: Protocol to use for outgoing RPC connections' is set to 'Enabled: RPC over TCP' (Automated) 567
18.7.4 Ensure 'Configure RPC connection settings: Use authentication for outgoing RPC connections' is set to 'Enabled: Default' (Automated) 569
18.7.5 Ensure 'Configure RPC listener settings: Protocols to allow for incoming RPC connections' is set to 'Enabled: RPC over TCP' (Automated) 571
18.7.6 Ensure 'Configure RPC listener settings: Authentication protocol to use for incoming RPC connections:' is set to 'Enabled: Negotiate' or higher (Automated) 573
18.7.7 Ensure 'Configure RPC over TCP port' is set to 'Enabled: 0' (Automated) 575
18.7.8 Ensure 'Configure RPC packet level privacy setting for incoming connections' is set to 'Enabled' (Automated) 577
18.7.9 Ensure 'Limits print driver installation to Administrators' is set to 'Enabled' (Automated) 579

18.7.10 Ensure 'Manage processing of Queue-specific files' is set to 'Enabled: Limit Queue-specific files to Color profiles' (Automated) 581
18.7.11 Ensure 'Point and Print Restrictions: When installing drivers for a new connection' is set to 'Enabled: Show warning and elevation prompt' (Automated) 583
18.7.12 Ensure 'Point and Print Restrictions: When updating drivers for an existing connection' is set to 'Enabled: Show warning and elevation prompt' (Automated) 586
18.8 Start Menu and Taskbar 588
18.8.1 Notifications 589
18.8.1.1 Ensure 'Turn off notifications network usage' is set to 'Enabled' (Automated) 590
18.9 System 592
18.9.1 Access-Denied Assistance 592
18.9.2 App-V 592
18.9.3 Audit Process Creation 592
18.9.3.1 Ensure 'Include command line in process creation events' is set to 'Enabled' (Automated) 593
18.9.4 Credentials Delegation 595
18.9.4.1 Ensure 'Encryption Oracle Remediation' is set to 'Enabled: Force Updated Clients' (Automated) 596
18.9.4.2 Ensure 'Remote host allows delegation of non-exportable credentials' is set to 'Enabled' (Automated) 598
18.9.5 Device Guard 600
18.9.5.1 Ensure 'Turn On Virtualization Based Security' is set to 'Enabled' (Automated) 601
18.9.5.2 Ensure 'Turn On Virtualization Based Security: Select Platform Security Level' is set to 'Secure Boot' or higher (Automated) 603
18.9.5.3 Ensure 'Turn On Virtualization Based Security: Virtualization Based Protection of Code Integrity' is set to 'Enabled with UEFI lock' (Automated) 605
18.9.5.4 Ensure 'Turn On Virtualization Based Security: Require UEFI Memory Attributes Table' is set to 'True (checked)' (Automated) 607
18.9.5.5 Ensure 'Turn On Virtualization Based Security: Credential Guard Configuration' is set to 'Enabled with UEFI lock' (MS Only) (Automated) 609
18.9.5.6 Ensure 'Turn On Virtualization Based Security: Credential Guard Configuration' is set to 'Disabled' (DC Only) (Automated) 612
18.9.5.7 Ensure 'Turn On Virtualization Based Security: Secure Launch Configuration' is set to 'Enabled' (Automated) 614
18.9.6 Device Health Attestation Service 616
18.9.7 Device Installation 616
18.9.7.1 Device Installation Restrictions 617
18.9.7.2 Ensure 'Prevent automatic download of applications associated with device metadata' is set to 'Enabled' (Automated) 618
18.9.8 Disk NV Cache 620
18.9.9 Disk Quotas 620
18.9.10 Display 620
18.9.11 Distributed COM 620
18.9.12 Driver Installation 620
18.9.13 Early Launch Antimalware 621
18.9.13.1 Ensure 'Boot-Start Driver Initialization Policy' is set to 'Enabled: Good, unknown and bad but critical' (Automated) 622
18.9.14 Enhanced Storage Access 624
18.9.15 File Classification Infrastructure 624
18.9.16 File Share Shadow Copy Provider 624
18.9.17 Filesystem (formerly NTFS Filesystem) 625
18.9.17.1 Ensure 'Enable / disable CLFS logfile authentication' is set to 'Enabled' (Automated) 626
18.9.18 Folder Redirection 628
18.9.19 Group Policy 628
18.9.19.1 Logging and tracing 629

18.9.19.2 Ensure 'Configure security policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE' (Automated) 630
18.9.19.3 Ensure 'Configure security policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE' (Automated) 632
18.9.19.4 Ensure 'Continue experiences on this device' is set to 'Disabled' (Automated) 634
18.9.19.5 Ensure 'Turn off background refresh of Group Policy' is set to 'Disabled' (Automated) 636
18.9.20 Internet Communication Management 638
18.9.20.1 Internet Communication settings 639
18.9.20.1.1 Ensure 'Turn off downloading of print drivers over HTTP' is set to 'Enabled' (Automated) 640
18.9.20.1.2 Ensure 'Turn off handwriting personalization data sharing' is set to 'Enabled' (Automated) 642
18.9.20.1.3 Ensure 'Turn off handwriting recognition error reporting' is set to 'Enabled' (Automated) 644
18.9.20.1.4 Ensure 'Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com' is set to 'Enabled' (Automated) 646
18.9.20.1.5 Ensure 'Turn off Internet download for Web publishing and online ordering wizards' is set to 'Enabled' (Automated) 648
18.9.20.1.6 Ensure 'Turn off printing over HTTP' is set to 'Enabled' (Automated) 650
18.9.20.1.7 Ensure 'Turn off Registration if URL connection is referring to Microsoft.com' is set to 'Enabled' (Automated) 652
18.9.20.1.8 Ensure 'Turn off Search Companion content file updates' is set to 'Enabled' (Automated) 654
18.9.20.1.9 Ensure 'Turn off the "Order Prints" picture task' is set to 'Enabled' (Automated) 656
18.9.20.1.10 Ensure 'Turn off the "Publish to Web" task for files and folders' is set to 'Enabled' (Automated) 658
18.9.20.1.11 Ensure 'Turn off the Windows Messenger Customer Experience Improvement Program' is set to 'Enabled' (Automated) 660
18.9.20.1.12 Ensure 'Turn off Windows Customer Experience Improvement Program' is set to 'Enabled' (Automated) 662
18.9.20.1.13 Ensure 'Turn off Windows Error Reporting' is set to 'Enabled' (Automated) 664
18.9.21 iSCSI 666
18.9.22 KDC 666
18.9.23 Kerberos 667
18.9.23.1 Ensure 'Support device authentication using certificate' is set to 'Enabled: Automatic' (Automated) 668
18.9.24 Kernel DMA Protection 670
18.9.24.1 Ensure 'Enumeration policy for external devices incompatible with Kernel DMA Protection' is set to 'Enabled: Block All' (Automated) 671
18.9.25 Keyboard Filter 673
18.9.26 LAPS 674
18.9.26.1 Ensure 'Configure password backup directory' is set to 'Enabled: Active Directory' or 'Enabled: Azure Active Directory' (MS only) (Automated) 675
18.9.26.2 Ensure 'Do not allow password expiration time longer than required by policy' is set to 'Enabled' (MS only) (Automated) 677
18.9.26.3 Ensure 'Enable password encryption' is set to 'Enabled' (MS only) (Automated) .. 679
18.9.26.4 Ensure 'Password Settings: Password Complexity' is set to 'Enabled: Large letters + small letters + numbers + specials' (MS only) (Automated) 681
18.9.26.5 Ensure 'Password Settings: Password Length' is set to 'Enabled: 15 or more' (MS only) (Automated) 684
18.9.26.6 Ensure 'Password Settings: Password Age (Days)' is set to 'Enabled: 30 or fewer' (MS only) (Automated) 687
18.9.26.7 Ensure 'Post-authentication actions: Grace period (hours)' is set to 'Enabled: 8 or fewer hours, but not 0' (MS only) (Automated) 689

18.9.26.8 Ensure 'Post-authentication actions: Actions' is set to 'Enabled: Reset the password and logoff the managed account' or higher (MS only) (Automated) 691
18.9.27 Local Security Authority 694
18.9.27.1 Ensure 'Allow Custom SSPs and APs to be loaded into LSASS' is set to 'Disabled' (DC only) (Automated) 695
18.9.27.2 Ensure 'Configures LSASS to run as a protected process' is set to 'Enabled: Enabled with UEFI Lock' (Automated) 697
18.9.28 Locale Services 700
18.9.28.1 Ensure 'Disallow copying of user input methods to the system account for sign-in' is set to 'Enabled' (Automated) 701
18.9.29 Logon 703
18.9.29.1 Ensure 'Block user from showing account details on sign-in' is set to 'Enabled' (Automated) 704
18.9.29.2 Ensure 'Do not display network selection UI' is set to 'Enabled' (Automated) 706
18.9.29.3 Ensure 'Do not enumerate connected users on domain-joined computers' is set to 'Enabled' (Automated) 708
18.9.29.4 Ensure 'Enumerate local users on domain-joined computers' is set to 'Disabled' (MS only) (Automated) 710
18.9.29.5 Ensure 'Turn off app notifications on the lock screen' is set to 'Enabled' (Automated) 712
18.9.29.6 Ensure 'Turn on convenience PIN sign-in' is set to 'Disabled' (Automated) 714
18.9.30 Mitigation Options 716
18.9.31 Net Logon 716
18.9.32 NTLM 716
18.9.33 OS Policies 717
18.9.33.1 Ensure 'Allow Clipboard synchronization across devices' is set to 'Disabled' (Automated) 718
18.9.33.2 Ensure 'Allow upload of User Activities' is set to 'Disabled' (Automated) 720
18.9.34 PIN Complexity 722
18.9.35 Power Management 722
18.9.35.1 Button Settings 722
18.9.35.2 Energy Saver Settings 722
18.9.35.3 Hard Disk Settings 722
18.9.35.4 Notification Settings 722
18.9.35.5 Power Throttling Settings 723
18.9.35.6 Sleep Settings 724
18.9.35.6.1 Ensure 'Allow network connectivity during connected-standby (on battery)' is set to 'Disabled' (Automated) 725
18.9.35.6.2 Ensure 'Allow network connectivity during connected-standby (plugged in)' is set to 'Disabled' (Automated) 727
18.9.35.6.3 Ensure 'Require a password when a computer wakes (on battery)' is set to 'Enabled' (Automated) 729
18.9.35.6.4 Ensure 'Require a password when a computer wakes (plugged in)' is set to 'Enabled' (Automated) 731
18.9.36 Recovery 733
18.9.37 Remote Assistance 734
18.9.37.1 Ensure 'Configure Offer Remote Assistance' is set to 'Disabled' (Automated) 735
18.9.37.2 Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled' (Automated) 737
18.9.38 Remote Procedure Call 739
18.9.38.1 Ensure 'Enable RPC Endpoint Mapper Client Authentication' is set to 'Enabled' (MS only) (Automated) 740
18.9.38.2 Ensure 'Restrict Unauthenticated RPC clients' is set to 'Enabled: Authenticated' (MS only) (Automated) 742
18.9.39 Removable Storage Access 744
18.9.40 Scripts 744
18.9.41 Security Account Manager 745

18.9.41.1 Ensure 'Configure validation of ROCA-vulnerable WHfB keys during authentication' is set to 'Enabled: Block' (DC only) (Automated) 746
18.9.42 Server Manager 749
18.9.43 Service Control Manager Settings 749
18.9.44 Shutdown 749
18.9.45 Shutdown Options 749
18.9.46 Storage Health 749
18.9.47 Storage Sense 750
18.9.48 System Restore 750
18.9.49 Troubleshooting and Diagnostics 750
18.9.49.1 Application Compatibility Diagnostics 750
18.9.49.2 Corrupted File Recovery 750
18.9.49.3 Disk Diagnostic 751
18.9.49.4 Fault Tolerant Heap 751
18.9.49.5 Microsoft Support Diagnostic Tool 752
18.9.49.5.1 Ensure 'Microsoft Support Diagnostic Tool: Turn on MSDT interactive communication with support provider' is set to 'Disabled' (Automated) 753
18.9.49.6 MSI Corrupted File Recovery 755
18.9.49.7 Scheduled Maintenance 755
18.9.49.8 Scripted Diagnostics 755
18.9.49.9 Windows Boot Performance Diagnostics 755
18.9.49.10 Windows Memory Leak Diagnosis 755
18.9.49.11 Windows Performance PerfTrack 756
18.9.49.11.1 Ensure 'Enable/Disable PerfTrack' is set to 'Disabled' (Automated) 757
18.9.50 Trusted Platform Module Services 759
18.9.51 User Profiles 760
18.9.51.1 Ensure 'Turn off the advertising ID' is set to 'Enabled' (Automated) 761
18.9.52 Windows File Protection 763
18.9.53 Windows Time Service 763
18.9.53.1 Time Providers 764
18.9.53.1.1 Ensure 'Enable Windows NTP Client' is set to 'Enabled' (Automated) 765
18.9.53.1.2 Ensure 'Enable Windows NTP Server' is set to 'Disabled' (MS only) (Automated) 767
18.10 Windows Components 769
18.10.1 ActiveX Installer Service 769
18.10.2 Add features to Windows 10 (formerly Windows Anytime Upgrade) 769
18.10.3 App and Device Inventory 769
18.10.4 App Package Deployment 769
18.10.4.1 Ensure 'Allow a Windows app to share application data between users' is set to 'Disabled' (Automated) 770
18.10.5 App Privacy 772
18.10.6 App runtime 772
18.10.6.1 Ensure 'Allow Microsoft accounts to be optional' is set to 'Enabled' (Automated) 773
18.10.7 Application Compatibility 775
18.10.8 AutoPlay Policies 775
18.10.8.1 Ensure 'Disallow Autoplay for non-volume devices' is set to 'Enabled' (Automated) 776
18.10.8.2 Ensure 'Set the default behavior for AutoRun' is set to 'Enabled: Do not execute any autorun commands' (Automated) 778
18.10.8.3 Ensure 'Turn off Autoplay' is set to 'Enabled: All drives' (Automated) 780
18.10.9 Biometrics 782
18.10.9.1 Facial Features 782
18.10.9.1.1 Ensure 'Configure enhanced anti-spoofing' is set to 'Enabled' (Automated) 783
18.10.10 BitLocker Drive Encryption 785
18.10.11 Camera 785
18.10.11.1 Ensure 'Allow Use of Camera' is set to 'Disabled' (Automated) 786

18.10.12 Chat 788
18.10.13 Cloud Content 788
18.10.13.1 Ensure 'Turn off cloud consumer account state content' is set to 'Enabled' (Automated) 789
18.10.13.2 Ensure 'Turn off cloud optimized content' is set to 'Enabled' (Automated) 791
18.10.14 Connect 793
18.10.14.1 Ensure 'Require pin for pairing' is set to 'Enabled: First Time' OR 'Enabled: Always' (Automated) 794
18.10.15 Credential User Interface 796
18.10.15.1 Ensure 'Do not display the password reveal button' is set to 'Enabled' (Automated) 797
18.10.15.2 Ensure 'Enumerate administrator accounts on elevation' is set to 'Disabled' (Automated) 799
18.10.16 Data Collection and Preview Builds 801
18.10.16.1 Ensure 'Allow Diagnostic Data' is set to 'Enabled: Diagnostic data off (not recommended)' or 'Enabled: Send required diagnostic data' (Automated) 802
18.10.16.2 Ensure 'Configure Authenticated Proxy usage for the Connected User Experience and Telemetry service' is set to 'Enabled: Disable Authenticated Proxy usage' (Automated) 805
18.10.16.3 Ensure 'Do not show feedback notifications' is set to 'Enabled' (Automated) 807
18.10.16.4 Ensure 'Enable OneSettings Auditing' is set to 'Enabled' (Automated) 809
18.10.16.5 Ensure 'Limit Diagnostic Log Collection' is set to 'Enabled' (Automated) 811
18.10.16.6 Ensure 'Limit Dump Collection' is set to 'Enabled' (Automated) 813
18.10.17 Delivery Optimization 815
18.10.18 Desktop App Installer 815
18.10.18.1 Ensure 'Enable App Installer' is set to 'Disabled' (Automated) 816
18.10.18.2 Ensure 'Enable App Installer Experimental Features' is set to 'Disabled' (Automated) 818
18.10.18.3 Ensure 'Enable App Installer Hash Override' is set to 'Disabled' (Automated) 820
18.10.18.4 Ensure 'Enable App Installer Local Archive Malware Scan Override' is set to 'Disabled' (Automated) 822
18.10.18.5 Ensure 'Enable App Installer Microsoft Store Source Certificate Validation Bypass' is set to 'Disabled' (Automated) 824
18.10.18.6 Ensure 'Enable App Installer ms-appinstaller protocol' is set to 'Disabled' (Automated) 826
18.10.18.7 Ensure 'Enable Windows Package Manager command line interfaces' is set to 'Disabled' (Automated) 828
18.10.19 Desktop Gadgets 830
18.10.20 Desktop Window Manager 830
18.10.21 Device and Driver Compatibility 830
18.10.22 Device Registration (formerly Workplace Join) 830
18.10.23 Digital Locker 830
18.10.24 Edge UI 831
18.10.25 Event Forwarding 831
18.10.26 Event Log Service 831
18.10.26.1 Application 831
18.10.26.1.1 Ensure 'Application: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Automated) 832
18.10.26.1.2 Ensure 'Application: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (Automated) 834
18.10.26.2 Security 836
18.10.26.2.1 Ensure 'Security: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Automated) 837
18.10.26.2.2 Ensure 'Security: Specify the maximum log file size (KB)' is set to 'Enabled: 196,608 or greater' (Automated) 839
18.10.26.3 Setup 841

18.10.26.3.1 Ensure 'Setup: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Automated) 842
18.10.26.3.2 Ensure 'Setup: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (Automated) 844
18.10.26.4 System 846
18.10.26.4.1 Ensure 'System: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Automated) 847
18.10.26.4.2 Ensure 'System: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (Automated) 849
18.10.27 Event Logging 851
18.10.28 Event Viewer 851
18.10.29 File Explorer (formerly Windows Explorer) 851
18.10.29.1 Previous Versions 851
18.10.29.2 Ensure 'Do not apply the Mark of the Web tag to files copied from insecure sources' is set to 'Disabled' (Automated) 852
18.10.29.3 Ensure 'Turn off Data Execution Prevention for Explorer' is set to 'Disabled' (Automated) 854
18.10.29.4 Ensure 'Turn off heap termination on corruption' is set to 'Disabled' (Automated) 856
18.10.29.5 Ensure 'Turn off shell protocol protected mode' is set to 'Disabled' (Automated) 858
18.10.30 File History 860
18.10.31 Find My Device 860
18.10.32 Handwriting 860
18.10.33 HomeGroup 860
18.10.34 Human Presence 860
18.10.35 Internet Explorer 861
18.10.36 Location and Sensors 861
18.10.36.1 Ensure 'Turn off location' is set to 'Enabled' (Automated) 862
18.10.37 Maintenance Scheduler 864
18.10.38 Maps 864
18.10.39 MDM 864
18.10.40 Messaging 864
18.10.40.1 Ensure 'Allow Message Service Cloud Sync' is set to 'Disabled' (Automated) 865
18.10.41 Microsoft account 867
18.10.41.1 Ensure 'Block all consumer Microsoft account user authentication' is set to 'Enabled' (Automated) 868
18.10.42 Microsoft Defender Antivirus (formerly Windows Defender and Windows Defender Antivirus) 870
18.10.43 Microsoft Defender Application Guard (formerly Windows Defender Application Guard) 870
18.10.44 Microsoft Defender Exploit Guard (formerly Windows Defender Exploit Guard) 870
18.10.45 Microsoft Edge 871
18.10.46 Microsoft Secondary Authentication Factor 871
18.10.47 Microsoft User Experience Virtualization 871
18.10.48 NetMeeting 871
18.10.49 News and interests 871
18.10.50 OneDrive (formerly SkyDrive) 872
18.10.51 Online Assistance 872
18.10.52 OOBE 872
18.10.53 Paint 872
18.10.54 Portable Operating System 872
18.10.55 Presentation Settings 873
18.10.56 Push To Install 873
18.10.56.1 Ensure 'Turn off Push To Install service' is set to 'Enabled' (Automated) 874
18.10.57 Remote Desktop Services (formerly Terminal Services) 876
18.10.57.1 RD Licensing (formerly TS Licensing) 876

18.10.57.2 Remote Desktop Connection Client 876
18.10.57.2.1 RemoteFX USB Device Redirection 876
18.10.57.2.2 Ensure 'Do not allow passwords to be saved' is set to 'Enabled' (Automated) . 877
18.10.57.3 Remote Desktop Session Host (formerly Terminal Server) 879
18.10.57.3.1 Application Compatibility 879
18.10.57.3.2 Connections 879
18.10.57.3.2.1 Ensure 'Restrict Remote Desktop Services users to a single Remote Desktop Services session' is set to 'Enabled' (Automated) 880
18.10.57.3.3 Device and Resource Redirection 882
18.10.57.3.3.1 Ensure 'Allow UI Automation redirection' is set to 'Disabled' (Automated) 883
18.10.57.3.3.2 Ensure 'Do not allow COM port redirection' is set to 'Enabled' (Automated) . 885
18.10.57.3.3.3 Ensure 'Do not allow drive redirection' is set to 'Enabled' (Automated) 887
18.10.57.3.3.4 Ensure 'Do not allow location redirection' is set to 'Enabled' (Automated) 889
18.10.57.3.3.5 Ensure 'Do not allow LPT port redirection' is set to 'Enabled' (Automated) ... 891
18.10.57.3.3.6 Ensure 'Do not allow supported Plug and Play device redirection' is set to 'Enabled' (Automated) 893
18.10.57.3.3.7 Ensure 'Do not allow WebAuthn redirection' is set to 'Enabled' (Automated) 895
18.10.57.3.4 Licensing 897
18.10.57.3.5 Printer Redirection 897
18.10.57.3.6 Profiles 897
18.10.57.3.7 RD Connection Broker (formerly TS Connection Broker) 897
18.10.57.3.8 Remote Session Environment 897
18.10.57.3.9 Security 898
18.10.57.3.9.1 Ensure 'Always prompt for password upon connection' is set to 'Enabled' (Automated) 899
18.10.57.3.9.2 Ensure 'Require secure RPC communication' is set to 'Enabled' (Automated) 901
18.10.57.3.9.3 Ensure 'Require use of specific security layer for remote (RDP) connections' is set to 'Enabled: SSL' (Automated) 903
18.10.57.3.9.4 Ensure 'Require user authentication for remote connections by using Network Level Authentication' is set to 'Enabled' (Automated) 905
18.10.57.3.9.5 Ensure 'Set client connection encryption level' is set to 'Enabled: High Level' (Automated) 907
18.10.57.3.10 Session Time Limits 909
18.10.57.3.10.1 Ensure 'Set time limit for active but idle Remote Desktop Services sessions' is set to 'Enabled: 15 minutes or less, but not Never (0)' (Automated) 910
18.10.57.3.11 Temporary folders 912
18.10.57.3.11.1 Ensure 'Do not delete temp folders upon exit' is set to 'Disabled' (Automated) 913
18.10.57.3.11.2 Ensure 'Do not use temporary folders per session' is set to 'Disabled' (Automated) 915
18.10.58 RSS Feeds 917
18.10.58.1 Ensure 'Prevent downloading of enclosures' is set to 'Enabled' (Automated) 918
18.10.58.2 Ensure 'Turn on Basic feed authentication over HTTP' is set to 'Disabled' (Automated) 920
18.10.59 Search 922
18.10.59.1 OCR 922
18.10.59.2 Ensure 'Allow Cloud Search' is set to 'Enabled: Disable Cloud Search' (Automated) 923
18.10.59.3 Ensure 'Allow indexing of encrypted files' is set to 'Disabled' (Automated) 925
18.10.59.4 Ensure 'Allow search highlights' is set to 'Disabled' (Automated) 927
18.10.60 Security Center 929
18.10.61 Shutdown Options 929
18.10.62 Smart Card 929
18.10.63 Software Protection Platform 929

18.10.63.1 Ensure 'Turn off KMS Client Online AVS Validation' is set to 'Enabled' (Automated) 930
18.10.64 Sound Recorder 932
18.10.65 Speech 932
18.10.66 Store 932
18.10.67 Sync your settings 932
18.10.68 Tablet PC 932
18.10.69 Task Scheduler 933
18.10.70 Tenant Restrictions 933
18.10.71 Text Input 933
18.10.72 Widgets 933
18.10.73 Windows AI 933
18.10.74 Windows Calendar 934
18.10.75 Windows Color System 934
18.10.76 Windows Customer Experience Improvement Program 934
18.10.77 Windows Defender SmartScreen 935
18.10.77.1 Enhanced Phishing Protection 935
18.10.77.2 Explorer 935
18.10.77.2.1 Ensure 'Configure Windows Defender SmartScreen' is set to 'Enabled: Warn and prevent bypass' (Automated) 936
18.10.78 Windows Error Reporting 938
18.10.79 Windows Game Recording and Broadcasting 938
18.10.80 Windows Hello for Business (formerly Microsoft Passport for Work) 938
18.10.81 Windows Ink Workspace 938
18.10.81.1 Ensure 'Allow suggested apps in Windows Ink Workspace' is set to 'Disabled' (Automated) 939
18.10.81.2 Ensure 'Allow Windows Ink Workspace' is set to 'Enabled: On, but disallow access above lock' OR 'Enabled: Disabled' (Automated) 941
18.10.82 Windows Installer 943
18.10.82.1 Ensure 'Allow user control over installs' is set to 'Disabled' (Automated) 944
18.10.82.2 Ensure 'Always install with elevated privileges' is set to 'Disabled' (Automated) 946
18.10.82.3 Ensure 'Prevent Internet Explorer security prompt for Windows Installer scripts' is set to 'Disabled' (Automated) 948
18.10.83 Windows Logon Options 950
18.10.83.1 Ensure 'Configure the transmission of the user's password in the content of MPR notifications sent by winlogon.' is set to 'Disabled' (Automated) 951
18.10.83.2 Ensure 'Sign-in and lock last interactive user automatically after a restart' is set to 'Disabled' (Automated) 953
18.10.84 Windows Media Digital Rights Management 955
18.10.85 Windows Media Player 955
18.10.86 Windows Messenger 955
18.10.87 Windows Mobility Center 955
18.10.88 Windows PowerShell 955
18.10.88.1 Ensure 'Turn on PowerShell Script Block Logging' is set to 'Enabled' (Automated) 956
18.10.88.2 Ensure 'Turn on PowerShell Transcription' is set to 'Enabled' (Automated) 958
18.10.89 Windows Reliability Analysis 960
18.10.90 Windows Remote Management (WinRM) 960
18.10.90.1 WinRM Client 960
18.10.90.1.1 Ensure 'Allow Basic authentication' is set to 'Disabled' (Automated) 961
18.10.90.1.2 Ensure 'Allow unencrypted traffic' is set to 'Disabled' (Automated) 963
18.10.90.1.3 Ensure 'Disallow Digest authentication' is set to 'Enabled' (Automated) 965
18.10.90.2 WinRM Service 967
18.10.90.2.1 Ensure 'Allow Basic authentication' is set to 'Disabled' (Automated) 968
18.10.90.2.2 Ensure 'Allow remote server management through WinRM' is set to 'Disabled' (Automated) 970

18.10.90.2.3 Ensure 'Allow unencrypted traffic' is set to 'Disabled' (Automated) 972
18.10.90.2.4 Ensure 'Disallow WinRM from storing RunAs credentials' is set to 'Enabled' (Automated) 974
18.10.91 Windows Remote Shell 976
18.10.91.1 Ensure 'Allow Remote Shell Access' is set to 'Disabled' (Automated) 977
18.10.92 Windows Sandbox 979
18.10.93 Windows Security (formerly Windows Defender Security Center) 979
18.10.93.1 Account protection 979
18.10.93.2 App and browser protection 979
18.10.93.2.1 Ensure 'Prevent users from modifying settings' is set to 'Enabled' (Automated) 980
18.10.94 Windows Update 982
18.10.94.1 Legacy Policies 982
18.10.94.1.1 Ensure 'No auto-restart with logged on users for scheduled automatic updates installations' is set to 'Disabled' (Automated) 983
18.10.94.2 Manage end user experience 985
18.10.94.2.1 Ensure 'Configure Automatic Updates' is set to 'Enabled' (Automated) 986
18.10.94.2.2 Ensure 'Configure Automatic Updates: Scheduled install day' is set to '0 - Every day' (Automated) 989
18.10.94.3 Manage updates offered from Windows Server Update Service 991
18.10.94.4 Manage updates offered from Windows Update (formerly Defer Windows Updates and Windows Update for Business) 991
18.10.94.4.1 Ensure 'Manage preview builds' is set to 'Disabled' (Automated) 992
18.10.94.4.2 Ensure 'Select when Quality Updates are received' is set to 'Enabled: 0 days' (Automated) 994
18.11 Custom Settings 997
18.11.1 Ensure 'Disable HTTP proxy features: Disable WPAD' is set to 'Enabled: Checked' (Automated) 998
18.11.2 Ensure 'Disable HTTP proxy features: Disable proxy authentication' is set to 'Enabled: Disable authentication over loopback interfaces' or higher (Automated) 1000

19 Administrative Templates (User) 1002
19.1 Control Panel 1004
19.2 Desktop 1004
19.3 Network 1004
19.4 Shared Folders 1004
19.5 Start Menu and Taskbar 1005
19.5.1 Notifications 1005
19.5.1.1 Ensure 'Turn off toast notifications on the lock screen' is set to 'Enabled' (Automated) 1006
19.6 System 1008
19.6.1 Ctrl+Alt+Del Options 1008
19.6.2 Display 1008
19.6.3 Driver Installation 1008
19.6.4 Folder Redirection 1008
19.6.5 Group Policy 1009
19.6.6 Internet Communication Management 1009
19.6.6.1 Internet Communication settings 1009
19.6.6.1.1 Ensure 'Turn off Help Experience Improvement Program' is set to 'Enabled' (Automated) 1010
19.6.7 Keyboard Filter 1012
19.7 Windows Components 1012
19.7.1 Account Notifications 1012
19.7.2 Add features to Windows 8 / 8.1 / 10 (formerly Windows Anytime Upgrade) 1012
19.7.3 App runtime 1012
19.7.4 Application Compatibility 1013

19.7.5 Attachment Manager **1013**
19.7.5.1 Ensure 'Do not preserve zone information in file attachments' is set to 'Disabled' (Automated) 1014
19.7.5.2 Ensure 'Notify antivirus programs when opening attachments' is set to 'Enabled' (Automated) 1016
19.7.6 AutoPlay Policies **1018**
19.7.7 Calculator **1018**
19.7.8 Cloud Content **1018**
19.7.8.1 Ensure 'Configure Windows spotlight on lock screen' is set to 'Disabled' (Automated) 1019
19.7.8.2 Ensure 'Do not suggest third-party content in Windows spotlight' is set to 'Enabled' (Automated) 1021
19.7.8.3 Ensure 'Do not use diagnostic data for tailored experiences' is set to 'Enabled' (Automated) 1023
19.7.8.4 Ensure 'Turn off all Windows spotlight features' is set to 'Enabled' (Automated) 1025
19.7.8.5 Ensure 'Turn off Spotlight collection on Desktop' is set to 'Enabled' (Automated) 1027
19.7.9 Credential User Interface **1029**
19.7.10 Data Collection and Preview Builds **1029**
19.7.11 Desktop Gadgets **1029**
19.7.12 Desktop Window Manager **1029**
19.7.13 Digital Locker **1029**
19.7.14 Edge UI **1030**
19.7.15 File Explorer (formerly Windows Explorer) **1030**
19.7.16 File Revocation **1030**
19.7.17 IME **1030**
19.7.18 Instant Search **1030**
19.7.19 Internet Explorer **1031**
19.7.20 Location and Sensors **1031**
19.7.21 Microsoft Edge **1031**
19.7.22 Microsoft Management Console **1031**
19.7.23 Microsoft User Experience Virtualization **1031**
19.7.24 Multitasking **1032**
19.7.25 NetMeeting **1032**
19.7.26 Network Sharing **1032**
19.7.26.1 Ensure 'Prevent users from sharing files within their profile.' is set to 'Enabled' (Automated) 1033
19.7.27 OOBE **1035**
19.7.28 Presentation Settings **1035**
19.7.29 Remote Desktop Services (formerly Terminal Services) **1035**
19.7.30 RSS Feeds **1035**
19.7.31 Search **1035**
19.7.32 Snipping Tool **1036**
19.7.33 Sound Recorder **1036**
19.7.34 Store **1036**
19.7.35 Tablet PC **1036**
19.7.36 Task Scheduler **1036**
19.7.37 Windows AI **1037**
19.7.38 Windows Calendar **1037**
19.7.39 Windows Color System **1037**
19.7.40 Windows Copilot **1037**
19.7.41 Windows Defender SmartScreen **1037**
19.7.42 Windows Error Reporting **1038**
19.7.43 Windows Hello for Business (formerly Microsoft Passport for Work) **1038**
19.7.44 Windows Installer **1038**
19.7.45 Windows Logon Options **1038**
19.7.46 Windows Media Player **1038**

19.7.46.1 Networking 1039
19.7.46.2 Playback 1039
19.7.46.2.1 Ensure 'Prevent Codec Download' is set to 'Enabled' (Automated) 1040
Appendix: Summary Table 1042
Appendix: Change History 1092

Overview

All CIS Benchmarks™ (Benchmarks) focus on technical configuration settings used to maintain and/or increase the security of the addressed technology, and they should be used in **conjunction** with other essential cyber hygiene tasks like:

- Monitoring the base operating system and applications for vulnerabilities and quickly updating with the latest security patches.
- End-point protection (Antivirus software, Endpoint Detection and Response (EDR), etc.).
- Logging and monitoring user and system activity.

In the end, the Benchmarks are designed to be a key **component** of a comprehensive cybersecurity program.

Important Usage Information

All Benchmarks are available free for non-commercial use from the CIS Website. They can be used to manually assess and remediate systems and applications. In lieu of manual assessment and remediation, there are several tools available to assist with assessment:

- CIS Configuration Assessment Tool (CIS-CAT® Pro Assessor)
- CIS Benchmarks™ Certified 3rd Party Tooling

These tools make the hardening process much more scalable for large numbers of systems and applications.

NOTE: Some tooling focuses only on the Benchmark Recommendations that can be fully automated (skipping ones marked **Manual**). It is important that ***ALL*** Recommendations (**Automated** and **Manual**) be addressed since all are important for properly securing systems and are typically in scope for audits.

Key Stakeholders

Cybersecurity is a collaborative effort, and cross functional cooperation is imperative within an organization to discuss, test, and deploy Benchmarks in an effective and efficient way. The Benchmarks are developed to be best practice configuration guidelines applicable to a wide range of use cases. In some organizations, exceptions to specific Recommendations will be needed, and this team should work to prioritize the problematic Recommendations based on several factors like risk, time, cost, and labor. These exceptions should be properly categorized and documented for auditing purposes.

Apply the Correct Version of a Benchmark

Benchmarks are developed and tested for a specific set of products and versions and applying an incorrect Benchmark to a system can cause the resulting pass/fail score to be incorrect. This is due to the assessment of settings that do not apply to the target systems. To assure the correct Benchmark is being assessed:

- **Deploy the Benchmark applicable to the way settings are managed in the environment:** An example of this is the Microsoft Windows family of Benchmarks, which have separate Benchmarks for Group Policy, Intune, and Stand-alone systems based upon how system management is deployed. Applying the wrong Benchmark in this case will give invalid results.

- **Use the most recent version of a Benchmark**: This is true for all Benchmarks, but especially true for cloud technologies. Cloud technologies change frequently and using an older version of a Benchmark may have invalid methods for auditing and remediation.

Exceptions

The guidance items in the Benchmarks are called recommendations and not requirements, and exceptions to some of them are expected and acceptable. The Benchmarks strive to be a secure baseline, or starting point, for a specific technology, with known issues identified during Benchmark development are documented in the Impact section of each Recommendation. In addition, organizational, system specific requirements, or local site policy may require changes as well, or an exception to a Recommendation or group of Recommendations (e.g. A Benchmark could Recommend that a Web server not be installed on the system, but if a system's primary purpose is to function as a Webserver, there should be a documented exception to this Recommendation for that specific server).

In the end, exceptions to some Benchmark Recommendations are common and acceptable, and should be handled as follows:

- The reasons for the exception should be reviewed cross-functionally and be well documented for audit purposes.
- A plan should be developed for mitigating, or eliminating, the exception in the future, if applicable.
- If the organization decides to accept the risk of this exception (not work toward mitigation or elimination), this should be documented for audit purposes.

It is the responsibility of the organization to determine their overall security policy, and which settings are applicable to their unique needs based on the overall risk profile for the organization.

Remediation

CIS has developed Build Kits for many technologies to assist in the automation of hardening systems. Build Kits are designed to correspond to Benchmark's "Remediation" section, which provides the manual remediation steps necessary to make that Recommendation compliant to the Benchmark.

When remediating systems (changing configuration settings on deployed systems as per the Benchmark's Recommendations), please approach this with caution and test thoroughly.

The following is a reasonable remediation approach to follow:

- CIS Build Kits, or internally developed remediation methods should never be applied to production systems without proper testing.
- Proper testing consists of the following:
  - Understand the configuration (including installed applications) of the targeted systems. Various parts of the organization may need different configurations (e.g., software developers vs standard office workers).
  - Read the Impact section of the given Recommendation to help determine if there might be an issue with the targeted systems.
  - Test the configuration changes with representative lab system(s). If issues arise during testing, they can be resolved prior to deploying to any production systems.
  - When testing is complete, initially deploy to a small sub-set of production systems and monitor closely for issues. If there are issues, they can be resolved prior to deploying more broadly.
  - When the initial deployment above is completed successfully, iteratively deploy to additional systems and monitor closely for issues. Repeat this process until the full deployment is complete.

Summary

Using the Benchmarks Certified tools, working as a team with key stakeholders, being selective with exceptions, and being careful with remediation deployment, it is possible to harden large numbers of deployed systems in a cost effective, efficient, and safe manner.

NOTE: As previously stated, the PDF versions of the CIS Benchmarks™ are available for free, non-commercial use on the CIS Website. All other formats of the CIS Benchmarks™ (MS Word, Excel, and Build Kits) are available for CIS SecureSuite® members.

CIS-CAT® Pro is also available to CIS SecureSuite® members.

Target Technology Details

This document provides prescriptive guidance for establishing a secure configuration posture for **Microsoft Windows Operating Systems** (OS).

This secure configuration guide is based on **Server 2022** and was tested against **Microsoft Windows Server 2022 Datacenter** edition.

Ensure that the latest version of this benchmark is downloaded, as it contains new and updated group policy objects (GPO) released by Microsoft. To be certain that all new and updated GPOs are installed on the system, please download the latest version of the `ADMX/ADML` templates for **Microsoft Windows 11**. The newest version of the templates can be downloaded from Microsoft here: Download Administrative Templates (.admx) for Windows 11 2025 Update (25H2) from Official Microsoft Download Center.

Please note that all versions of the Windows OS Benchmarks, including Server, need the newest Windows 11 `ADMX/ADML` templates, as these templates contain all required GPOs for Benchmark compliance.

To obtain the latest version of this secure configuration guide, please visit the CIS Website or visit the CIS WorkBench Community. If you have questions, comments, or have identified ways to improve this guide, please write to us at benchmarkinfo@cisecurity.org.

Intended Audience

The Microsoft Windows Benchmarks are written for **Active Directory domain-joined** systems using **Active Directory's Group Policy Manager** only. This benchmark is not intended for use on standalone or workgroup systems, systems joined to a cloud offering, such as Entra ID, or systems created, maintained, or used in the Cloud. This benchmark covers supported endpoint states for **Active Directory** and **Entra Hybrid joined** systems that receive policies from **Active Directory Group Policy Manager** only.

Consensus Guidance

This CIS Benchmark™ was created using a consensus review process comprised of a global community of subject matter experts. The process combines real world experience with data-based information to create technology specific guidance to assist users to secure their environments. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS Benchmark undergoes two phases of consensus review. The first phase occurs during initial Benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the Benchmark. This discussion occurs until consensus has been reached on Benchmark recommendations. The second phase begins after the Benchmark has been published. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the Benchmark. If you are interested in participating in the consensus process, please visit https://workbench.cisecurity.org/.

Typographical Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
`Stylized Monospace font`	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
`Monospace font`	Used for inline code, commands, UI/Menu selections or examples. Text should be interpreted exactly as presented.
`<Monospace font in brackets>`	Text set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to reference other relevant settings, CIS Benchmarks and/or Benchmark Communities. Also, used to denote the title of a book, article, or other publication.
Bold font	Additional information or caveats things like **Notes**, **Warnings**, or **Cautions** (usually just the word itself and the rest of the text normal).

Recommendation Definitions

The following defines the various components included in a CIS recommendation as applicable. If any of the components are not applicable it will be noted, or the component will not be included in the recommendation.

Title

Concise description for the recommendation's intended configuration.

Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

Profile

A collection of recommendations for securing a technology or a supporting platform. Most benchmarks include at least a Level 1 and Level 2 Profile. Level 2 extends Level 1 recommendations and is not a standalone profile. The Profile Definitions section in the benchmark provides the definitions as they pertain to the recommendations included for the technology.

Description

Detailed information pertaining to the setting with which the recommendation is concerned. In some cases, the description will include the recommended value.

Rationale Statement

Detailed reasoning for the recommendation to provide the user a clear and concise understanding on the importance of the recommendation.

Impact Statement

Any security, functionality, or operational consequences that can result from following the recommendation.

Audit Procedure

Systematic instructions for determining if the target system complies with the recommendation.

Remediation Procedure

Systematic instructions for applying recommendations to the target system to bring it into compliance according to the recommendation.

Default Value

Default value for the given setting in this recommendation, if known. If not known, either not configured or not defined will be applied.

References

Additional documentation relative to the recommendation.

CIS Critical Security Controls® (CIS Controls®)

The mapping between a recommendation and the CIS Controls is organized by CIS Controls version, Safeguard, and Implementation Group (IG). The Benchmark in its entirety addresses the CIS Controls safeguards of (v7) “5.1 - Establish Secure Configurations” and (v8) '4.1 - Establish and Maintain a Secure Configuration Process” so individual recommendations will not be mapped to these safeguards.

Additional Information

Supplementary information that does not correspond to any other field but may be useful to the user.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1 - Domain Controller**

  Items in this profile apply to Domain Controllers and intend to:

  - be practical and prudent;
  - provide a clear security benefit; and
  - not inhibit the utility of the technology beyond acceptable means.

- **Level 1 - Member Server**

  Items in this profile apply to Member Servers and intend to:

  - be practical and prudent;
  - provide a clear security benefit; and
  - not inhibit the utility of the technology beyond acceptable means.

  Items in this profile also apply to Member Servers that have the following Roles enabled:

  - AD Certificate Services
  - DHCP Server
  - DNS Server
  - File Server
  - Hyper-V
  - Network Policy and Access Services
  - Print Server
  - Remote Access Services
  - Remote Desktop Services
  - Web Server

- **Level 2 - Domain Controller**

  This profile extends the "Level 1 - Domain Controller" profile. Items in this profile exhibit one or more of the following characteristics:

  - are intended for environments or use cases where security is paramount
  - acts as defense in depth measure
  - may negatively inhibit the utility or performance of the technology

- **Level 2 - Member Server**

  This profile extends the "Level 1 - Member Server" profile. Items in this profile exhibit one or more of the following characteristics:

  - are intended for environments or use cases where security is paramount
  - acts as defense in depth measure
  - may negatively inhibit the utility or performance of the technology

- **Next Generation Windows Security - Domain Controller**

  This profile contains advanced Windows security features that have specific configuration dependencies, and may not be compatible with all systems. It therefore requires special attention to detail and testing before implementation. If your environment supports these features, they are highly recommended as they have tangible security benefits. This profile is intended to be an optional "add-on" to the Level 1 or Level 2 profiles.

- **Next Generation Windows Security - Member Server**

  This profile contains advanced Windows security features that have specific configuration dependencies, and may not be compatible with all systems. It therefore requires special attention to detail and testing before implementation. If your environment supports these features, they are highly recommended as they have tangible security benefits. This profile is intended to be an optional "add-on" to the Level 1 or Level 2 profiles.

Acknowledgements

This Benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

The Center for Internet Security extends special recognition and thanks to Rick Munck from Microsoft, as well as Mike Harris from General Dynamics Information Technology for their collaboration developing the configuration recommendations contained in this document.

Editor

Haemish Edgerton

Jennifer Jarose

Contributor

Caleb Eifert

Aaron Margosis

Hardeep Mehrotara

Phil White

Matthew Woods

Justin Young

Kevin Zhang

Recommendations

1 Account Policies

This section contains recommendations for account policies.

1.1 Password Policy

This section contains recommendations for password policy.

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines the number of renewed, unique passwords that have to be associated with a user account before you can reuse an old password. The value for this policy setting must be between 0 and 24 passwords. The default value for stand-alone systems is 0 passwords, but the default setting when joined to a domain is 24 passwords. To maintain the effectiveness of this policy setting, use the Minimum password age setting to prevent users from repeatedly changing their password.

The recommended state for this setting is: `24 or more password(s)`.

Note: Password Policy settings (section 1.1) and Account Lockout Policy settings (section 1.2) must be applied via the **Default Domain Policy** GPO in order to be globally in effect on **domain** user accounts as their default behavior. If these settings are configured in another GPO, they will only affect **local** user accounts on the computers that receive the GPO. However, custom exceptions to the default password policy and account lockout policy rules for specific domain users and/or groups can be defined using Password Settings Objects (PSOs), which are completely separate from Group Policy and most easily configured using Active Directory Administrative Center.

Note #2: As of the publication of this benchmark, Microsoft currently has a maximum limit of 24 saved passwords. For more information, please visit Enforce password history (Windows 10) - Windows security | Microsoft Docs

Rationale:

The longer a password is reused, the greater the chance that a threat actor can determine the password through brute force attacks. Also, accounts that may have been compromised will remain exploitable if the password is left unchanged. If password changes are required but password reuse is not prevented, or if a continually small number of passwords are reused, the effectiveness of a good password policy is greatly reduced.

If a low number for this policy setting is specified, users will be able to use the same small number of passwords repeatedly.

Note: If the Minimum password age setting is not configured, users might repeatedly change their passwords until they can reuse their original password.

Impact:

The major impact of this configuration is that users must create a new password every time they are required to change their old one. If users are required to change their passwords to new unique values, there is an increased risk of users who write their passwords somewhere so that they do not forget them. Another risk is that users may create passwords that change incrementally (for example, password01, password02, and so on) to facilitate memorization but make them easier to guess. Also, an excessively low value for the Minimum password age setting will likely increase administrative overhead, because users who forget their passwords might ask the help desk to reset them frequently.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `24 or more password(s)`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Enforce password history
```

Default Value:

On domain members: 24 passwords remembered

On stand-alone servers: 0 passwords remembered

References:

1. https://www.cisecurity.org/white-papers/cis-password-policy-guide/
2. GRID: MS-00000001

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	16.2 Configure Centralized Point of Authentication Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.		●	●

1.1.2 Ensure 'Maximum password age' is set to '365 or fewer days, but not 0' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting defines how long a user can use their password before it expires.

Values for this policy setting range from 0 to 999 days. If you set the value to 0, the password will never expire.

Because threat actors can crack passwords, the more frequently you change the password the less opportunity an threat actor has to use a cracked password. However, the lower this value is set, the higher the potential for an increase in calls to help desk support due to users having to change their password or forgetting which password is current.

The recommended state for this setting is `365 or fewer days, but not 0`.

Note: Password Policy settings (section 1.1) and Account Lockout Policy settings (section 1.2) must be applied via the **Default Domain Policy** GPO in order to be globally in effect on **domain** user accounts as their default behavior. If these settings are configured in another GPO, they will only affect **local** user accounts on the computers that receive the GPO. However, custom exceptions to the default password policy and account lockout policy rules for specific domain users and/or groups can be defined using Password Settings Objects (PSOs), which are completely separate from Group Policy and most easily configured using Active Directory Administrative Center.

Rationale:

The longer a password exists the higher the likelihood that it will be compromised by a brute force attack, a threat actor gaining general knowledge about the user, or by the user sharing the password. Configuring the Maximum password age setting to 0 so that users are never required to change their passwords is a major security risk because that allows a compromised password to be used by the threat actor for as long as the valid user has authorized access.

Because threat actors can crack passwords, the more frequently the password is changed, the less opportunity a threat actor has to use a cracked password. However, the lower this value is set, the higher the potential for an increase in calls to help desk support due to users having to change their password or forgetting which password is current.

Impact:

If the Maximum password age setting is too low, users are required to change their passwords often. Such a configuration can reduce security in the organization because users might write their passwords in an insecure location or lose them. If the value for this policy setting is too high, the level of security within an organization is reduced because it allows threat actors more time in which to discover user passwords or to use compromised accounts.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `365 or fewer days, but not 0`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Maximum password age
```

Default Value:

42 days.

References:

1. https://www.cisecurity.org/white-papers/cis-password-policy-guide/
2. GRID: MS-00000002

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	16.10 Ensure All Accounts Have An Expiration Date Ensure that all accounts have an expiration date that is monitored and enforced.		●	●

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines the number of days that you must use a password before you can change it. The range of values for this policy setting is between 1 and 999 days. (You may also set the value to 0 to allow immediate password changes.) The default value for this setting is 0 days.

The recommended state for this setting is: `1 or more day(s)`.

Note: Password Policy settings (section 1.1) and Account Lockout Policy settings (section 1.2) must be applied via the **Default Domain Policy** GPO in order to be globally in effect on **domain** user accounts as their default behavior. If these settings are configured in another GPO, they will only affect **local** user accounts on the computers that receive the GPO. However, custom exceptions to the default password policy and account lockout policy rules for specific domain users and/or groups can be defined using Password Settings Objects (PSOs), which are completely separate from Group Policy and most easily configured using Active Directory Administrative Center.

Rationale:

Users may have favorite passwords that they like to use because they are easy to remember Unfortunately, passwords are compromised and if a threat actor is targeting a specific individual's user account, with foreknowledge of data about that user, reuse of old passwords can cause a security breach. To address password reuse, a combination of security settings is required.

Using this policy setting with the Enforce password history setting prevents the easy reuse of old passwords. For example, if you configure the Enforce password history setting to ensure that users cannot reuse any of their last 12 passwords, they could change their password 13 times in a few minutes and reuse the password they started with, unless you also configure the Minimum password age setting to a number that is greater than 0. You must configure this policy setting to a number that is greater than 0 for the Enforce password history setting to be effective.

Impact:

If an administrator sets a password for a user but wants that user to change the password when the user first logs on, the administrator must select the User must change password at next logon check box, or the user will not be able to change the password until the next day.

In environments where access is limited to Remote Desktop Services, users cannot change their password prior to logging in. They must be assigned a temporary password, and once it is set by the administrator, the user will not be able to change it until the following day.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `1 or more day(s)`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Minimum password age
```

Default Value:

On domain members: 1 day.

On stand-alone servers: 0 days.

References:

1. https://www.cisecurity.org/white-papers/cis-password-policy-guide/
2. GRID: MS-00000003

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	16.10 Ensure All Accounts Have An Expiration Date Ensure that all accounts have an expiration date that is monitored and enforced.		●	●

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines the least number of characters that make up a password for a user account.

The recommended state for this setting is: `14 or more character(s)`.

Note: In Windows Server 2016 and older versions of Windows Server, the GUI of the Local Security Policy (LSP), Local Group Policy Editor (LGPE) and Group Policy Management Editor (GPME) would not let you set this value higher than 14 characters. However, starting with Windows Server 2019, Microsoft changed the GUI to allow up to a 20 character minimum password length.

Note #2: Password Policy settings (section 1.1) and Account Lockout Policy settings (section 1.2) must be applied via the **Default Domain Policy** GPO in order to be globally in effect on **domain** user accounts as their default behavior. If these settings are configured in another GPO, they will only affect **local** user accounts on the computers that receive the GPO. However, custom exceptions to the default password policy and account lockout policy rules for specific domain users and/or groups can be defined using Password Settings Objects (PSOs), which are completely separate from Group Policy and most easily configured using Active Directory Administrative Center.

Rationale:

Types of password attacks include dictionary attacks (which attempt to use common words and phrases) and brute force attacks (which try every possible combination of characters). Also, threat actors sometimes try to obtain the account database so they can use tools to discover the accounts and passwords.

Impact:

Requirements for extremely long passwords can decrease the security of an organization, because users might leave the information in an insecure location or lose it. If very long passwords are required, mistyped passwords could cause account lockouts and increase the volume of help desk calls. If your organization has issues with forgotten passwords due to password length requirements, consider teaching your users about passphrases, which are often easier to remember and, due to the larger number of character combinations, much harder to discover.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `14 or more character(s)`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Minimum password length
```

Default Value:

On domain members: 7 characters

On stand-alone servers: 0 characters

References:

1. https://www.cisecurity.org/white-papers/cis-password-policy-guide/
2. GRID: MS-00000004

Additional Information:

There are many different theories about how to determine the best password length for an organization, but perhaps "passphrase" is a better term than "password." In Microsoft Windows 2000 or newer, passphrases can be quite long and can include spaces. Therefore, a phrase such as "I want to drink a $5 milkshake" is a valid passphrase; it is a considerably stronger password than an 8- or 10-character string of random numbers and letters and yet is easier to remember. Users must be educated about the proper selection and maintenance of passwords, especially around password length. In enterprise environments, the ideal value for the Minimum password length setting is 14 characters, however you should adjust this value to meet your organization's business requirements.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

1.1.5 Ensure 'Password must meet complexity requirements' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting checks all new passwords to ensure that they meet basic requirements for strong passwords.

When this policy is enabled, passwords must meet the following minimum requirements:

- Not contain the user's account name or parts of the user's full name that exceed two consecutive characters
- Be at least six characters in length
- Contain characters from three of the following categories:
- English uppercase characters (A through Z)
- English lowercase characters (a through z)
- Base 10 digits (0 through 9)
- Non-alphabetic characters (for example, !, $, #, %)
- A catch-all category of any Unicode character that does not fall under the previous four categories. This fifth category can be regionally specific.

Each additional character in a password increases its complexity exponentially. For instance, a seven-character, all lower-case alphabetic password would have 26 to the power of 7 (approximately 8 x 10 to the power of 9 or 8 billion) possible combinations. At 1,000,000 attempts per second (a capability of many password-cracking utilities), it would only take 133 minutes to crack. A seven-character alphabetic password with case sensitivity has 52 to the power of 7 combinations. A seven-character case-sensitive alphanumeric password without punctuation has 62 to the power of 7 combinations. An eight-character password has 26 to the power of 8 (or 2 x 1011) possible combinations. Although this might seem to be a large number, at 1,000,000 attempts per second it would take only 59 hours to try all possible passwords. Remember, these times will significantly increase for passwords that use ALT characters and other special keyboard characters such as "!" or "@". Proper use of the password settings can help make it difficult to mount a brute force attack.

The recommended state for this setting is: `Enabled`.

Note: Password Policy settings (section 1.1) and Account Lockout Policy settings (section 1.2) must be applied via the **Default Domain Policy** GPO in order to be globally in effect on **domain** user accounts as their default behavior. If these settings are configured in another GPO, they will only affect **local** user accounts on the computers that receive the GPO. However, custom exceptions to the default password policy and account lockout policy rules for specific domain users and/or groups can be defined using Password Settings Objects (PSOs), which are completely separate from Group Policy and most easily configured using Active Directory Administrative Center.

Rationale:

Passwords that contain only alphanumeric characters are extremely easy to discover with several publicly available tools.

Impact:

If the default password complexity configuration is retained, additional help desk calls for locked-out accounts could occur because users might not be accustomed to passwords that contain non-alphabetic characters. However, all users should be able to comply with the complexity requirement with minimal difficulty.

If your organization has more stringent security requirements, you can create a custom version of the Passfilt.dll file that allows the use of arbitrarily complex password strength rules. For example, a custom password filter might require the use of non-upper row characters. (Upper row characters are those that require you to hold down the SHIFT key and press any of the digits between 1 and 0.) A custom password filter might also perform a dictionary check to verify that the proposed password does not contain common dictionary words or fragments.

Also, the use of ALT key character combinations can greatly enhance the complexity of a password. However, such stringent password requirements can result in unhappy users and an extremely busy help desk. Alternatively, your organization could consider a requirement for all administrator passwords to use ALT characters in the 0128 - 0159 range. (ALT characters outside of this range can represent standard alphanumeric characters that would not add additional complexity to the password.)

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Password must meet complexity requirements
```

Default Value:

On domain members: Enabled

On stand-alone servers: Disabled

References:

1. https://www.cisecurity.org/white-papers/cis-password-policy-guide/
2. GRID: MS-00000005

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

1.1.6 Ensure 'Relax minimum password length limits' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Member Server

Description:

This policy setting determines whether the minimum password length setting can be increased beyond the legacy limit of 14 characters. For more information please see the following Microsoft Security Blog.

The recommended state for this setting is: `Enabled`.

Note: This setting only affects *local* accounts on the computer. Domain accounts are only affected by settings on the Domain Controllers, because that is where domain accounts are stored.

Rationale:

This setting will enable the enforcement of longer and generally stronger passwords or passphrases where MFA is not in use.

Impact:

The *Minimum password length* setting may be configured higher than 14 characters.

If very long passwords are required, mistyped passwords could cause account lockouts and increase the volume of help desk calls. If your organization has issues with forgotten passwords due to password length requirements, consider teaching your users about passphrases, which are often easier to remember and, due to the larger number of character combinations, much harder to discover.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\System\CurrentControlSet\Control\SAM:RelaxMinimumPasswordLengthLimits
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Relax minimum password length limits
```

Note: This setting is only available within the built-in OS security template of Windows 10 version 2004 and Server 2022 (or newer), and is not available via older versions of the OS, or via downloadable Administrative Templates (ADMX/ADML). Therefore, you *must* use a Windows 10 version 2004 or Server 2022 system (or newer) to view or edit this setting with the Group Policy Management Console (GPMC) or Group Policy Management Editor (GPME).

Default Value:

Disabled. (The *Minimum password length* may be configured to a maximum of 14 characters.)

References:

1. https://www.cisecurity.org/white-papers/cis-password-policy-guide/
2. https://support.microsoft.com/en-us/topic/minimum-password-length-auditing-and-enforcement-on-certain-versions-of-windows-5ef7fecf-3325-f56b-cc10-4fd565aacc59
3. GRID: MS-00000006

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

1.1.7 Ensure 'Store passwords using reversible encryption' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether the operating system stores passwords in a way that uses reversible encryption, which provides support for application protocols that require knowledge of the user's password for authentication purposes. Passwords that are stored with reversible encryption are essentially the same as plaintext versions of the passwords.

The recommended state for this setting is: `Disabled`.

Note: Password Policy settings (section 1.1) and Account Lockout Policy settings (section 1.2) must be applied via the **Default Domain Policy** GPO in order to be globally in effect on **domain** user accounts as their default behavior. If these settings are configured in another GPO, they will only affect **local** user accounts on the computers that receive the GPO. However, custom exceptions to the default password policy and account lockout policy rules for specific domain users and/or groups can be defined using Password Settings Objects (PSOs), which are completely separate from Group Policy and most easily configured using Active Directory Administrative Center.

Rationale:

Enabling this policy setting allows the operating system to store passwords in a weaker format that is much more susceptible to compromise and weakens your system security.

Impact:

If your organization uses either the CHAP authentication protocol through remote access or IAS services or Digest Authentication in IIS, you must configure this policy setting to Enabled. This setting is extremely dangerous to apply through Group Policy on a user-by-user basis, because it requires the appropriate user account object to be opened in Active Directory Users and Computers.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Store passwords using reversible encryption
```

Default Value:

Disabled.

References:

1. https://www.cisecurity.org/white-papers/cis-password-policy-guide/
2. GRID: MS-00000007

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 Encrypt Sensitive Data at Rest Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		●	●
v7	16.4 Encrypt or Hash all Authentication Credentials Encrypt or hash with a salt all authentication credentials when stored.		●	●

1.2 Account Lockout Policy

This section contains recommendations for account lockout policy.

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines the length of time that must pass before a locked account is unlocked and a user can try to log on again. The setting does this by specifying the number of minutes a locked-out account will remain unavailable. If the value for this policy setting is configured to 0, locked out accounts will remain locked out until an administrator manually unlocks them.

Although it might seem like a good idea to configure the value for this policy setting to a high value, such a configuration will likely increase the number of calls that the help desk receives to unlock accounts locked by mistake. Users should be aware of the length of time a lock remains in place, so that they realize they only need to call the help desk if they have an extremely urgent need to regain access to their computer.

The recommended state for this setting is: `15 or more minute(s)`.

Note: Password Policy settings (section 1.1) and Account Lockout Policy settings (section 1.2) must be applied via the **Default Domain Policy** GPO in order to be globally in effect on **domain** user accounts as their default behavior. If these settings are configured in another GPO, they will only affect **local** user accounts on the computers that receive the GPO. However, custom exceptions to the default password policy and account lockout policy rules for specific domain users and/or groups can be defined using Password Settings Objects (PSOs), which are completely separate from Group Policy and most easily configured using Active Directory Administrative Center.

Rationale:

A denial-of-service (DoS) condition can be created if a threat actor abuses the Account lockout threshold and repeatedly attempts to log on with a specific account. Once the Account lockout threshold setting is configured, the account will be locked out after the specified number of failed attempts. If Account lockout duration is set to 0, then the account will remain locked out until an administrator unlocks it manually.

Impact:

Although it may seem like a good idea to configure this policy setting to never automatically unlock an account, such a configuration can increase the number of requests that your organization's help desk receives to unlock accounts that were locked by mistake.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `15 or more minute(s)`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Account lockout duration
```

Default Value:

None, because this policy setting only has meaning when an Account lockout threshold is specified. When an Account lockout threshold is configured, Windows automatically suggests a value of 30 minutes.

References:

1. https://www.cisecurity.org/white-papers/cis-password-policy-guide/
2. GRID: MS-00000008

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.10 Enforce Automatic Device Lockout on Portable End-User Devices Enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices, where supported. For laptops, do not allow more than 20 failed authentication attempts; for tablets and smartphones, no more than 10 failed authentication attempts. Example implementations include Microsoft® InTune Device Lock and Apple® Configuration Profile maxFailedAttempts.		●	●
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines the number of failed logon attempts before the account is locked.

The recommended state for this setting is: `5 or fewer invalid logon attempt(s), but not 0`.

Note: A value of `0` does not conform to the benchmark as it disables account lockout threshold.

Note #2: Password Policy settings (section 1.1) and Account Lockout Policy settings (section 1.2) must be applied via the **Default Domain Policy** GPO in order to be globally in effect on **domain** user accounts as their default behavior. If these settings are configured in another GPO, they will only affect **local** user accounts on the computers that receive the GPO. However, custom exceptions to the default password policy and account lockout policy rules for specific domain users and/or groups can be defined using Password Settings Objects (PSOs), which are completely separate from Group Policy and most easily configured using Active Directory Administrative Center.

Rationale:

Setting an account lockout threshold reduces the likelihood that an online password brute force attack will be successful. Setting the account lockout threshold too low introduces risk of increased accidental lockouts and/or a threat actor intentionally locking out accounts.

Impact:

If this policy setting is enabled, a locked-out account will not be usable until it is reset by an administrator or until the account lockout duration expires. This setting may generate additional help desk calls.

If you enforce this setting a threat actor could cause a denial-of-service condition by deliberately generating failed logons for multiple users, therefore you should also configure the Account Lockout Duration to a relatively low value.

If the Account Lockout Threshold is set to 0, there is a possibility that a threat actor's attempt to discover passwords with a brute force password attack might go undetected if a robust audit mechanism is not in place.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `5 or fewer invalid login attempt(s), but not 0`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Account lockout threshold
```

Default Value:

0 failed logon attempts.

References:

1. https://www.cisecurity.org/white-papers/cis-password-policy-guide/
2. GRID: MS-00000009

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.10 Enforce Automatic Device Lockout on Portable End-User Devices Enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices, where supported. For laptops, do not allow more than 20 failed authentication attempts; for tablets and smartphones, no more than 10 failed authentication attempts. Example implementations include Microsoft® InTune Device Lock and Apple® Configuration Profile maxFailedAttempts.		●	●
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

1.2.3 Ensure 'Allow Administrator account lockout' is set to 'Enabled' (MS only) (Manual)

Profile Applicability:

- Level 1 - Member Server

Description:

This policy setting determines whether the built-in Administrator account is subject to the following Account Lockout Policy settings: *Account lockout duration*, *Account lockout threshold*, and *Reset account lockout counter*. By default, this account is excluded from the account lockout controls and will never be locked out with repeated bad password attempts.

The recommended state for this setting is: `Enabled`.

Note: This setting applies only to OSes patched as of October 11, 2022 (see MS KB5020282).

Rationale:

Enabling account lockout policies for the built-in Administrator account will reduce the likelihood of a successful brute force attack.

Impact:

The built-in Administrator account will be subject to the policies in Section *1.2 Account Lockout Policy* of this benchmark.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policies\Allow Administrator account lockout
```

Default Value:

Disabled. (The built-in Administrator account is not subject to the account lockout policy.)

References:

1. https://support.microsoft.com/en-us/topic/kb5020282-account-lockout-available-for-built-in-local-administrators-bce45c4d-f28d-43ad-b6fe-70156cb2dc00
2. GRID: MS-00000010

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.10 Enforce Automatic Device Lockout on Portable End-User Devices Enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices, where supported. For laptops, do not allow more than 20 failed authentication attempts; for tablets and smartphones, no more than 10 failed authentication attempts. Example implementations include Microsoft® InTune Device Lock and Apple® Configuration Profile maxFailedAttempts.		●	●
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●
v7	16.12 Monitor Attempts to Access Deactivated Accounts Monitor attempts to access deactivated accounts through audit logging.		●	●

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines the length of time before the Account lockout threshold resets to zero. The default value for this policy setting is Not Defined. If the Account lockout threshold is defined, this reset time must be less than or equal to the value for the Account lockout duration setting.

The recommended state for this setting is: `15 or more minute(s)`.

Note: Password Policy settings (section 1.1) and Account Lockout Policy settings (section 1.2) must be applied via the **Default Domain Policy** GPO in order to be globally in effect on **domain** user accounts as their default behavior. If these settings are configured in another GPO, they will only affect **local** user accounts on the computers that receive the GPO. However, custom exceptions to the default password policy and account lockout policy rules for specific domain users and/or groups can be defined using Password Settings Objects (PSOs), which are completely separate from Group Policy and most easily configured using Active Directory Administrative Center.

Rationale:

If the account lockout policy is left at its default setting or configured with an excessively long interval, the environment may be vulnerable to denial-of-service (DoS) attacks. A threat actor could repeatedly attempt to login across multiple accounts, triggering lockouts and disrupting access.

Without a defined lockout threshold, administrators would need to manually reset affected accounts. However, by setting a reasonable lockout duration, accounts will automatically unlock after a specified period, reducing administrative overhead and maintaining security.

Impact:

Users can accidentally lock themselves out of their accounts if they mistype their password multiple times.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `15 or more minute(s)`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Reset account lockout counter after
```

Default Value:

None, because this policy setting only has meaning when an Account lockout threshold is specified. When an Account lockout threshold is configured, Windows automatically suggests a value of 30 minutes.

References:

1. https://www.cisecurity.org/white-papers/cis-password-policy-guide/
2. GRID: MS-00000011

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.10 Enforce Automatic Device Lockout on Portable End-User Devices Enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices, where supported. For laptops, do not allow more than 20 failed authentication attempts; for tablets and smartphones, no more than 10 failed authentication attempts. Example implementations include Microsoft® InTune Device Lock and Apple® Configuration Profile maxFailedAttempts.		●	●
v7	16.5 Encrypt Transmittal of Username and Authentication Credentials Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.		●	●

2 Local Policies

This section contains recommendations for local policies.

2.1 Audit Policy

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

2.2 User Rights Assignment

This section contains recommendations for user rights assignments.

2.2.1 Ensure 'Access Credential Manager as a trusted caller' is set to 'No One' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This security setting is used by Credential Manager during Backup and Restore. No accounts should have this user right, as it is only assigned to Winlogon. Users' saved credentials might be compromised if this user right is assigned to other entities.

The recommended state for this setting is: `No One`.

Rationale:

If an account is given this right the user of the account may create an application that calls into Credential Manager and is returned the credentials for another user.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `No One`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Access Credential Manager as a trusted caller
```

Default Value:

No one.

References:

1. GRID: MS-00000012

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
v7	4.8 Log and Alert on Changes to Administrative Group Membership Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.		●	●

2.2.2 Ensure 'Access this computer from the network' is set to 'Administrators, Authenticated Users, ENTERPRISE DOMAIN CONTROLLERS' (DC only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This policy setting allows other users on the network to connect to the computer and is required by various network protocols that include Server Message Block (SMB)-based protocols, NetBIOS, Common Internet File System (CIFS), and Component Object Model Plus (COM+).

The recommended state for this setting *on Domain Controllers* is: `Administrators, Authenticated Users, ENTERPRISE DOMAIN CONTROLLERS`.

Note: Certain policy settings must be configured in the **Default Domain Controller Policy** to ensure they are applied globally to domain controllers. Exercise caution when modifying these policies, as improper changes can negatively impact the environment.

Only policies that are configured by Microsoft by default should reside in these baseline GPOs. Any additional or custom policy settings should be implemented through separate GPOs rather than modifying the default policies.

Rationale:

Users who can connect from their computer to the network can access resources on target computers for which they have permission. For example, the *Access this computer from the network* user right is required for users to connect to shared printers and folders. If this user right is assigned to the `Everyone` group, then anyone will be able to read the files in those shared folders. However, this situation is unlikely for new installations of Windows Server 2003 with Service Pack 1 (SP1), because the default share and NTFS permissions in Windows Server 2003 do not include the `Everyone` group. This vulnerability may have a higher level of risk for computers that you upgrade from Windows NT 4.0 or Windows 2000, because the default permissions for these operating systems are not as restrictive as the default permissions in Windows Server 2003.

Impact:

If you remove the *Access this computer from the network* user right on Domain Controllers for all users, no one will be able to log on to the domain or use network resources. If you remove this user right on Member Servers, users will not be able to connect to those servers through the network. Successful negotiation of IPsec connections requires that the initiating machine has this right, therefore if using IPsec, it is recommended that it is assigned to the `Authenticated Users` group. If you have installed optional components such as ASP.NET or Internet Information Services (IIS), you may need to assign this user right to additional accounts that are required by those components. It is important to verify that authorized users are assigned this user right for the computers they need to access the network.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, configure the following UI path to `Administrators, Authenticated Users, ENTERPRISE DOMAIN CONTROLLERS`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Access this computer from the network
```

Default Value:

Administrators, Authenticated Users, Enterprise Domain Controllers, Everyone, Pre-Windows 2000 Compatible Access.

References:

1. GRID: MS-00000013

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running		●	●

Controls Version	Control	IG 1	IG 2	IG 3
	Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

2.2.3 Ensure 'Access this computer from the network' is set to 'Administrators, Authenticated Users' (MS only) (Automated)

Profile Applicability:

- Level 1 - Member Server

Description:

This policy setting allows other users on the network to connect to the computer and is required by various network protocols that include Server Message Block (SMB)-based protocols, NetBIOS, Common Internet File System (CIFS), and Component Object Model Plus (COM+).

The recommended state for this setting *on Member Servers* is: `Administrators, Authenticated Users`.

Rationale:

Users who can connect from their computer to the network can access resources on target computers for which they have permission. For example, the *Access this computer from the network* user right is required for users to connect to shared printers and folders. If this user right is assigned to the `Everyone` group, then anyone will be able to read the files in those shared folders. However, this situation is unlikely for new installations of Windows Server 2003 with Service Pack 1 (SP1), because the default share and NTFS permissions in Windows Server 2003 do not include the `Everyone` group. This vulnerability may have a higher level of risk for computers that you upgrade from Windows NT 4.0 or Windows 2000, because the default permissions for these operating systems are not as restrictive as the default permissions in Windows Server 2003.

Impact:

If you remove the *Access this computer from the network* user right on Domain Controllers for all users, no one will be able to log on to the domain or use network resources. If you remove this user right on Member Servers, users will not be able to connect to those servers through the network. Successful negotiation of IPsec connections requires that the initiating machine has this right, therefore if using IPsec, it is recommended that it is assigned to the `Authenticated Users` group. If you have installed optional components such as ASP.NET or Internet Information Services (IIS), you may need to assign this user right to additional accounts that are required by those components. It is important to verify that authorized users are assigned this user right for the computers they need to access the network.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, configure the following UI path to `Administrators, Authenticated Users`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Access this computer from the network
```

Default Value:

Administrators, Backup Operators, Everyone, Users.

References:

1. GRID: MS-00000013

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

2.2.4 Ensure 'Act as part of the operating system' is set to 'No One' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows a process to assume the identity of any user and thus gain access to the resources that the user is authorized to access.

The recommended state for this setting is: `No One`.

Note: This user right is considered a "sensitive privilege" for the purposes of auditing.

Rationale:

The **Act as part of the operating system** user right is extremely powerful. Anyone with this user right can take complete control of the computer and erase evidence of their activities.

Impact:

There should be little or no impact because the **Act as part of the operating system** user right is rarely needed by any accounts other than the `Local System` account, which implicitly has this right.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `No One`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Act as part of the operating system
```

Default Value:

No one.

References:

1. GRID: MS-00000014

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●

2.2.5 Ensure 'Add workstations to domain' is set to 'Administrators' (DC only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This policy setting specifies which users can add computer workstations to the domain. For this policy setting to take effect, it must be assigned to the user as part of the **Default Domain Controller Policy** for the domain. A user who has been assigned this right can add up to 10 workstations to the domain. Users who have been assigned the *Create Computer Objects* permission for an OU or the Computers container in Active Directory can add an unlimited number of computers to the domain, regardless of whether or not they have been assigned the **Add workstations to domain** user right.

In Windows-based networks, the term security principal is defined as a user, group, or computer that is automatically assigned a security identifier to control access to resources. In an Active Directory domain, each computer account is a full security principal with the ability to authenticate and access domain resources. However, some organizations may want to limit the number of computers in an Active Directory environment so that they can consistently track, build, and manage the computers. If users are allowed to add computers to the domain, tracking and management efforts would be hampered. Also, users could perform activities that are more difficult to trace because of their ability to create additional unauthorized domain computers.

The recommended state for this setting is: `Administrators`.

Note: Certain policy settings must be configured in the **Default Domain Controller Policy** to ensure they are applied globally to domain controllers. Exercise caution when modifying these policies, as improper changes can negatively impact the environment.

Only policies that are configured by Microsoft by default should reside in these baseline GPOs. Any additional or custom policy settings should be implemented through separate GPOs rather than modifying the default policies.

Rationale:

The **Add workstations to domain** user right presents a moderate vulnerability. Users with this right could add a computer to the domain that is configured in a way that violates organizational security policies. For example, if your organization does not want its users to have administrative privileges on their computers, a user could (re-)install Windows on his or her computer and then add the computer to the domain. The user would know the password for the local Administrator account, and could log on with that account and then add his or her domain account to the local Administrators group.

Impact:

For organizations that have never allowed users to set up their own computers and add them to the domain, this countermeasure will have no impact. For those that have allowed some or all users to configure their own computers, this countermeasure will force the organization to establish a formal process for these procedures going forward. It will not affect existing domain computers unless they are removed from and re-added to the domain.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Administrators`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Add workstations to domain
```

Default Value:

Authenticated Users. (All domain users have the ability to add up to 10 computer accounts to an Active Directory domain. These new computer accounts are created in the Computers container.)

References:

1. GRID: MS-00000015

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
v7	4.3 Ensure the Use of Dedicated Administrative Accounts Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	●	●	●

2.2.6 Ensure 'Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows a user to adjust the maximum amount of memory that is available to a process. The ability to adjust memory quotas is useful for system tuning, but it can be abused. In the wrong hands, it could be used to launch a denial-of-service (DoS) attack.

The recommended state for this setting is: `Administrators, LOCAL SERVICE, NETWORK SERVICE`.

Note: Certain policy settings must be configured in the **Default Domain Controller Policy** to ensure they are applied globally to domain controllers. Exercise caution when modifying these policies, as improper changes can negatively impact the environment.

Only policies that are configured by Microsoft by default should reside in these baseline GPOs. Any additional or custom policy settings should be implemented through separate GPOs rather than modifying the default policies.

Note #2: A Member Server that holds the *Web Server (IIS)* Role with *Web Server* Role Service will require a special exception to this recommendation, to allow IIS application pool(s) to be granted this user right.

Note #3: A Member Server with Microsoft SQL Server installed will require a special exception to this recommendation for additional SQL-generated entries to be granted this user right.

Rationale:

A user with the **Adjust memory quotas for a process** user right can reduce the amount of memory that is available to any process, which could cause business-critical network applications to become slow or to fail. In the wrong hands, this privilege could be used to start a DoS attack.

Impact:

Organizations that have not restricted users to roles with limited privileges will find it difficult to impose this countermeasure. Also, if you have installed optional components such as ASP.NET or IIS, you may need to assign the **Adjust memory quotas for a process** user right to additional accounts that are required by those components. Otherwise, this countermeasure should have no impact on most computers. If this user right is necessary for a user account, it can be assigned to a local computer account instead of a domain account.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Administrators, LOCAL SERVICE, NETWORK SERVICE`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Adjust memory quotas for a process
```

Default Value:

Administrators, LOCAL SERVICE, NETWORK SERVICE.

References:

1. GRID: MS-00000016

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●

2.2.7 Ensure 'Allow log on locally' is set to 'Administrators, ENTERPRISE DOMAIN CONTROLLERS' (DC only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This policy setting determines which users can interactively log on to computers in your environment. Logons that are initiated by pressing the CTRL+ALT+DEL key sequence on the client computer keyboard require this user right. Users who attempt to log on through Terminal Services / Remote Desktop Services or IIS also require this user right.

The recommended state for this setting *on Domain Controllers* is: `Administrators, ENTERPRISE DOMAIN CONTROLLERS`.

Note: Certain policy settings must be configured in the **Default Domain Controller Policy** to ensure they are applied globally to domain controllers. Exercise caution when modifying these policies, as improper changes can negatively impact the environment.

Only policies that are configured by Microsoft by default should reside in these baseline GPOs. Any additional or custom policy settings should be implemented through separate GPOs rather than modifying the default policies.

Note #2: This user right should generally be restricted to the `Administrators` group. Assign this user right to the `Backup Operators` group if your organization requires that they have this capability.

Note #3: When a server is promoted to a Domain Controller `ENTERPRISE DOMAIN CONTROLLERS` is granted this user right by default.

Rationale:

Any account with the **Allow log on locally** user right can log on at the console of the computer. If you do not restrict this user right to legitimate users who need to be able to log on to the console of the computer, unauthorized users could download and run malicious software to elevate their privileges.

Impact:

If you remove these default groups, you could limit the abilities of users who are assigned to specific administrative roles in your environment. You should confirm that delegated activities will not be adversely affected by any changes that you make to the **Allow log on locally** user right.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, configure the following UI path to `Administrators, ENTERPRISE DOMAIN CONTROLLERS`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Allow log on locally
```

Default Value:

Account Operators, Administrators, Backup Operators, ENTERPRISE DOMAIN CONTROLLERS, Print Operators, Server Operators.

References:

1. GRID: MS-00000017

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●

2.2.8 Ensure 'Allow log on locally' is set to 'Administrators' (MS only) (Automated)

Profile Applicability:

- Level 1 - Member Server

Description:

This policy setting determines which users can interactively log on to computers in your environment. Logons that are initiated by pressing the CTRL+ALT+DEL key sequence on the client computer keyboard require this user right. Users who attempt to log on through Terminal Services / Remote Desktop Services or IIS also require this user right.

The recommended state for this setting *on Member Servers* is: `Administrators`.

Note: This user right should generally be restricted to the `Administrators` group. Assign this user right to the `Backup Operators` group if your organization requires that they have this capability.

Rationale:

Any account with the **Allow log on locally** user right can log on at the console of the computer. If you do not restrict this user right to legitimate users who need to be able to log on to the console of the computer, unauthorized users could download and run malicious software to elevate their privileges.

Impact:

If you remove these default groups, you could limit the abilities of users who are assigned to specific administrative roles in your environment. You should confirm that delegated activities will not be adversely affected by any changes that you make to the **Allow log on locally** user right.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, configure the following UI path to `Administrators`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Allow log on locally
```

Default Value:

Administrators, Backup Operators, Users.

References:

1. GRID: MS-00000017

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●

2.2.9 Ensure 'Allow log on through Remote Desktop Services' is set to 'Administrators' (DC only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This policy setting determines which users or groups have the right to log on as a Remote Desktop Services client. If your organization uses Remote Assistance as part of its help desk strategy, create a group and assign it this user right through Group Policy. If the help desk in your organization does not use Remote Assistance, assign this user right only to the `Administrators` group or use the Restricted Groups feature to ensure that no user accounts are part of the `Remote Desktop Users` group.

Restrict this user right to the `Administrators` group, and possibly the `Remote Desktop Users` group, to prevent unwanted users from gaining access to computers on your network by means of the Remote Assistance feature.

The recommended state for this setting *on Domain Controllers* is: `Administrators`.

Note: The above lists are to be treated as whitelists, which implies that the above principals need not be present for assessment of this recommendation to pass.

Note #2: In all versions of Windows Server prior to Server 2008 R2, **Remote Desktop Services** was known as **Terminal Services**, so you should substitute the older term if comparing against an older OS.

Rationale:

Any account with the **Allow log on through Remote Desktop Services** user right can log on to the remote console of the computer. If you do not restrict this user right to legitimate users who need to log on to the console of the computer, unauthorized users could download and run malicious software to elevate their privileges.

Impact:

Removal of the **Allow log on through Remote Desktop Services** user right from other groups or membership changes in these default groups could limit the abilities of users who perform specific administrative roles in your environment. You should confirm that delegated activities will not be adversely affected.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, configure the following UI path to `Administrators`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Allow log on through Remote Desktop Services
```

Default Value:

Administrators.

References:

1. GRID: MS-00000018

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
v7	4.3 Ensure the Use of Dedicated Administrative Accounts Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	●	●	●

2.2.10 Ensure 'Allow log on through Remote Desktop Services' is set to 'Administrators, Remote Desktop Users' (MS only) (Automated)

Profile Applicability:

- Level 1 - Member Server

Description:

This policy setting determines which users or groups have the right to log on as a Remote Desktop Services client. If your organization uses Remote Assistance as part of its help desk strategy, create a group and assign it this user right through Group Policy. If the help desk in your organization does not use Remote Assistance, assign this user right only to the `Administrators` group or use the Restricted Groups feature to ensure that no user accounts are part of the `Remote Desktop Users` group.

Restrict this user right to the `Administrators` group, and possibly the `Remote Desktop Users` group, to prevent unwanted users from gaining access to computers on your network by means of the Remote Assistance feature.

The recommended state for this setting *on Member Servers* is: `Administrators, Remote Desktop Users`.

Note: The above lists are to be treated as whitelists, which implies that the above principals need not be present for assessment of this recommendation to pass.

Note #2: In all versions of Windows Server prior to Server 2008 R2, **Remote Desktop Services** was known as **Terminal Services**, so you should substitute the older term if comparing against an older OS.

Note #3: A Member Server that holds the *Remote Desktop Services* Role with *Remote Desktop Connection Broker* Role Service will require a special exception to this recommendation, to allow the `Authenticated Users` group to be granted this user right.

Rationale:

Any account with the **Allow log on through Remote Desktop Services** user right can log on to the remote console of the computer. If you do not restrict this user right to legitimate users who need to log on to the console of the computer, unauthorized users could download and run malicious software to elevate their privileges.

Impact:

Removal of the **Allow log on through Remote Desktop Services** user right from other groups or membership changes in these default groups could limit the abilities of users who perform specific administrative roles in your environment. You should confirm that delegated activities will not be adversely affected.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, configure the following UI path to `Administrators, Remote Desktop Users`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Allow log on through Remote Desktop Services
```

Default Value:

Administrators, Remote Desktop Users.

References:

1. GRID: MS-00000018

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
v7	4.3 Ensure the Use of Dedicated Administrative Accounts Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	●	●	●

2.2.11 Ensure 'Back up files and directories' is set to 'Administrators' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows users to circumvent file and directory permissions to back up the system. This user right is enabled only when an application (such as `NTBACKUP`) attempts to access a file or directory through the NTFS file system backup application programming interface (API). Otherwise, the assigned file and directory permissions apply.

The recommended state for this setting is: `Administrators`.

Note: Certain policy settings must be configured in the **Default Domain Controller Policy** to ensure they are applied globally to domain controllers. Exercise caution when modifying these policies, as improper changes can negatively impact the environment.

Only policies that are configured by Microsoft by default should reside in these baseline GPOs. Any additional or custom policy settings should be implemented through separate GPOs rather than modifying the default policies.

Note #2: This user right is considered a "sensitive privilege" for the purposes of auditing.

Rationale:

Users who are able to back up data from a computer could take the backup media to a non-domain computer on which they have administrative privileges and restore the data. They could take ownership of the files and view any unencrypted data that is contained within the backup set.

Impact:

Changes in the membership of the groups that have the **Back up files and directories** user right could limit the abilities of users who are assigned to specific administrative roles in your environment. You should confirm that authorized backup administrators are still able to perform backup operations.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Administrators`.

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Back up files and directories
```

Default Value:

On Member Servers: Administrators, Backup Operators.

On Domain Controllers: Administrators, Backup Operators, Server Operators.

References:

1. GRID: MS-00000019

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●

2.2.12 Ensure 'Change the system time' is set to 'Administrators, LOCAL SERVICE' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines which users and groups can change the time and date on the internal clock of the computers in your environment. Users who are assigned this user right can affect the appearance of event logs. When a computer's time setting is changed, logged events reflect the new time, not the actual time that the events occurred.

The recommended state for this setting is: `Administrators, LOCAL SERVICE`.

Note: Certain policy settings must be configured in the **Default Domain Controller Policy** to ensure they are applied globally to domain controllers. Exercise caution when modifying these policies, as improper changes can negatively impact the environment.

Only policies that are configured by Microsoft by default should reside in these baseline GPOs. Any additional or custom policy settings should be implemented through separate GPOs rather than modifying the default policies.

Note #2: Discrepancies between the time on the local computer and on the Domain Controllers in your environment may cause problems for the Kerberos authentication protocol, which could make it impossible for users to log on to the domain or obtain authorization to access domain resources after they are logged on. Also, problems will occur when Group Policy is applied to client computers if the system time is not synchronized with the Domain Controllers.

Rationale:

Users who can change the time on a computer could cause several problems. For example, time stamps on event log entries could be made inaccurate, time stamps on files and folders that are created or modified could be incorrect, and computers that belong to a domain may not be able to authenticate themselves or users who try to log on to the domain from them. Also, because the Kerberos authentication protocol requires that the requestor and authenticator have their clocks synchronized within an administrator-defined skew period, a threat actor who changes a computer's time may cause that computer to be unable to obtain or grant Kerberos tickets.

The risk from these types of events is mitigated on most Domain Controllers, Member Servers, and end-user computers because the Windows Time service automatically synchronizes time with Domain Controllers in the following ways:

- All client desktop computers and Member Servers use the authenticating Domain Controller as their inbound time partner.
- All Domain Controllers in a domain nominate the Primary Domain Controller (PDC) Emulator operations master as their inbound time partner.
- All PDC Emulator operations masters follow the hierarchy of domains in the selection of their inbound time partner.
- The PDC Emulator operations master at the root of the domain is authoritative for the organization. Therefore it is recommended that you configure this computer to synchronize with a reliable external time server.

This vulnerability becomes much more serious if a threat actor is able to change the system time and then stop the Windows Time service or reconfigure it to synchronize with a time server that is not accurate.

Impact:

There should be no impact, because time synchronization for most organizations should be fully automated for all computers that belong to the domain. Computers that do not belong to the domain should be configured to synchronize with an external source.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Administrators, LOCAL SERVICE`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Change the system time
```

Default Value:

On Member Servers: Administrators, LOCAL SERVICE.

On Domain Controllers: Administrators, LOCAL SERVICE, Server Operators.

References:

1. GRID: MS-00000020

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control			●

Controls Version	Control	IG 1	IG 2	IG 3
	Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			

2.2.13 Ensure 'Create a pagefile' is set to 'Administrators' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows users to change the size of the pagefile. The page file is a hidden system file on the hard drive that serves as an extension of the system's RAM. When physical memory is full, the system moves less frequently used data to the page file to free up RAM for active processes

The recommended state for this setting is: `Administrators`.

Note: Certain policy settings must be configured in the **Default Domain Controller Policy** to ensure they are applied globally to domain controllers. Exercise caution when modifying these policies, as improper changes can negatively impact the environment.

Only policies that are configured by Microsoft by default should reside in these baseline GPOs. Any additional or custom policy settings should be implemented through separate GPOs rather than modifying the default policies.

Rationale:

Users who can change the page file size could make it extremely small or move the file to a highly fragmented storage volume, which could cause reduced computer performance.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Administrators`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Create a pagefile
```

Default Value:

Administrators.

References:

1. GRID: MS-00000022

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●

2.2.14 Ensure 'Create a token object' is set to 'No One' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows a process to create an access token, which may provide elevated rights to access sensitive data.

The recommended state for this setting is: `No One`.

Note: This user right is considered a "sensitive privilege" for the purposes of auditing.

Rationale:

A user account that is given this user right has complete control over the system and can lead to the system being compromised. It is highly recommended that you do not assign any user accounts this right.

The operating system examines a user's access token to determine the level of the user's privileges. Access tokens are built when users log on to the local computer or connect to a remote computer over a network. When you revoke a privilege, the change is immediately recorded, but the change is not reflected in the user's access token until the next time the user logs on or connects. Users with the ability to create or modify tokens can change the level of access for any currently logged on account. They could escalate their own privileges or create a DoS condition.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `No One`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Create a token object
```

Default Value:

No one.

References:

1. GRID: MS-00000023

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●

2.2.15 Ensure 'Create global objects' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether users can create global objects that are available to all sessions. Users can still create objects that are specific to their own session if they do not have this user right.

Users who can create global objects could affect processes that run under other users' sessions. This capability could lead to a variety of problems, such as application failure or data corruption.

The recommended state for this setting is: `Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE`.

Note: A Member Server with Microsoft SQL Server *and* its optional "Integration Services" component installed will require a special exception to this recommendation for additional SQL-generated entries to be granted this user right.

Rationale:

Users who can create global objects could affect Windows services and processes that run under other user or system accounts. This capability could lead to a variety of problems, such as application failure, data corruption and elevation of privilege.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Create global objects
```

Default Value:

Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE.

References:

1. GRID: MS-00000024

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●

2.2.16 Ensure 'Create permanent shared objects' is set to 'No One' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This user right is useful to kernel-mode components that extend the object namespace. However, components that run in kernel mode have this user right inherently. Therefore, it is typically not necessary to specifically assign this user right.

The recommended state for this setting is: `No One`.

Rationale:

Users who have the **Create permanent shared objects** user right could create new shared objects and expose sensitive data to the network.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `No One`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Create permanent shared objects
```

Default Value:

No one.

References:

1. GRID: MS-00000025

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●

2.2.17 Ensure 'Create symbolic links' is set to 'Administrators' (DC only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This policy setting determines which users can create symbolic links. In Windows Vista, existing NTFS file system objects, such as files and folders, can be accessed by referring to a new kind of file system object called a symbolic link. A symbolic link is a pointer (much like a shortcut or .lnk file) to another file system object, which can be a file, folder, shortcut or another symbolic link. The difference between a shortcut and a symbolic link is that a shortcut only works from within the Windows shell. To other programs and applications, shortcuts are just another file, whereas with symbolic links, the concept of a shortcut is implemented as a feature of the NTFS file system.

Symbolic links can potentially expose security vulnerabilities in applications that are not designed to use them. For this reason, the privilege for creating symbolic links should only be assigned to trusted users. By default, only `Administrators` can create symbolic links.

The recommended state for this setting *on Domain Controllers* is: `Administrators`.

Rationale:

Users who have the **Create symbolic links** user right could inadvertently or maliciously expose your system to symbolic link attacks. Symbolic link attacks can be used to change the permissions on a file, to corrupt data, to destroy data, or as a denial-of-service attack.

Impact:

In most cases there will be no impact because this is the default configuration. However, on Windows Servers with the Hyper-V server role installed, this user right should also be granted to the special group `Virtual Machines` - otherwise you will not be able to create new virtual machines.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, configure the following UI path to `Administrators`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Create symbolic links
```

Default Value:

Administrators.

References:

1. GRID: MS-00000026

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●

2.2.18 Ensure 'Create symbolic links' is set to 'Administrators, NT VIRTUAL MACHINE\Virtual Machines' (MS only) (Automated)

Profile Applicability:

- Level 1 - Member Server

Description:

This policy setting determines which users can create symbolic links. In Windows Vista, existing NTFS file system objects, such as files and folders, can be accessed by referring to a new kind of file system object called a symbolic link. A symbolic link is a pointer (much like a shortcut or .lnk file) to another file system object, which can be a file, folder, shortcut or another symbolic link. The difference between a shortcut and a symbolic link is that a shortcut only works from within the Windows shell. To other programs and applications, shortcuts are just another file, whereas with symbolic links, the concept of a shortcut is implemented as a feature of the NTFS file system.

Symbolic links can potentially expose security vulnerabilities in applications that are not designed to use them. For this reason, the privilege for creating symbolic links should only be assigned to trusted users. By default, only `Administrators` can create symbolic links.

The recommended state for this setting *on Member Servers* is: `Administrators` and (when the *Hyper-V* Role is installed) `NT VIRTUAL MACHINE\Virtual Machines`.

Rationale:

Users who have the **Create symbolic links** user right could inadvertently or maliciously expose your system to symbolic link attacks. Symbolic link attacks can be used to change the permissions on a file, to corrupt data, to destroy data, or as a denial-of-service attack.

Impact:

In most cases there will be no impact because this is the default configuration. However, on Windows Servers with the Hyper-V server role installed, this user right should also be granted to the special group `Virtual Machines` - otherwise you will not be able to create new virtual machines.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, configure the following UI path to `Administrators` and (when the *Hyper-V* Role is installed) `NT VIRTUAL MACHINE\Virtual Machines`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Create symbolic links
```

Default Value:

Administrators.

References:

1. GRID: MS-00000026

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●

2.2.19 Ensure 'Debug programs' is set to 'Administrators' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines which user accounts will have the right to attach a debugger to any process or to the kernel, which provides complete access to sensitive and critical operating system components. Developers who are debugging their own applications do not need to be assigned this user right; however, developers who are debugging new system components will need it.

The recommended state for this setting is: `Administrators`.

Note: Certain policy settings must be configured in the **Default Domain Controller Policy** to ensure they are applied globally to domain controllers. Exercise caution when modifying these policies, as improper changes can negatively impact the environment.

Only policies that are configured by Microsoft by default should reside in these baseline GPOs. Any additional or custom policy settings should be implemented through separate GPOs rather than modifying the default policies.

Note #2: This user right is considered a "sensitive privilege" for the purposes of auditing.

Rationale:

The **Debug programs** user right can be exploited to capture sensitive computer information from system memory, or to access and modify kernel or application structures. Some attack tools exploit this user right to extract hashed passwords and other private security information, or to insert rootkit code. By default, the **Debug programs** user right is assigned only to administrators, which helps to mitigate the risk from this vulnerability.

Impact:

If you revoke this user right, no one will be able to debug programs. However, typical circumstances rarely require this capability on production computers. If a problem arises that requires an application to be debugged on a production server, you can move the server to a different OU temporarily and assign the **Debug programs** user right to a separate Group Policy for that OU.

The service account that is used for the cluster service needs the **Debug programs** user right; if it does not have it, Windows Clustering will fail.

Tools that are used to manage processes will be unable to affect processes that are not owned by the person who runs the tools. For example, the Windows Server 2003 Resource Kit tool `Kill.exe` requires this user right for administrators to terminate processes that they did not start.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Administrators`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Debug programs
```

Default Value:

Administrators.

References:

1. GRID: MS-00000027

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
v7	18.2 Ensure Explicit Error Checking is Performed for All In-house Developed Software For in-house developed software, ensure that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats.		●	●

2.2.20 Ensure 'Deny access to this computer from the network' to include 'Guests' (DC only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This policy setting prohibits users from connecting to a computer from across the network, which would allow users to access and potentially modify data remotely. In high security environments, there should be no need for remote users to access data on a computer. Instead, file sharing should be accomplished through the use of network servers. This user right supersedes the **Access this computer from the network** user right if an account is subject to both policies.

The recommended state for this setting *on Domain Controllers* is to include: `Guests`.

Rationale:

Users who can log on to the computer over the network can enumerate lists of account names, group names, and shared resources. Users with permission to access shared folders and files can connect over the network and possibly view or modify data.

Impact:

If you configure the **Deny access to this computer from the network** user right for other groups, you could limit the abilities of users who are assigned to specific administrative roles in your environment. You should verify that delegated tasks will not be negatively affected.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, configure the following UI path to include `Guests`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Deny access to this computer from the network
```

Default Value:

Guest.

References:

1. GRID: MS-00000028

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●

2.2.21 Ensure 'Deny access to this computer from the network' to include 'Guests, Local account and member of Administrators group' (MS only) (Automated)

Profile Applicability:

- Level 1 - Member Server

Description:

This policy setting prohibits users from connecting to a computer from across the network, which would allow users to access and potentially modify data remotely. In high security environments, there should be no need for remote users to access data on a computer. Instead, file sharing should be accomplished through the use of network servers. This user right supersedes the **Access this computer from the network** user right if an account is subject to both policies.

The recommended state for this setting *on Member Servers* is to include: `Guests, Local account and member of Administrators group`.

Caution: Configuring a standalone (non-domain-joined) server as described above may result in an inability to remotely administer the server.

Note: The security identifier `Local account and member of Administrators group` is not available in Server 2008 R2 and Server 2012 (non-R2) unless MSKB 2871997 has been installed.

Note #2: Configuring a Member Server or standalone server as described above may adversely affect applications that create a local service account and place it in the Administrators group - in which case you must either convert the application to use a domain-hosted service account, or remove `Local account and member of Administrators group` from this User Right Assignment. Using a domain-hosted service account is strongly preferred over making an exception to this rule, where possible.

Rationale:

Users who can log on to the computer over the network can enumerate lists of account names, group names, and shared resources. Users with permission to access shared folders and files can connect over the network and possibly view or modify data.

Impact:

If you configure the **Deny access to this computer from the network** user right for other groups, you could limit the abilities of users who are assigned to specific administrative roles in your environment. You should verify that delegated tasks will not be negatively affected.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, configure the following UI path to include `Guests, Local account and member of Administrators group`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny access to this computer from the network
```

Default Value:

No one.

References:

1. GRID: MS-00000028

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●

2.2.22 Ensure 'Deny log on as a batch job' to include 'Guests' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines which accounts will not be able to log on to the computer as a batch job. A batch job is not a batch (.bat) file, but rather a batch-queue facility. Accounts that use the Task Scheduler to schedule jobs need this user right.

This user right supersedes the **Log on as a batch job** user right, which could be used to allow accounts to schedule jobs that consume excessive system resources. Such an occurrence could cause a DoS condition. Failure to assign this user right to the recommended accounts can be a security risk.

The recommended state for this setting is to include: `Guests`.

Rationale:

Accounts that have the **Log on as a batch job** user right could be used to schedule jobs that could consume excessive computer resources and cause a DoS condition.

Impact:

If you assign the **Deny log on as a batch job** user right to other accounts, you could deny users who are assigned to specific administrative roles the ability to perform their required job activities. You should confirm that delegated tasks will not be affected adversely.

For example, if you assign this user right to the `IWAM_`*(ComputerName)* account, the MSM Management Point will fail. On a newly installed computer that runs Windows Server 2003 this account does not belong to the `Guests` group, but on a computer that was upgraded from Windows 2000 this account is a member of the `Guests` group. Therefore, it is important that you understand which accounts belong to any groups that you assign the **Deny log on as a batch job** user right.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to include `Guests`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Deny log on as a batch job
```

Default Value:

No one.

References:

1. GRID: MS-00000029

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●

2.2.23 Ensure 'Deny log on as a service' to include 'Guests' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This security setting determines which service accounts are prevented from registering a process as a service. This user right supersedes the **Log on as a service** user right if an account is subject to both policies.

The recommended state for this setting is to include: `Guests`.

Note: This security setting does not apply to the `System`, `Local Service`, or `Network Service` accounts.

Rationale:

Accounts that can log on as a service could be used to configure and start new unauthorized services, such as a keylogger or other malicious software. The benefit of the specified countermeasure is somewhat reduced by the fact that only users with administrative privileges can install and configure services, and a threat actor who has already attained that level of access could configure the service to run with the `System` account.

Impact:

If you assign the **Deny log on as a service** user right to specific accounts, services may not be able to start and a DoS condition could result.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to include `Guests`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny log on as a service
```

Default Value:

No one.

References:

1. GRID: MS-00000030

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●

2.2.24 Ensure 'Deny log on locally' to include 'Guests' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This security setting determines which users are prevented from logging on at the computer. This policy setting supersedes the **Allow log on locally** policy setting if an account is subject to both policies.

The recommended state for this setting is to include: `Guests`.

Important: If you apply this security policy to the `Everyone` group, no one will be able to log on locally.

Rationale:

Any account with the ability to log on locally could be used to log on at the console of the computer. If this user right is not restricted to legitimate users who need to log on to the console of the computer, unauthorized users might download and run malicious software that elevates their privileges.

Impact:

If you assign the **Deny log on locally** user right to additional accounts, you could limit the abilities of users who are assigned to specific roles in your environment. However, this user right should explicitly be assigned to the `ASPNET` account on computers that run IIS 6.0. You should confirm that delegated activities will not be adversely affected.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to include `Guests`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Deny log on locally
```

Default Value:

No one.

References:

1. GRID: MS-00000031

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●

2.2.25 Ensure 'Deny log on through Remote Desktop Services' to include 'Guests' (DC only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This policy setting determines whether users can log on as Remote Desktop clients. After the baseline Member Server is joined to a domain environment, there is no need to use local accounts to access the server from the network. Domain accounts can access the server for administration and end-user processing. This user right supersedes the **Allow log on through Remote Desktop Services** user right if an account is subject to both policies.

The recommended state for this setting is to include: `Guests`.

Note: The security identifier `Local account` is not available in Server 2008 R2 and Server 2012 (non-R2) unless MSKB 2871997 has been installed.

Note #2: In all versions of Windows Server prior to Server 2008 R2, **Remote Desktop Services** was known as **Terminal Services**, so you should substitute the older term if comparing against an older OS.

Rationale:

Any account with the right to log on through Remote Desktop Services could be used to log on to the remote console of the computer. If this user right is not restricted to legitimate users who need to log on to the console of the computer, unauthorized users might download and run malicious software that elevates their privileges.

Impact:

If you assign the **Deny log on through Remote Desktop Services** user right to other groups, you could limit the abilities of users who are assigned to specific administrative roles in your environment. Accounts that have this user right will be unable to connect to the computer through either Remote Desktop Services or Remote Assistance. You should confirm that delegated tasks will not be negatively impacted.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, configure the following UI path to include `Guests`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Deny log on through Remote Desktop Services
```

Default Value:

No one.

References:

1. GRID: MS-00000032

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●

2.2.26 Ensure 'Deny log on through Remote Desktop Services' is set to 'Guests, Local account' (MS only) (Automated)

Profile Applicability:

- Level 1 - Member Server

Description:

This policy setting determines whether users can log on as Remote Desktop clients. After the baseline Member Server is joined to a domain environment, there is no need to use local accounts to access the server from the network. Domain accounts can access the server for administration and end-user processing. This user right supersedes the **Allow log on through Remote Desktop Services** user right if an account is subject to both policies.

The recommended state for this setting is: `Guests, Local account`.

Note: The security identifier `Local account` is not available in Server 2008 R2 and Server 2012 (non-R2) unless MSKB 2871997 has been installed.

Note #2: In all versions of Windows Server prior to Server 2008 R2, **Remote Desktop Services** was known as **Terminal Services**, so you should substitute the older term if comparing against an older OS.

Rationale:

Any account with the right to log on through Remote Desktop Services could be used to log on to the remote console of the computer. If this user right is not restricted to legitimate users who need to log on to the console of the computer, unauthorized users might download and run malicious software that elevates their privileges.

Impact:

If you assign the **Deny log on through Remote Desktop Services** user right to other groups, you could limit the abilities of users who are assigned to specific administrative roles in your environment. Accounts that have this user right will be unable to connect to the computer through either Remote Desktop Services or Remote Assistance. You should confirm that delegated tasks will not be negatively impacted.

Caution: Configuring a standalone (non-domain-joined) or a system hosted in the Cloud (Azure) as described above (Local account) will result in an inability to remotely administer the workstation.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, configure the following UI path to `Guests, Local account`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Deny log on through Remote Desktop Services
```

Default Value:

No one.

References:

1. GRID: MS-00000032

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●

2.2.27 Ensure 'Enable computer and user accounts to be trusted for delegation' is set to 'Administrators' (DC only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This policy setting allows users to change the Trusted for Delegation setting on a computer object in Active Directory.

The recommended state for this setting *on Domain Controllers* is: `Administrators`.

Note: Certain policy settings must be configured in the **Default Domain Controller Policy** to ensure they are applied globally to domain controllers. Exercise caution when modifying these policies, as improper changes can negatively impact the environment.

Only policies that are configured by Microsoft by default should reside in these baseline GPOs. Any additional or custom policy settings should be implemented through separate GPOs rather than modifying the default policies.

Note #2: This user right is considered a "sensitive privilege" for the purposes of auditing.

Rationale:

Misuse of this user right could allow unauthorized users to impersonate other users on the network. A threat actor could exploit this privilege to gain access to network resources and make it difficult to determine what has happened after a security incident.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, configure the following UI path to `Administrators`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Enable computer and user accounts to be trusted for delegation
```

Default Value:

Administrators.

References:

1. GRID: MS-00000033

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
v7	4.1 Maintain Inventory of Administrative Accounts Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.		●	●

2.2.28 Ensure 'Enable computer and user accounts to be trusted for delegation' is set to 'No One' (MS only) (Automated)

Profile Applicability:

- Level 1 - Member Server

Description:

This policy setting allows users to change the Trusted for Delegation setting on a computer object in Active Directory.

The recommended state for this setting *on Member Servers* is: `No One`.

Note: This user right is considered a "sensitive privilege" for the purposes of auditing.

Rationale:

Misuse of this user right could allow unauthorized users to impersonate other users on the network. A threat actor could exploit this privilege to gain access to network resources and make it difficult to determine what has happened after a security incident.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, configure the following UI path to `No One`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Enable computer and user accounts to be
trusted for delegation
```

Default Value:

No one.

References:

1. GRID: MS-00000033

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
v7	4.1 Maintain Inventory of Administrative Accounts Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.		●	●

2.2.29 Ensure 'Force shutdown from a remote system' is set to 'Administrators' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows users to shut down Windows Vista-based or newer computers from remote locations on the network. Anyone who has been assigned this user right can cause a denial-of-service (DoS) condition, which would make the computer unavailable to service user requests. Therefore, it is recommended that only highly trusted administrators be assigned this user right.

The recommended state for this setting is: `Administrators`.

Note: Certain policy settings must be configured in the **Default Domain Controller Policy** to ensure they are applied globally to domain controllers. Exercise caution when modifying these policies, as improper changes can negatively impact the environment.

Only policies that are configured by Microsoft by default should reside in these baseline GPOs. Any additional or custom policy settings should be implemented through separate GPOs rather than modifying the default policies.

Rationale:

Any user who can shut down a computer could cause a DoS condition to occur. Therefore, this user right should be tightly restricted.

Impact:

If you remove the **Force shutdown from a remote system** user right from the Server Operators group you could limit the abilities of users who are assigned to specific administrative roles in your environment. You should confirm that delegated activities will not be adversely affected.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Administrators`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Force shutdown from a remote system
```

Default Value:

On Member Servers: Administrators.

On Domain Controllers: Administrators, Server Operators.

References:

1. GRID: MS-00000034

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
v7	4.1 Maintain Inventory of Administrative Accounts Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.		●	●

2.2.30 Ensure 'Generate security audits' is set to 'LOCAL SERVICE, NETWORK SERVICE' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines which users or processes can generate audit records in the Security log.

The recommended state for this setting is: `LOCAL SERVICE, NETWORK SERVICE`.

Note: This user right is considered a "sensitive privilege" for the purposes of auditing.

Note #2: A Member Server that holds the *Web Server (IIS)* Role with *Web Server* Role Service will require a special exception to this recommendation, to allow IIS application pool(s) to be granted this user right.

Note #3: A Member Server that holds the *Active Directory Federation Services* Role will require a special exception to this recommendation, to allow the `NT SERVICE\ADFSSrv` and `NT SERVICE\DRS` services, as well as the associated Active Directory Federation Services service account, to be granted this user right.

Rationale:

A threat actor could use this capability to create a large number of audited events, which would make it more difficult for a system administrator to locate any illicit activity. Also, if the event log is configured to overwrite events as needed, any evidence of unauthorized activities could be overwritten.

Impact:

On most computers, this is the default configuration and there will be no negative impact. However, if the *Web Server (IIS)* Role with *Web Services* Role Service is installed, the IIS application pool(s) must be granted this user right.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `LOCAL SERVICE, NETWORK SERVICE`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Generate security audits
```

Default Value:

LOCAL SERVICE, NETWORK SERVICE.

References:

1. GRID: MS-00000035
2. https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/generate-security-audits

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

2.2.31 Ensure 'Impersonate a client after authentication' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' (DC only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller

Description:

The policy setting allows programs that run on behalf of a user to impersonate that user (or another specified account) so that they can act on behalf of the user. If this user right is required for this kind of impersonation, an unauthorized user will not be able to convince a client to connect—for example, by remote procedure call (RPC) or named pipes—to a service that they have created to impersonate that client, which could elevate the unauthorized user's permissions to administrative or system levels.

Services that are started by the Service Control Manager have the built-in Service group added by default to their access tokens. COM servers that are started by the COM infrastructure and configured to run under a specific account also have the Service group added to their access tokens. As a result, these processes are assigned this user right when they are started.

Also, a user can impersonate an access token if any of the following conditions exist:

- The access token that is being impersonated is for this user.
- The user, in this logon session, logged on to the network with explicit credentials to create the access token.
- The requested level is less than Impersonate, such as Anonymous or Identify.

The recommended state for this setting *on Domain Controllers* is: `Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE`.

Note: This user right is considered a "sensitive privilege" for the purposes of auditing.

Rationale:

A threat actor with the **Impersonate a client after authentication** user right could create a service, trick a client to make them connect to the service, and then impersonate that client to elevate the threat actor's level of access to that of the client.

Impact:

In most cases this configuration will have no impact. If you have installed the *Web Server (IIS)* Role with *Web Services* Role Service, you will need to also assign the user right to `IIS_IUSRS`.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, configure the following UI path to `Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Impersonate a client after authentication
```

Default Value:

Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE.

References:

1. GRID: MS-00000036

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●

2.2.32 Ensure 'Impersonate a client after authentication' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' (MS only) (Automated)

Profile Applicability:

- Level 1 - Member Server

Description:

The policy setting allows programs that run on behalf of a user to impersonate that user (or another specified account) so that they can act on behalf of the user. If this user right is required for this kind of impersonation, an unauthorized user will not be able to convince a client to connect—for example, by remote procedure call (RPC) or named pipes—to a service that they have created to impersonate that client, which could elevate the unauthorized user's permissions to administrative or system levels.

Services that are started by the Service Control Manager have the built-in Service group added by default to their access tokens. COM servers that are started by the COM infrastructure and configured to run under a specific account also have the Service group added to their access tokens. As a result, these processes are assigned this user right when they are started.

Also, a user can impersonate an access token if any of the following conditions exist:

- The access token that is being impersonated is for this user.
- The user, in this logon session, logged on to the network with explicit credentials to create the access token.
- The requested level is less than Impersonate, such as Anonymous or Identify.

The recommended state for this setting *on Member Servers* is: `Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE` and (when the *Web Server (IIS)* Role with *Web Services* Role Service is installed) `IIS_IUSRS`.

Note: This user right is considered a "sensitive privilege" for the purposes of auditing.

Note #2: A Member Server with Microsoft SQL Server *and* its optional "Integration Services" component installed will require a special exception to this recommendation for additional SQL-generated entries to be granted this user right.

Rationale:

A threat actor with the **Impersonate a client after authentication** user right could create a service, trick a client to make them connect to the service, and then impersonate that client to elevate the threat actor's level of access to that of the client.

Impact:

In most cases this configuration will have no impact. If you have installed the *Web Server (IIS)* Role with *Web Services* Role Service, you will need to also assign the user right to `IIS_IUSRS`.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, configure the following UI path to `Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE` and (when the *Web Server (IIS)* Role with *Web Services* Role Service is installed) `IIS_IUSRS`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Impersonate a client after authentication
```

Default Value:

Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE.

References:

1. GRID: MS-00000036

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●

2.2.33 Ensure 'Increase scheduling priority' is set to 'Administrators, Window Manager\Window Manager Group' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether users can increase the base priority class of a process. (It is not a privileged operation to increase relative priority within a priority class.) This user right is not required by administrative tools that are supplied with the operating system but might be required by software development tools.

The recommended state for this setting is: `Administrators, Window Manager\Window Manager Group`.

Rationale:

A user who is assigned this user right could increase the scheduling priority of a process to Real-Time, which would leave little processing time for all other processes and could lead to a DoS condition.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Administrators, Window Manager\Window Manager Group`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Increase scheduling priority
```

Default Value:

On Windows Server 2016 or older: Administrators.

On Windows Server 2019 or newer: Administrators, Window Manager\Window Manager Group.

References:

1. GRID: MS-00000037

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●

2.2.34 Ensure 'Load and unload device drivers' is set to 'Administrators' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows users to dynamically load a new device driver on a system. This user right is not required if a signed driver for the new hardware already exists in the Driver.cab file on the system.

The recommended state for this setting is: `Administrators`.

Note: Certain policy settings must be configured in the **Default Domain Controller Policy** to ensure they are applied globally to domain controllers. Exercise caution when modifying these policies, as improper changes can negatively impact the environment.

Only policies that are configured by Microsoft by default should reside in these baseline GPOs. Any additional or custom policy settings should be implemented through separate GPOs rather than modifying the default policies.

Note #2: This user right is considered a "sensitive privilege" for the purposes of auditing.

Rationale:

Device drivers run as highly privileged code. A user or threat actor who has the Load and unload device drivers user right could unintentionally install malicious code that masquerades as a device driver. Administrators should exercise greater care and install only drivers with verified digital signatures.

Impact:

If the Load and unload device drivers user right is removed from the `Print Operators` group or other accounts, it could limit the abilities of users who are assigned to specific administrative roles in your environment. Ensure that delegated tasks will not be negatively affected by this setting.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Administrators`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Load and unload device drivers
```

Default Value:

On Member Servers: Administrators.

On Domain Controllers: Administrators, Print Operators.

References:

1. GRID: MS-00000038

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●

2.2.35 Ensure 'Lock pages in memory' is set to 'No One' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows a process to keep data in physical memory, which prevents the system from paging the data to virtual memory on disk. If this user right is assigned, significant degradation of system performance can occur.

The recommended state for this setting is: `No One`.

Note: A Member Server with Microsoft SQL Server installed will require a special exception to this recommendation for additional SQL-generated entries to be granted this user right.

Rationale:

Users with the **Lock pages in memory** user right could assign physical memory to several processes, which could leave little or no RAM for other processes and result in a DoS condition.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `No One`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Lock pages in memory
```

Default Value:

No one.

References:

1. GRID: MS-00000039

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●

2.2.36 Ensure 'Log on as a batch job' is set to 'Administrators' (DC Only) (Automated)

Profile Applicability:

- Level 2 - Domain Controller

Description:

This policy setting allows accounts to log on using the task scheduler service. Because the task scheduler is often used for administrative purposes, it may be needed in enterprise environments. However, its use should be restricted in high security environments to prevent misuse of system resources or to prevent threat actors from using the right to launch malicious code after gaining user level access to a computer.

The recommended state for this setting is: `Administrators`.

Note: Certain policy settings must be configured in the **Default Domain Controller Policy** to ensure they are applied globally to domain controllers. Exercise caution when modifying these policies, as improper changes can negatively impact the environment.

Only policies that are configured by Microsoft by default should reside in these baseline GPOs. Any additional or custom policy settings should be implemented through separate GPOs rather than modifying the default policies.

Rationale:

The Log on as a batch job user right presents a low-risk vulnerability. For most organizations, the default settings are sufficient.

Impact:

If you configure the Log on as a batch job setting through domain-based Group Policies, the computer will not be able to assign the user right to accounts that are used for scheduled jobs in the Task Scheduler. If you install optional components such as ASP.NET or IIS, you might need to assign this user right to additional accounts that are required by those components. For example, IIS requires assignment of this user right to the `IIS_WPG` group and the `IUSR_`*(ComputerName)*, `ASPNET`, and `IWAM_`*(ComputerName)* accounts. If this user right is not assigned to this group and these accounts, IIS will be unable to run some COM objects that are necessary for proper functionality.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Administrators`:

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Log on as a batch job
```

Default Value:

Administrators, Backup Operators.

References:

1. GRID: MS-00000040

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●

2.2.37 Ensure 'Manage auditing and security log' is set to 'Administrators' (DC only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This policy setting determines which users can change the auditing options for files and directories and clear the Security log.

The recommended state for this setting *on Domain Controllers* is: `Administrators`.

Note: Certain policy settings must be configured in the **Default Domain Controller Policy** to ensure they are applied globally to domain controllers. Exercise caution when modifying these policies, as improper changes can negatively impact the environment.

Only policies that are configured by Microsoft by default should reside in these baseline GPOs. Any additional or custom policy settings should be implemented through separate GPOs rather than modifying the default policies.

Note #2: This user right is considered a "sensitive privilege" for the purposes of auditing.

Note #3: For environments running Microsoft Exchange Server, the `Exchange Servers` group must possess this privilege on Domain Controllers (DC) to properly function. Given this, an exception will be required if the DC grants the `Exchange Servers` group this privilege. If the environment does not use Microsoft Exchange Server, then this privilege should be limited to only `Administrators` on the DC.

Rationale:

The ability to manage the Security event log is a powerful user right and it should be closely guarded. Anyone with this user right can clear the Security log to erase important evidence of unauthorized activity.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, configure the following UI path to `Administrators`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Manage auditing and security log
```

Default Value:

Administrators.

References:

1. GRID: MS-00000042

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●

2.2.38 Ensure 'Manage auditing and security log' is set to 'Administrators' (MS only) (Automated)

Profile Applicability:

- Level 1 - Member Server

Description:

This policy setting determines which users can change the auditing options for files and directories and clear the Security log.

The recommended state for this setting *on Member Servers* is: `Administrators`.

Note: This user right is considered a "sensitive privilege" for the purposes of auditing.

Rationale:

The ability to manage the Security event log is a powerful user right and it should be closely guarded. Anyone with this user right can clear the Security log to erase important evidence of unauthorized activity.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, configure the following UI path to `Administrators`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Manage auditing and security log
```

Default Value:

Administrators.

References:

1. GRID: MS-00000042

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●

2.2.39 Ensure 'Modify an object label' is set to 'No One' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This privilege determines which user accounts can modify the integrity label of objects, such as files, registry keys, or processes owned by other users. Processes running under a user account can modify the label of an object owned by that user to a lower level without this privilege.

The recommended state for this setting is: `No One`.

Rationale:

By modifying the integrity label of an object owned by another user a threat actor may cause them to execute code at a higher level of privilege than intended.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `No One`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Modify an object label
```

Default Value:

No one.

References:

1. GRID: MS-00000043

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●

2.2.40 Ensure 'Modify firmware environment values' is set to 'Administrators' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows users to configure the system-wide environment variables that affect hardware configuration. This information is typically stored in the Last Known Good Configuration. Modification of these values could lead to a hardware failure that would result in a denial-of-service condition.

The recommended state for this setting is: `Administrators`.

Note: Certain policy settings must be configured in the **Default Domain Controller Policy** to ensure they are applied globally to domain controllers. Exercise caution when modifying these policies, as improper changes can negatively impact the environment.

Only policies that are configured by Microsoft by default should reside in these baseline GPOs. Any additional or custom policy settings should be implemented through separate GPOs rather than modifying the default policies.

Note #2: This user right is considered a "sensitive privilege" for the purposes of auditing.

Rationale:

Anyone who is assigned the **Modify firmware environment values** user right could configure the settings of a hardware component to cause it to fail, which could lead to data corruption or a DoS condition.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Administrators`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Modify firmware environment values
```

Default Value:

Administrators.

References:

1. GRID: MS-00000044

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●

2.2.41 Ensure 'Perform volume maintenance tasks' is set to 'Administrators' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows users to manage the system's volume or disk configuration, which could allow a user to delete a volume and cause data loss as well as a denial-of-service condition.

The recommended state for this setting is: `Administrators`.

Note: A Member Server with Microsoft SQL Server installed will require a special exception to this recommendation for the account that runs the SQL Server service to be granted this user right.

Rationale:

A user who is assigned the **Perform volume maintenance tasks** user right could delete a volume, which could result in the loss of data or a DoS condition.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Administrators`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Perform volume maintenance tasks
```

Default Value:

Administrators.

References:

1. GRID: MS-00000045

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●

2.2.42 Ensure 'Profile single process' is set to 'Administrators' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines which users can use tools to monitor the performance of non-system processes. Typically, this setting does not need to be configured to use the Microsoft Management Console (MMC) Performance snap-in. However, this user right is needed if System Monitor is configured to collect data using Windows Management Instrumentation (WMI).

The recommended state for this setting is: `Administrators`.

Note: Certain policy settings must be configured in the **Default Domain Controller Policy** to ensure they are applied globally to domain controllers. Exercise caution when modifying these policies, as improper changes can negatively impact the environment.

Only policies that are configured by Microsoft by default should reside in these baseline GPOs. Any additional or custom policy settings should be implemented through separate GPOs rather than modifying the default policies.

Rationale:

The **Profile single process** user right presents a moderate vulnerability. A threat actor with this user right could monitor a computer's performance to help identify critical processes that they might wish to attack directly. The threat actor may also be able to determine what processes run on the computer so that they can identify countermeasures that they may need to avoid, such as antivirus software, an intrusion-detection system, or which other users are logged on to a computer.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Administrators`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Profile single process
```

Default Value:

Administrators.

References:

1. GRID: MS-00000046

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●

2.2.43 Ensure 'Profile system performance' is set to 'Administrators, NT SERVICE\WdiServiceHost' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines which users can use Windows performance monitoring tools to monitor the performance of system processes.

The recommended state for this setting is: `Administrators, NT SERVICE\WdiServiceHost`.

Note: Certain policy settings must be configured in the **Default Domain Controller Policy** to ensure they are applied globally to domain controllers. Exercise caution when modifying these policies, as improper changes can negatively impact the environment.

Only policies that are configured by Microsoft by default should reside in these baseline GPOs. Any additional or custom policy settings should be implemented through separate GPOs rather than modifying the default policies.

Rationale:

Threat actors with this user right could monitor a computer's performance to help identify critical processes that they might wish to attack directly. Threat actors may also be able to determine what processes are active on the computer so that they could identify countermeasures that they may need to avoid, such as antivirus software or an intrusion detection system.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Administrators, NT SERVICE\WdiServiceHost`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Profile system performance
```

Default Value:

Windows Server 2008 (non-R2): Administrators.

Windows Server 2008 R2 or newer: Administrators, NT SERVICE\WdiServiceHost.

References:

1. GRID: MS-00000047

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●

2.2.44 Ensure 'Replace a process level token' is set to 'LOCAL SERVICE, NETWORK SERVICE' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows one process or service to start another service or process with a different security access token, which can be used to modify the security access token of that sub-process and result in the escalation of privileges.

The recommended state for this setting is: `LOCAL SERVICE, NETWORK SERVICE`.

Note: Certain policy settings must be configured in the **Default Domain Controller Policy** to ensure they are applied globally to domain controllers. Exercise caution when modifying these policies, as improper changes can negatively impact the environment.

Only policies that are configured by Microsoft by default should reside in these baseline GPOs. Any additional or custom policy settings should be implemented through separate GPOs rather than modifying the default policies.

Note #2: This user right is considered a "sensitive privilege" for the purposes of auditing.

Note #3: A Member Server that holds the *Web Server (IIS)* Role with *Web Server* Role Service will require a special exception to this recommendation, to allow IIS application pool(s) to be granted this user right.

Note #4: A Member Server with Microsoft SQL Server installed will require a special exception to this recommendation for additional SQL-generated entries to be granted this user right.

Rationale:

Users with the **Replace a process level token** privilege are able to start processes as other users whose credentials they know. They could use this method to hide their unauthorized actions on the computer. (On Windows 2000-based computers, use of the **Replace a process level token** user right also requires the user to have the **Adjust memory quotas for a process** user right that is discussed earlier in this section.)

Impact:

On most computers, this is the default configuration and there will be no negative impact. However, if you have installed the *Web Server (IIS)* Role with *Web Services* Role Service, you will need to allow the IIS application pool(s) to be granted this User Right Assignment.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `LOCAL SERVICE, NETWORK SERVICE`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Replace a process level token
```

Default Value:

LOCAL SERVICE, NETWORK SERVICE.

References:

1. GRID: MS-00000048

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●

2.2.45 Ensure 'Restore files and directories' is set to 'Administrators' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines which users can bypass file, directory, registry, and other persistent object permissions when restoring backed up files and directories on systems that run Windows Vista (or newer).

This user right also determines which users can set valid security principals as object owners; it is similar to the Back up files and directories user right.

The recommended state for this setting is: `Administrators`.

Note: Certain policy settings must be configured in the **Default Domain Controller Policy** to ensure they are applied globally to domain controllers. Exercise caution when modifying these policies, as improper changes can negatively impact the environment.

Only policies that are configured by Microsoft by default should reside in these baseline GPOs. Any additional or custom policy settings should be implemented through separate GPOs rather than modifying the default policies.

Note #2: This user right is considered a "sensitive privilege" for the purposes of auditing.

Rationale:

A threat actor with the Restore files and directories user right could restore sensitive data to a computer and overwrite data that is more recent, which could lead to loss of important data, data corruption, or a denial-of-service (DoS).

Threat actors could overwrite executable files that are used by legitimate administrators or system services with versions that include malicious software to grant themselves elevated privileges, compromise data, or install backdoors for continued access to the computer.

Note: Even if the following countermeasure is configured, a threat actor could still restore data to a computer in a domain that is controlled by the actor. Therefore, it is critical that organizations carefully protect the media that is used to back up data.

Impact:

Removing the "Restore files and directories" user right from the Backup Operators group or other delegated accounts may prevent authorized users from performing essential tasks. Before making this change, it's important to assess whether it will disrupt operational responsibilities.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Administrators`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Restore files and directories
```

Default Value:

On Member Servers: Administrators, Backup Operators.

On Domain Controllers: Administrators, Backup Operators, Server Operators.

References:

1. GRID: MS-00000049

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●

2.2.46 Ensure 'Shut down the system' is set to 'Administrators' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines which users who are logged on locally to the computers in your environment can shut down the operating system with the Shut Down command. Misuse of this user right can result in a denial-of-service condition.

The recommended state for this setting is: `Administrators`.

Note: Certain policy settings must be configured in the **Default Domain Controller Policy** to ensure they are applied globally to domain controllers. Exercise caution when modifying these policies, as improper changes can negatively impact the environment.

Rationale:

The ability to shut down Domain Controllers and Member Servers should be limited to a very small number of trusted Administrators. Although the **Shut down the system** user right requires the ability to log on to the server, you should be very careful about which accounts and groups you allow to shut down a Domain Controller or Member Server.

When a Domain Controller is shut down, it is no longer available to process logons, serve Group Policy, and answer Lightweight Directory Access Protocol (LDAP) queries. If you shut down Domain Controllers that possess Flexible Single Master Operations (FSMO) roles, you can disable key domain functionality, such as processing logons for new passwords — one of the functions of the Primary Domain Controller (PDC) Emulator role.

Impact:

The impact of removing these default groups from the **Shut down the system** user right could limit the delegated abilities of assigned roles in your environment. You should confirm that delegated activities will not be adversely affected.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Administrators`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Shut down the system
```

Default Value:

On Member Servers: Administrators, Backup Operators.

On Domain Controllers: Administrators, Backup Operators, Print Operators, Server Operators.

References:

1. GRID: MS-00000050

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●

2.2.47 Ensure 'Synchronize directory service data' is set to 'No One' (DC only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This security setting determines which users and groups have the authority to synchronize all directory service data. This is also known as Active Directory synchronization.

The recommended state for this setting is: `No One`.

Note: Certain policy settings must be configured in the **Default Domain Controller Policy** to ensure they are applied globally to domain controllers. Exercise caution when modifying these policies, as improper changes can negatively impact the environment.

Rationale:

The Synchronize directory service data user right affects Domain Controllers as only Domain Controllers should be able to synchronize directory service data.

Domain Controllers have this user right inherently, because the synchronization process runs in the context of the `System` account on Domain Controllers. Threat actors who have this user right can view all information stored within the directory. They could then use some of that information to facilitate additional attacks or expose sensitive data, such as direct telephone numbers or physical addresses.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `No One`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Synchronize directory service data
```

Default Value:

No one.

References:

1. GRID: MS-00000051

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●

2.2.48 Ensure 'Take ownership of files or other objects' is set to 'Administrators' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows users to take ownership of files, folders, registry keys, processes, or threads. This user right bypasses any permissions that are in place to protect objects to give ownership to the specified user.

The recommended state for this setting is: `Administrators`.

Note: Certain policy settings must be configured in the **Default Domain Controller Policy** to ensure they are applied globally to domain controllers. Exercise caution when modifying these policies, as improper changes can negatively impact the environment.
Note #2: This user right is considered a "sensitive privilege" for the purposes of auditing.

Rationale:

Any users with the **Take ownership of files or other objects** user right can take control of any object, regardless of the permissions on that object, and then make any changes they wish to that object. Such changes could result in exposure of data, corruption of data, or a DoS condition.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Administrators`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\User Rights Assignment\Take ownership of files or other objects
```

Default Value:

Administrators.

References:

1. GRID: MS-00000052

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

2.3 Security Options

This section contains recommendations for security options.

2.3.1 Accounts

This section contains recommendations related to default accounts.

2.3.1.1 Ensure 'Accounts: Guest account status' is set to 'Disabled' (MS only) (Automated)

Profile Applicability:

- Level 1 - Member Server

Description:

This policy setting determines whether the Guest account is enabled or disabled. The Guest account allows unauthenticated network users to gain access to the system.

The recommended state for this setting is: `Disabled`.

Note: This setting will have no impact when applied to the Domain Controllers organizational unit via group policy because Domain Controllers have no local account database. It can be configured at the domain level via group policy, similar to account lockout and password policy settings.

Rationale:

The default Guest account allows unauthenticated network users to log on as Guest with no password. These unauthorized users could access any resources that are accessible to the Guest account over the network. This capability means that any network shares with permissions that allow access to the Guest account, the Guests group, or the Everyone group will be accessible over the network, which could lead to the exposure or corruption of data.

Impact:

All network users will need to authenticate before they can access shared resources. If you disable the Guest account and the Network Access: Sharing and Security Model option is set to Guest Only, network logons, such as those performed by the Microsoft Network Server (SMB Service), will fail. This policy setting should have little impact on most organizations because it is the default setting in Microsoft Windows 2000, Windows XP, and Windows Server™ 2003.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Accounts: Guest account status
```

Default Value:

Disabled.

References:

1. GRID: MS-00000054

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.7 Manage Default Accounts on Enterprise Assets and Software Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.	●	●	●
v7	16.8 Disable Any Unassociated Accounts Disable any account that cannot be associated with a business process or business owner.	●	●	●

2.3.1.2 Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether local accounts that are not password protected can be used to log on from locations other than the physical computer console. If you enable this policy setting, local accounts that have blank passwords will not be able to log on to the network from remote client computers. Such accounts will only be able to log on at the keyboard of the computer.

The recommended state for this setting is: `Enabled`.

Rationale:

Blank passwords are a serious threat to computer security and should be forbidden through both organizational policy and suitable technical measures. In fact, the default settings for Active Directory domains require complex passwords of at least seven characters. However, if users with the ability to create new accounts bypass your domain-based password policies, they could create accounts with blank passwords. For example, a user could build a stand-alone computer, create one or more accounts with blank passwords, and then join the computer to the domain. The local accounts with blank passwords would still function. Anyone who knows the name of one of these unprotected accounts could then use it to log on.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SYSTEM\CurrentControlSet\Control\Lsa:LimitBlankPasswordUse
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Accounts: Limit local account use of blank
passwords to console logon only
```

Default Value:

Enabled.

References:

1. GRID: MS-00000055

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

2.3.1.3 Configure 'Accounts: Rename administrator account' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting enables the ability to rename the built-in local administrator account. This account is a well-known account that is known to be targeted by threat actors.

It is recommended to choose another name for this account, and to avoid names that denote administrative or elevated access accounts. Be sure to also change the default description for the local administrator (through the Computer Management console).

Rationale:

The built-in Administrator account exists on all systems that run the Windows 2000 or newer operating systems. If this account is renamed, it is slightly more difficult for threat actors to guess this privileged username and password combination.

The built-in Administrator account cannot be locked out, regardless of how many times a threat actor might use a bad password. This capability makes the Administrator account a popular target for brute force attacks that attempt to guess passwords. The value of this countermeasure is lessened because this account has a well-known SID, and there are third-party tools that allow authentication by using the SID rather than the account name. Therefore, even if the Administrator account is renamed, a threat actor could launch a brute force attack by using the SID to log on.

Note: As of October 11, 2022 (see MS KB5020282), a new policy was introduced (Allow Administrator account), which allows the built-in administrator account to be locked out if applied. This setting only applies to OSes that are patched with MS KB5020282)

Impact:

Users who are authorized to use this account will need to be aware of the new account name. (The guidance for this setting assumes that the Administrator account was not disabled, which was recommended earlier in this chapter.)

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, configure the following UI path:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Accounts: Rename administrator account
```

Default Value:

Administrator.

References:

1. GRID: MS-00000056

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.7 Manage Default Accounts on Enterprise Assets and Software Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.	●	●	●

2.3.1.4 Configure 'Accounts: Rename guest account' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting enables the ability to rename the built-in local guest account. This account is a well-known account that is known to be targeted by threat actors.

It is recommended to rename this account to something that does not indicate its purpose, even if this account is disabled.

On Domain Controllers, since they do not have their own local accounts, this rule refers to the built-in Guest account that was established when the domain was first created.

Rationale:

The Guest account exists on all computers that run Windows 2000 or newer operating systems. If this account is renamed it is slightly more difficult for threat actors to guess this privileged username and password combination.

Impact:

There should be little impact, because the Guest account is disabled by default.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, configure the following UI path:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Accounts: Rename guest account
```

Default Value:

Guest.

References:

1. GRID: MS-00000057

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.7 Manage Default Accounts on Enterprise Assets and Software Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.	●	●	●

2.3.2 Audit

This section contains recommendations related to auditing controls.

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows administrators to enable the more precise auditing capabilities present in Windows Vista.

The Audit Policy settings available in Windows Server 2003 Active Directory do not yet contain settings for managing the new auditing subcategories. To properly apply the auditing policies prescribed in this baseline, the Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings setting needs to be configured to Enabled.

The recommended state for this setting is: `Enabled`.

Important: Be very cautious about audit settings that can generate a large volume of traffic. For example, if you enable either success or failure auditing for all of the Privilege Use subcategories, the high volume of audit events generated can make it difficult to find other types of entries in the Security log. Such a configuration could also have a significant impact on system performance.

Rationale:

Prior to the introduction of auditing subcategories in Windows Vista, it was difficult to track events at a per-system or per-user level. The larger event categories created too many events and the key information that needed to be audited was difficult to find.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SYSTEM\CurrentControlSet\Control\Lsa:SCENoApplyLegacyAuditPolicy
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Audit: Force audit policy subcategory settings
(Windows Vista or later) to override audit policy category settings
```

Default Value:

Enabled. (Advanced Audit Policy Configuration settings will be used for auditing configuration, and legacy Audit Policy configuration settings will be ignored.)

References:

1. https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing#to-ensure-that-advanced-audit-policy-configuration-settings-are-not-overwritten
2. GRID: MS-00000058

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

2.3.2.2 Ensure 'Audit: Shut down system immediately if unable to log security audits' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether the system shuts down if it is unable to log Security events. It is a requirement for Trusted Computer System Evaluation Criteria (TCSEC)-C2 and Common Criteria certification to prevent auditable events from occurring if the audit system is unable to log them. Microsoft has chosen to meet this requirement by halting the system and displaying a stop message if the auditing system experiences a failure. When this policy setting is enabled, the system will be shut down if a security audit cannot be logged for any reason.

The recommended state for this setting is: `Disabled`.

Rationale:

If the *Audit: Shut down system immediately if unable to log security audits* setting is enabled, unplanned system failures can occur. The administrative burden can be significant, especially if the *Retention method for the Security log to Do not overwrite events (clear log manually)* is configured. This configuration causes a repudiation threat (a backup operator could deny that they backed up or restored data) to become a denial-of-service (DoS) vulnerability, because a server could be forced to shut down if it is overwhelmed with logon events and other security events that are written to the Security log. Also, because the shutdown is not graceful, it is possible that irreparable damage to the operating system, applications, or data could result. Although the NTFS file system guarantees its integrity when an ungraceful computer shutdown occurs, it cannot guarantee that every data file for every application will still be in a usable form when the computer restarts.

If the system is unable to record events to the Security log, critical evidence or important troubleshooting information may not be available for review after a security incident. Also, a threat actor could potentially generate a large volume of Security log events to purposely force a computer shutdown.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SYSTEM\CurrentControlSet\Control\Lsa:CrashOnAuditFail
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Audit: Shut down system immediately if unable to
log security audits
```

Default Value:

Disabled.

References:

1. GRID: MS-00000059

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 Ensure Adequate Audit Log Storage Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	●	●	●
v7	6.4 Ensure adequate storage for logs Ensure that all systems that store logs have adequate storage space for the logs generated.		●	●

2.3.3 DCOM

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

2.3.4 Devices

This section contains recommendations related to managing devices.

2.3.4.1 Ensure 'Devices: Prevent users from installing printer drivers' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines who is allowed to install a printer driver as part of connecting to a shared printer. For a computer to print to a shared printer, the driver for that shared printer must be installed on the local computer.

The recommended state for this setting is: `Enabled`.

Note: This setting does not affect the ability to add a local printer. This setting does not affect Administrators.

Rationale:

It may be appropriate in some organizations to allow users to install printer drivers on their own workstations. However, in a high security environment, only Administrators should be allowed, not users, to do this, because printer driver installation may unintentionally cause the computer to become less stable.

A threat actor could install inappropriate printer drivers in a deliberate attempt to damage the computer, or a user might accidentally install malicious software that masquerades as a printer driver. It is feasible for a threat actor to disguise a Trojan horse program as a printer driver. The program may appear to users as if they must use it to print, but such a program could unleash malicious code on the network.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SYSTEM\CurrentControlSet\Control\Print\Providers\LanMan Print
Services\Servers:AddPrinterDrivers
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Devices: Prevent users from installing printer
drivers
```

Default Value:

Enabled. (Only Administrators will be able to install a printer driver as part of connecting to a shared printer. The ability to add a local printer will not be affected.)

References:

1. GRID: MS-00000060

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●

2.3.5 Domain controller

This section contains recommendations related to Domain Controllers.

2.3.5.1 Ensure 'Domain controller: Allow server operators to schedule tasks' is set to 'Disabled' (DC only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This policy setting determines whether members of the Server Operators group are allowed to submit jobs by means of the AT schedule facility. The impact of this policy setting configuration should be small for most organizations. Users, including those in the Server Operators group, will still be able to create jobs by means of the Task Scheduler Wizard, but those jobs will run in the context of the account with which the user authenticates when they set up the job.

Note: An AT Service Account can be modified to select a different account rather than the LOCAL SYSTEM account. To change the account, open System Tools, click Scheduled Tasks, and then click Accessories folder. Then click AT Service Account on the Advanced menu.

The recommended state for this setting is: `Disabled`.

Rationale:

If you enable this policy setting, jobs that are created by server operators by means of the AT service will execute in the context of the account that runs that service. By default, that is the local SYSTEM account. If you enable this policy setting, server operators could perform tasks that SYSTEM is able to do but that they would typically not be able to do, such as add their account to the local Administrators group.

Impact:

None - this is the default behavior. Note that users (including those in the Server Operators group) are still able to create jobs by means of the Task Scheduler Wizard. However, those jobs will run in the context of the account that the user authenticates with when setting up the job.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SYSTEM\CurrentControlSet\Control\Lsa:SubmitControl
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Domain controller: Allow server operators to
schedule tasks
```

Default Value:

Disabled. (Server Operators are not allowed to submit jobs by means of the AT schedule facility.)

References:

1. GRID: MS-00000061

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.3.5.2 Ensure 'Domain controller: Allow vulnerable Netlogon secure channel connections' is set to 'Not Configured' (DC Only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This security setting determines whether the domain controller bypasses secure RPC for Netlogon secure channel connections for specified machine accounts.

When deployed, this policy should be applied to all domain controllers in a forest by enabling the policy on the domain controllers OU.

When the `Create Vulnerable Connections` list (allow list) is configured:

- Given allow permission, the domain controller will allow accounts to use a Netlogon secure channel without secure RPC.
- Given deny permission, the domain controller will require accounts to use a Netlogon secure channel with secure RPC which is the same as the default (not necessary).

Note: Warning from Microsoft - enabling this policy will expose your domain-joined devices and can expose your Active Directory forest to risk. This policy should be used as a temporary measure for 3rd-party devices as you deploy updates. Once a 3rd-party device is updated to support using secure RPC with Netlogon secure channels, the account should be removed from the Create Vulnerable Connections list. To better understand the risk of configuring accounts to be allowed to use vulnerable Netlogon secure channel connections, please visit How to manage the changes in Netlogon secure channel connections associated with CVE-2020-1472.

The recommended state for this setting is: `Not Configured`.

Rationale:

Enabling this policy will expose your domain-joined devices and can expose your Active Directory forest to security risks. It is highly recommended that this setting not be used (i.e. be left completely unconfigured) so as not to add risk.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location and when set properly a `REG_SZ` value of `does not exist`.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters:Vuln
erableChannelAllowList
```

Note: If this policy is set as prescribed, the registry key `vulnerablechannelallowlist`, will not be present in the above registry location.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Not Configured`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Domain controller: Allow vulnerable Netlogon secure
channel connections
```

Default Value:

Not Configured. (No machines or trust accounts are explicitly exempt from secure RPC with Netlogon secure channel connections enforcement.)

References:

1. https://go.microsoft.com/fwlink/?linkid=2133485
2. GRID: MS-00000463

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.3.5.3 Ensure 'Domain controller: LDAP server channel binding token requirements' is set to 'Always' (DC Only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This policy setting determines whether the LDAP server (Domain Controller) enforces validation of Channel Binding Tokens (CBT) received in LDAP bind requests that are sent over SSL/TLS (i.e. LDAPS).

The recommended state for this setting is: `Always`.

Note: All LDAP clients must have the CVC-2017-8563 security update to be compatible with Domain Controllers that have this setting enabled. More information on this setting is available at: MSKB 4520412: 2020 LDAP channel binding and LDAP signing requirements for Windows

Rationale:

Requiring Channel Binding Tokens (CBT) can prevent a threat actor who is able to capture users' authentication credentials (e.g. OAuth tokens, session identifiers, etc.) from reusing those credentials in another TLS session. This also helps to increase protection against "man-in-the-middle" attacks using LDAP authentication over SSL/TLS (LDAPS).

Impact:

All LDAP clients must provide channel binding information over SSL/TLS (i.e. LDAPS). The LDAP server (Domain Controller) rejects authentication requests from clients that do not do so. Clients must have the CVC-2017-8563 security update to support this feature, and may have compatibility issues with this setting without the security update. This may also mean that LDAP authentication requests over SSL/TLS that previously worked may stop working until the security update is installed.

When first deploying this setting, you may **initially** want to only set it to the alternate setting of `When supported` (instead of `Always`) on all Domain Controllers. This alternate, **interim** setting enables support for LDAP client channel binding but does not *require* it. Then set one DC that is not currently being targeted by LDAP clients to `Always`, and test each of the critical LDAP clients against that DC (and remediating as necessary), before deploying `Always` to the rest of the DCs.

We also recommend using the new Event ID 3039 on your Domain Controllers (added with the March 2020 security update) to help locate clients that do not use Channel Binding Tokens (CBT) in their LDAPS connections. This new Event ID requires increasing the logging level of the `16 LDAP Interface Events` portion of the NTDS service diagnostics to a value of `2` (Basic). For more information, please see *Table 2: CBT events* at this link: MSKB 4520412: 2020 LDAP channel binding and LDAP signing requirements for Windows

Older OSes such as Windows XP, Windows Server 2003, Windows Vista and Windows Server 2008 (non-R2), will first require patches for Microsoft Security Advisory 973811, as well as all associated fixes, in order to be compatible with domain controllers that have this setting deployed.

Note: Only `Always` is actually considered compliant to the CIS benchmark.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `2`.

```
HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Parameters:LdapEnforceChannelBinding
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Always`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain controller: LDAP server channel binding token requirements
```

Note: This Group Policy path requires the installation of the March 2020 (or later) Windows security update. With that update, Microsoft added this setting to the built-in OS security template.

Default Value:

Never. (No LDAP channel binding validation is performed.)

References:

1. GRID: MS-00000062

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	16.5 Encrypt Transmittal of Username and Authentication Credentials Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.		●	●

2.3.5.4 Ensure 'Domain controller: LDAP server signing requirements' is set to 'Require signing' (DC only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This policy setting determines whether the Lightweight Directory Access Protocol (LDAP) server requires LDAP clients to negotiate data signing.

The recommended state for this setting is: `Require signing`.

Note: Certain policy settings must be configured in the **Default Domain Controller Policy** to ensure they are applied globally to domain controllers. Exercise caution when modifying these policies, as improper changes can negatively impact the environment.

Note #2: Domain member computers must have *Network security: LDAP signing requirements* (Section 2.3.11) set to `Negotiate signing` or higher. If not, they will fail to authenticate once the above `Require signing` value is configured on the Domain Controllers. Fortunately, `Negotiate signing` is the default in the client configuration.

Note #3: This policy setting does not have any impact on LDAP simple bind (`ldap_simple_bind`) or LDAP simple bind through SSL (`ldap_simple_bind_s`). No Microsoft LDAP clients that are shipped with Windows XP Professional use LDAP simple bind or LDAP simple bind through SSL to talk to a Domain Controller.

Note #4: Before enabling this setting, first ensure that there are no clients (including server-based applications) that are configured to authenticate with Active Directory via unsigned LDAP, because changing this setting will break those applications. Such applications should first be reconfigured to use signed LDAP, Secure LDAP (LDAPS), or IPsec-protected connections.

Rationale:

Unsigned network traffic is susceptible to man-in-the-middle attacks. In such attacks, an intruder captures packets between the server and the client, modifies them, and then forwards them to the client. Where LDAP servers are concerned, a threat actor could cause a client to make decisions that are based on false records from the LDAP directory. To lower the risk of such an intrusion in an organization's network, you can implement strong physical security measures to protect the network infrastructure. Also, you could implement Internet Protocol security (IPsec) authentication header mode (AH), which performs mutual authentication and packet integrity for IP traffic to make all types of man-in-the-middle attacks extremely difficult.

Additionally, allowing the use of regular, unsigned LDAP permits credentials to be received over the network in clear text, which could very easily result in the interception of account passwords by other systems on the network.

Impact:

Unless TLS/SSL is being used, the LDAP data signing option must be negotiated. Clients that do not support LDAP signing will be unable to run LDAP queries against the Domain Controllers. All Windows 2000-based computers in your organization that are managed from Windows Server 2003-based or Windows XP-based computers and that use Windows NT Challenge/Response (NTLM) authentication must have Windows 2000 Service Pack 3 (SP3) installed. Alternatively, these clients must have a registry change. Also, some non-Microsoft operating systems do not support LDAP signing. If you enable this policy setting, client computers that use those operating systems may be unable to access domain resources.

Some non-Microsoft operating systems do not support LDAP signing. If you enable this policy setting, client computers that use those operating systems may be unable to access domain resources. More information about this registry change was published in Microsoft Knowledge Base article 325465.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `2`.

```
HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Parameters:LDAPServerIntegrity
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Require signing`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Domain controller: LDAP server signing requirements
```

Default Value:

None. (Data signing is not required in order to bind with the server. If the client requests data signing, the server supports it.)

References:

1. https://msrc.microsoft.com/update-guide/en-us/advisory/ADV190023
2. https://support.microsoft.com/en-us/topic/frequently-asked-questions-about-changes-to-lightweight-directory-access-protocol-41a40287-810a-e799-d067-f578fca055fc
3. GRID: MS-00000516

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●

2.3.5.5 Ensure 'Domain controller: Refuse machine account password changes' is set to 'Disabled' (DC only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This security setting determines whether Domain Controllers will refuse requests from member computers to change computer account passwords.

The recommended state for this setting is: `Disabled`.

Note: Some problems can occur as a result of machine account password expiration, particularly if a machine is reverted to a previous point-in-time state, as is common with virtual machines. Depending on how far back the reversion is, the older machine account password stored on the machine may no longer be recognized by the domain controllers, and therefore the computer loses its domain trust. This can also disrupt non-persistent VDI implementations, and devices with write filters that disallow permanent changes to the OS volume. Some organizations may choose to exempt themselves from this recommendation and disable machine account password expiration for these situations.

Rationale:

If you enable this policy setting on all Domain Controllers in a domain, domain members will not be able to change their computer account passwords, and those passwords will be more susceptible to attack.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters:RefusePasswordChan
ge
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Domain controller: Refuse machine account password
changes
```

Default Value:

Disabled. (By default, member computers change their computer account passwords as specified by the *Domain member: Maximum machine account password age* setting (Rule 2.3.6.5), which is by default every 30 days.)

References:

1. GRID: MS-00000519

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

2.3.6 Domain member

This section contains recommendations related to domain membership.

2.3.6.1 Ensure 'Domain member: Digitally encrypt or sign secure channel data (always)' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether all secure channel traffic that is initiated by the domain member must be signed or encrypted.

The recommended state for this setting is: `Enabled`.

Note: Certain policy settings must be configured in the **Default Domain Controller Policy** to ensure they are applied globally to domain controllers. Exercise caution when modifying these policies, as improper changes can negatively impact the environment.

Rationale:

When a computer joins a domain, a computer account is created. After it joins the domain, the computer uses the password for that account to create a secure channel with the Domain Controller for its domain every time that it restarts. Requests that are sent on the secure channel are authenticated—and sensitive information such as passwords are encrypted—but the channel is not integrity-checked, and not all information is encrypted.

Digital encryption and signing of the secure channel is a good idea where it is supported. The secure channel protects domain credentials as they are sent to the Domain Controller.

Impact:

None - this is the default behavior. However, only Windows NT 4.0 with Service Pack 6a (SP6a) and subsequent versions of the Windows operating system support digital encryption and signing of the secure channel. Windows 98 Second Edition clients do not support it unless they have `Dsclient` installed. Therefore, you cannot enable the Domain member: Digitally encrypt or sign secure channel data (always) setting on Domain Controllers that support Windows 98 clients as members of the domain. Potential impacts can include the following:

- The ability to create or delete trust relationships with clients running versions of Windows earlier than Windows NT 4.0 with SP6a will be disabled.
- Logons from clients running versions of Windows earlier than Windows NT 4.0 with SP6a will be disabled.

- The ability to authenticate other domains' users from a Domain Controller running a version of Windows earlier than Windows NT 4.0 with SP6a in a trusted domain will be disabled.

You can enable this policy setting after you eliminate all Windows 9x clients from the domain and upgrade all Windows NT 4.0 servers and Domain Controllers from trusted/trusting domains to Windows NT 4.0 with SP6a.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters:RequireSignOrSeal
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Domain member: Digitally encrypt or sign secure
channel data (always)
```

Default Value:

Enabled. (All secure channel data must be signed or encrypted.)

References:

1. GRID: MS-00000064

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	14.4 Encrypt All Sensitive Information in Transit Encrypt all sensitive information in transit.		●	●

2.3.6.2 Ensure 'Domain member: Digitally encrypt secure channel data (when possible)' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether a domain member should attempt to negotiate encryption for all secure channel traffic that it initiates.

The recommended state for this setting is: `Enabled`.

Rationale:

When a computer joins a domain, a computer account is created. After it joins the domain, the computer uses the password for that account to create a secure channel with the Domain Controller for its domain every time that it restarts. Requests that are sent on the secure channel are authenticated—and sensitive information such as passwords are encrypted—but the channel is not integrity-checked, and not all information is encrypted.

Digital encryption and signing of the secure channel is a good idea where it is supported. The secure channel protects domain credentials as they are sent to the Domain Controller.

Impact:

None - this is the default behavior. However, only Windows NT 4.0 Service Pack 6a (SP6a) and subsequent versions of the Windows operating system support digital encryption and signing of the secure channel. Windows 98 Second Edition clients do not support it unless they have `Dsclient` installed.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters:SealSecureChannel
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Domain member: Digitally encrypt secure channel
data (when possible)
```

Default Value:

Enabled. (The domain member will request encryption of all secure channel traffic.)

References:

1. GRID: MS-00000065

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	14.4 Encrypt All Sensitive Information in Transit Encrypt all sensitive information in transit.		●	●

2.3.6.3 Ensure 'Domain member: Digitally sign secure channel data (when possible)' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether a domain member should attempt to negotiate whether all secure channel traffic that it initiates must be digitally signed. Digital signatures protect the traffic from being modified by anyone who captures the data as it traverses the network.

The recommended state for this setting is: `Enabled`.

Rationale:

When a computer joins a domain, a computer account is created. After it joins the domain, the computer uses the password for that account to create a secure channel with the Domain Controller for its domain every time that it restarts. Requests that are sent on the secure channel are authenticated—and sensitive information such as passwords are encrypted—but the channel is not integrity-checked, and not all information is encrypted.

Digital encryption and signing of the secure channel is a good idea where it is supported. The secure channel protects domain credentials as they are sent to the Domain Controller.

Impact:

None - this is the default behavior. However, only Windows NT 4.0 with Service Pack 6a (SP6a) and subsequent versions of the Windows operating system support digital encryption and signing of the secure channel. Windows 98 Second Edition clients do not support it unless they have `Dsclient` installed.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters:SignSecureChannel
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Domain member: Digitally sign secure channel data
(when possible)
```

Default Value:

Enabled. (The domain member will request digital signing of all secure channel traffic.)

References:

1. GRID: MS-00000066

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●

2.3.6.4 Ensure 'Domain member: Disable machine account password changes' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether a domain member can periodically change its computer account password.

The recommended state for this setting is: `Disabled`.

Rationale:

If a system does not change their password, there are security risks because the security channel is used for pass-through authentication. If a threat actor discovers a password, the actor can potentially perform pass-through authentication to the domain controller.

Impact:

None - this is the default behavior.

Note: Some problems can occur as a result of machine account password expiration, particularly if a machine is reverted to a previous point-in-time state, as is common with virtual machines. Depending on how far back the reversion is, the older machine account password stored on the machine may no longer be recognized by the domain controllers, and therefore the computer loses its domain trust. This can also disrupt non-persistent VDI implementations, and devices with write filters that disallow permanent changes to the OS volume. Some organizations may choose to exempt themselves from this recommendation and disable machine account password expiration for these situations.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters:DisablePasswordChange
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Domain member: Disable machine account password
changes
```

Default Value:

Disabled. (The domain member can change its computer account password as specified by the recommendation *Domain Member: Maximum machine account password age*, which by default is every 30 days.)

References:

1. GRID: MS-00000067
2. https://learn.microsoft.com/en-us/troubleshoot/windows-server/windows-security/disable-machine-account-password
3. https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/domain-member-disable-machine-account-password-changes

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.6 Centralize Account Management Centralize account management through a directory or identity service.		●	●

2.3.6.5 Ensure 'Domain member: Maximum machine account password age' is set to '30 or fewer days, but not 0' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines the maximum allowable age for a computer account password. By default, domain members automatically change their domain passwords every 30 days. If you increase this interval significantly so that the computers no longer change their passwords, a threat actor would have more time to undertake a brute force attack against one of the computer accounts.

The recommended state for this setting is: `30 or fewer days, but not 0`.

Note: A value of `0` does not conform to the benchmark as it disables maximum password age.

Rationale:

In Active Directory-based domains, each computer has an account and password just like every user. By default, the domain members automatically change their domain password every 30 days. If this interval is increased significantly or set it to `0` so that the computers no longer change their passwords, a threat actor will have more time to undertake a brute force attack to guess the password of one or more computer accounts.

Impact:

None - this is the default behavior.

Note: Some problems can occur as a result of machine account password expiration, particularly if a machine is reverted to a previous point-in-time state, as is common with virtual machines. Depending on how far back the reversion is, the older machine account password stored on the machine may no longer be recognized by the domain controllers, and therefore the computer loses its domain trust. This can also disrupt non-persistent VDI implementations, and devices with write filters that disallow permanent changes to the OS volume. Some organizations may choose to exempt themselves from this recommendation and disable machine account password expiration for these situations.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a REG_DWORD value of `30` or less, but not `0`

```
HKLM\System\CurrentControlSet\Services\Netlogon\Parameters:MaximumPasswordAge
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `30 or fewer days, but not 0`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Domain member: Maximum machine account password age
```

Default Value:

30 days.

References:

1. GRID: MS-00000068

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●

2.3.6.6 Ensure 'Domain member: Require strong (Windows 2000 or later) session key' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

When this policy setting is enabled, a secure channel can only be established with Domain Controllers that are capable of encrypting secure channel data with a strong (128-bit) session key.

The recommended state for this setting is: `Enabled`.

Rationale:

Session keys that are used to establish secure channel communications between Domain Controllers and member computers are much stronger in Windows 2000 than they were in previous Microsoft operating systems. Whenever possible, these stronger session keys should be used to help protect secure channel communications from attacks that attempt to hijack network sessions and eavesdropping.

Eavesdropping is a form of hacking in which network data is read or altered in transit. The data can be modified to hide or change the sender, or be redirected.

Impact:

None - this is the default behavior. However, computers will not be able to join Windows NT 4.0 domains, and trusts between Active Directory domains and Windows NT-style domains may not work properly. Also, Domain Controllers with this setting configured will not allow older pre-Windows 2000 clients (that that do not support this policy setting) to join the domain.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters:RequireStrongKey
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Domain member: Require strong (Windows 2000 or
later) session key
```

Default Value:

Enabled. (The secure channel will not be established unless 128-bit encryption can be performed.)

References:

1. GRID: MS-00000069

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●

2.3.7 Interactive logon

This section contains recommendations related to interactive logons.

2.3.7.1 Ensure 'Interactive logon: Do not require CTRL+ALT+DEL' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting determines whether users must press CTRL+ALT+DEL before they log on.

The recommended state for this setting is: `Disabled`.

Rationale:

If users are not required to press CTRL+ALT+DEL, they are susceptible to attacks that attempt to intercept their passwords. If CTRL+ALT+DEL is required before logon, user passwords are communicated by means of a trusted path.

A threat actor could install a Trojan horse program that looks like the standard Windows logon dialog box and capture the user's password. The threat actor would then be able to log on to the compromised account with whatever level of privilege that user has.

Impact:

Users must press CTRL+ALT+DEL before they log on to Windows unless they use a smart card for Windows logon. A smart card is a tamper-proof device that stores security information.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:DisableCAD
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Interactive logon: Do not require CTRL+ALT+DEL
```

Default Value:

On Windows Server 2008 R2 or older: Disabled.

On Windows Server 2012 (non-R2) or newer: Enabled.

References:

1. GRID: MS-00000071

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.10 Enforce Automatic Device Lockout on Portable End-User Devices Enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices, where supported. For laptops, do not allow more than 20 failed authentication attempts; for tablets and smartphones, no more than 10 failed authentication attempts. Example implementations include Microsoft® InTune Device Lock and Apple® Configuration Profile maxFailedAttempts.		●	●

2.3.7.2 Ensure 'Interactive logon: Don't display last signed-in' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether the account name of the last user to log on to the client computers in your organization will be displayed on each computer's respective Windows logon screen.

The recommended state for this setting is: `Enabled`.

Rationale:

A threat actor with access to the console (for example, someone with physical access or someone who is able to connect to the server through Remote Desktop Services) could view the name of the last user who logged on to the server. The threat actor could then try to guess the password, use a dictionary, or use a brute-force attack to try and log on.

Impact:

The name of the last user to successfully log on will not be displayed in the Windows logon screen.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:DontDisplayLas
tUserName
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Interactive logon: Don't display last signed-in
```

Note: In older versions of Microsoft Windows, this setting was named *Interactive logon: Do not display last user name*, but it was renamed starting with Windows Server 2019.

Default Value:

Disabled. (The name of the last user to log on is displayed in the Windows logon screen.)

References:

1. GRID: MS-00000072

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.10 Enforce Automatic Device Lockout on Portable End-User Devices Enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices, where supported. For laptops, do not allow more than 20 failed authentication attempts; for tablets and smartphones, no more than 10 failed authentication attempts. Example implementations include Microsoft® InTune Device Lock and Apple® Configuration Profile maxFailedAttempts.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Windows notices inactivity of a logon session, and if the amount of inactive time exceeds the inactivity limit, then the screen saver will run, locking the session.

The recommended state for this setting is: `900 or fewer second(s), but not 0`.

Note: A value of `0` does not conform to the benchmark as it disables the machine inactivity limit.

Rationale:

If a user forgets to lock their computer when they walk away it's possible that a passerby will hijack it.

Impact:

The screen saver will automatically activate when the computer has been unattended for the amount of time specified. The impact should be minimal since the screen saver is enabled by default.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a REG_DWORD value of `900` or less, but not `0`

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:
InactivityTimeoutSecs
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `900 or fewer seconds, but not 0`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Interactive logon: Machine inactivity limit
```

Default Value:

0 seconds. (There is no inactivity limit.)

References:

1. GRID: MS-00000074

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 Configure Automatic Session Locking on Enterprise Assets Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	●	●	●
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

2.3.7.4 Configure 'Interactive logon: Message text for users attempting to log on' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting specifies a text message that is display to users when they log on. Configure this setting in a manner that is consistent with the security and operational requirements of the organization.

Rationale:

Displaying a warning message before logon may help prevent malicious logins by a threat actor warning of the consequences of their misconduct.

It also helps to reinforce corporate policy by notifying employees of the appropriate policy during the logon process. This text is often used for legal reasons, for example, to warn users about the ramifications of misusing company information or to warn them that their actions may be audited.

Note: Any warning that is displayed should first be approved by the organization's legal and human resources representative.

Impact:

Users will have to acknowledge a dialog box containing the configured text before they can log on to the computer.

Note: Windows Vista and Windows XP Professional support logon banners that can exceed 512 characters in length and that can also contain carriage-return line-feed sequences. However, Windows 2000-based clients cannot interpret and display these messages. You must use a Windows 2000-based computer to create a logon message policy that applies to Windows 2000-based computers.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_SZ` value of `text`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:
LegalNoticeText
```

Remediation:

To establish the recommended configuration via GP, configure the following UI path to a value that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Interactive logon: Message text for users
attempting to log on
```

Default Value:

No message.

References:

1. GRID: MS-00000075

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.3.7.5 Configure 'Interactive logon: Message title for users attempting to log on' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting specifies the text displayed in the title bar of the window that is displayed to users when they log on to the system. Configure this setting in a manner that is consistent with the security and operational requirements of the organization.

Rationale:

Displaying a warning message before logon may help prevent malicious logins by a threat actor warning of the consequences of their misconduct.

It also helps to reinforce corporate policy by notifying employees of the appropriate policy during the logon process. This text is often used for legal reasons, for example, to warn users about the ramifications of misusing company information or to warn them that their actions may be audited.

Note: Any warning that is displayed should first be approved by the organization's legal and human resources representative.

Impact:

Users will have to acknowledge a dialog box with the configured title before they can log on to the computer.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_SZ` value of `text`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:
LegalNoticeCaption
```

Remediation:

To establish the recommended configuration via GP, configure the following UI path to a value that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Interactive logon: Message title for users
attempting to log on
```

Default Value:

No message.

References:

1. GRID: MS-00000076

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.3.7.6 Ensure 'Interactive logon: Number of previous logons to cache (in case domain controller is not available)' is set to '4 or fewer logon(s)' (MS only) (Automated)

Profile Applicability:

- Level 2 - Member Server

Description:

This policy setting determines whether a user can log on to a Windows domain using cached account information. Logon information for domain accounts can be cached locally to allow users to log on even if a Domain Controller cannot be contacted.

The recommended state for this setting is: `4 or fewer logon(s)`.

Note: The number that is assigned to this policy setting indicates the number of users whose logon information the computer will cache locally. If the number is set to 4, then the computer caches logon information for 4 users. When a 5th user logs on to the computer, the server overwrites the oldest cached logon session.

Rationale:

Users who access the computer console will have their logon credentials cached on that computer. A threat actor who is able to access the file system of the computer could locate this cached information and use a brute force attack to attempt to determine user passwords. To mitigate this type of attack, Windows encrypts the information and obscures its physical location.

Impact:

Users will be unable to log on to any computers if there is no Domain Controller available to authenticate them. Organizations may want to configure this value to `2` for end-user computers, especially for mobile users. A configuration value of `2` means that the user's logon information will still be in the cache, even if a member of the IT department has recently logged on to their computer to perform system maintenance. This method allows users to log on to their computers when they are not connected to the organization's network.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon:CachedLogonsCount
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `4 or fewer logon(s)`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Interactive logon: Number of previous logons to
cache (in case domain controller is not available)
```

Default Value:

On Windows Server 2008 (non-R2): 25 logons.

On Windows Server 2008 R2 or newer: 10 logons.

References:

1. GRID: MS-00000077

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.3.7.7 Ensure 'Interactive logon: Prompt user to change password before expiration' is set to 'between 5 and 14 days' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines how far in advance users are warned that their password will expire. It is recommended that you configure this policy setting to at least 5 days but no more than 14 days to sufficiently warn users when their passwords will expire.

The recommended state for this setting is: `between 5 and 14 days`.

Rationale:

It is recommended that user passwords be configured to expire periodically. Users will need to be warned that their passwords are going to expire, or they may inadvertently be locked out of the computer when their passwords expire. This condition could lead to confusion for users who access the network locally, or make it impossible for users to access your organization's network through dial-up or virtual private network (VPN) connections.

Impact:

Users will see a dialog box prompt to change their password each time that they log on to the domain when their password is configured to expire between 5 and 14 days.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value between `5` and `14`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon:PasswordExpiryWarning
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to a value `between 5 and 14 days`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Interactive logon: Prompt user to change password
before expiration
```

Default Value:

5 days.

References:

1. GRID: MS-00000078

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.3.7.8 Ensure 'Interactive logon: Require Domain Controller Authentication to unlock workstation' is set to 'Enabled' (MS only) (Automated)

Profile Applicability:

- Level 1 - Member Server

Description:

Logon information is required to unlock a locked computer. For domain accounts, this security setting determines whether it is necessary to contact a Domain Controller to unlock a computer.

The recommended state for this setting is: `Enabled`.

Rationale:

By default, the computer caches in memory the credentials of any users who are authenticated locally. The computer uses these cached credentials to authenticate anyone who attempts to unlock the console. When cached credentials are used, any changes that have recently been made to the account — such as user rights assignments, account lockout, or the account being disabled — are not considered or applied after the account is authenticated. User privileges are not updated, and (more importantly) disabled accounts are still able to unlock the console of the computer.

Impact:

When the console on a computer is locked, either by a user or automatically by a screen saver time-out, the console can only be unlocked if a Domain Controller is available to re-authenticate the domain account that is being used to unlock the computer. If no Domain Controller is available, the user cannot unlock the computer.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon:ForceUnlockLogon
```

Remediation:

To implement the recommended configuration via GP, set the following UI path to `Enabled:`

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Interactive logon: Require Domain Controller
Authentication to unlock workstation
```

Default Value:

Disabled. (Logon information confirmation with a Domain Controller is not required for a user to unlock the computer, and the user can unlock the computer using cached credentials, if they are present.)

References:

1. GRID: MS-00000079

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 Configure Automatic Session Locking on Enterprise Assets Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	●	●	●
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

2.3.7.9 Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or higher (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines what happens when the smart card for a logged-on user is removed from the smart card reader.

The recommended state for this setting is: `Lock Workstation`. Configuring this setting to `Force Logoff` or `Disconnect if a Remote Desktop Services session` also conforms to the benchmark.

Rationale:

Users sometimes forget to lock their workstations when they are away from them, allowing the possibility for threat actors to access their computers. If smart cards are used for authentication, the computer should automatically lock itself when the card is removed to ensure that only the user with the smart card is accessing resources using those credentials.

Impact:

If you select `Lock Workstation`, the workstation is locked when the smart card is removed, allowing users to leave the area, take their smart card with them, and still maintain a protected session.

If you select `Force Logoff`, users are automatically logged off when their smart card is removed.

If you select `Disconnect if a Remote Desktop Services session`, removal of the smart card disconnects the session without logging the users off. This allows the user to insert the smart card and resume the session later, or at another smart card reader-equipped computer, without having to log on again. If the session is local, this policy will function identically to `Lock Workstation`.

Enforcing this setting on computers used by people who must log onto multiple computers in order to perform their duties could be frustrating and lower productivity. For example, if network administrators are limited to a single account but need to log into several computers simultaneously in order to effectively manage the network enforcing this setting will limit them to logging onto one computer at a time. For these reasons it is recommended that this setting only be enforced on workstations used for purposes commonly associated with typical users such as document creation and email.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_SZ` value of `1`, `2`, or `3`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon:ScRemoveOption
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Lock Workstation`, `Force Logoff` or `Disconnect if a Remote Desktop Services session`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Smart card removal behavior
```

Default Value:

No action.

References:

1. GRID: MS-00000080

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 Configure Automatic Session Locking on Enterprise Assets Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	●	●	●
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

2.3.8 Microsoft network client

This section contains recommendations related to configuring the Microsoft network client.

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether packet signing is required by the Server Message Block (SMB) client component. SMB is the resource sharing protocol that is supported by many Windows operating systems. It is the basis of NetBIOS and many other protocols. SMB signatures authenticate both users and the servers that host the data. If either side fails the authentication process, data transmission will not take place.

The recommended state for this setting is: `Enabled`.

Rationale:

Session hijacking uses tools that allow threat actors who have access to the same network as the client or server to interrupt, end, or steal a session in progress. threat actors can potentially intercept and modify unsigned SMB packets and then modify the traffic and forward it so that the server might perform undesirable actions. Alternatively, the threat actors could pose as the server or client after legitimate authentication and gain unauthorized access to data.

Impact:

The Microsoft network client will not communicate with a Microsoft network server unless that server agrees to perform SMB packet signing.

Implementation of SMB signing may negatively affect performance, because each packet needs to be signed and verified. If these settings are enabled on a server that is performing multiple roles, such as a small business server that is serving as a Domain Controller, file server, print server, and application server performance may be substantially slowed. Additionally, if computers are configured to ignore all unsigned SMB communications, older applications and operating systems will not be able to connect. However, if SMB signing is completely disabled, computers will be vulnerable to session hijacking attacks.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters:RequireSe
curitySignature
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Microsoft network client: Digitally sign
communications (always)
```

Default Value:

Disabled. (SMB packet signing is negotiated between the client and server.)

References:

1. GRID: MS-00000081

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●

2.3.8.2 Ensure 'Microsoft network client: Send unencrypted password to third-party SMB servers' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether the SMB redirector will send plaintext passwords during authentication to third-party SMB servers that do not support password encryption.

It is recommended that you disable this policy setting unless there is a strong business case to enable it. If this policy setting is enabled, unencrypted passwords will be allowed across the network.

The recommended state for this setting is: `Disabled`.

Rationale:

If you enable this policy setting, the server can transmit passwords in plaintext across the network to other computers that offer SMB services, which is a significant security risk. These other computers may not use any of the SMB security mechanisms that are included with Windows Server 2003.

Impact:

None - this is the default behavior.

Some very old applications and operating systems such as MS-DOS, Windows for Workgroups 3.11, and Windows 95a may not be able to communicate with the servers in your organization by means of the SMB protocol.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters:EnablePlainTextPassword
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Microsoft network client: Send unencrypted password
to third-party SMB servers
```

Default Value:

Disabled. (Plaintext passwords will not be sent during authentication to third-party SMB servers that do not support password encryption.)

References:

1. GRID: MS-00000083

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	16.4 Encrypt or Hash all Authentication Credentials Encrypt or hash with a salt all authentication credentials when stored.		●	●

2.3.9 Microsoft network server

This section contains recommendations related to configuring the Microsoft network server.

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to specify the amount of continuous idle time that must pass in an SMB session before the session is suspended because of inactivity. Administrators can use this policy setting to control when a computer suspends an inactive SMB session. If client activity resumes, the session is automatically reestablished.

The maximum value is 99999, which is over 69 days; in effect, this value disables the setting.

The recommended state for this setting is: `15 or fewer minute(s)`.

Rationale:

Each SMB session consumes server resources, and numerous null sessions will slow the server or possibly cause it to fail. A threat actor could repeatedly establish SMB sessions until the server's SMB services become slow or unresponsive.

Impact:

There will be little impact because SMB sessions will be re-established automatically if the client resumes activity.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `15` or less.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters:
AutoDisconnect
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `15 or fewer minute(s)`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Microsoft network server: Amount of idle time
required before suspending session
```

Default Value:

15 minutes.

References:

1. GRID: MS-00000084

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether packet signing is required by the SMB server component. This setting should be enabled in a mixed environment to prevent downstream clients from using the workstation as a network server.

The recommended state for this setting is: `Enabled`.

Note: Certain policy settings must be configured in the **Default Domain Controller Policy** to ensure they are applied globally to domain controllers. Exercise caution when modifying these policies, as improper changes can negatively impact the environment.

Rationale:

Session hijacking uses tools that allow threat actors who have access to the same network as the client or server to interrupt, end, or steal a session in progress. threat actors can potentially intercept and modify unsigned SMB packets and then modify the traffic and forward it so that the server might perform undesirable actions. Alternatively, the threat actor could pose as the server or client after legitimate authentication and gain unauthorized access to data.

SMB is the resource sharing protocol that is supported by many Windows operating systems. It is the basis of NetBIOS and many other protocols. SMB signatures authenticate both users and the servers that host the data. If either side fails the authentication process, data transmission will not take place.

Impact:

The Microsoft network client will not communicate with a Microsoft network server unless that server agrees to perform SMB packet signing.

Implementation of SMB signing may negatively affect performance, because each packet needs to be signed and verified. If these settings are enabled on a server that is performing multiple roles, such as a small business server that is serving as a Domain Controller, file server, print server, and application server performance may be substantially slowed. Additionally, if computers are configured to ignore all unsigned SMB communications, older applications and operating systems will not be able to connect. However, if SMB signing is completely disabled, computers will be vulnerable to session hijacking attacks.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters:RequireSecurit
ySignature
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Microsoft network server: Digitally sign
communications (always)
```

Default Value:

On Member Servers: Disabled. (SMB packet signing is negotiated between the client and server.)

On Domain Controllers: Enabled. (The Microsoft network server will not communicate with a Microsoft network client unless that client agrees to perform SMB packet signing.)

References:

1. GRID: MS-00000085

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●

2.3.9.3 Ensure 'Microsoft network server: Disconnect clients when logon hours expire' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This security setting determines whether to disconnect users who are connected to the local computer outside their user account's valid logon hours. This setting affects the Server Message Block (SMB) component. If you enable this policy setting you should also enable *Network security: Force logoff when logon hours expire* (Rule 2.3.11.6).

If your organization configures logon hours for users, this policy setting is necessary to ensure they are effective.

The recommended state for this setting is: `Enabled`.

Rationale:

If your organization configures logon hours for users, then it makes sense to enable this policy setting. Otherwise, users who should not have access to network resources outside of their logon hours may actually be able to continue to use those resources with sessions that were established during allowed hours.

Impact:

None - this is the default behavior. If logon hours are not used in your organization, this policy setting will have no impact. If logon hours are used, existing user sessions will be forcibly terminated when their logon hours expire.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters:enableforcedlogoff
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Microsoft network server: Disconnect clients when
logon hours expire
```

Default Value:

Enabled. (Client sessions with the SMB service are forcibly disconnected when the client's logon hours expire.)

References:

1. GRID: MS-00000087

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	16.13 Alert on Account Login Behavior Deviation Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			●

2.3.9.4 Ensure 'Microsoft network server: Server SPN target name validation level' is set to 'Accept if provided by client' or higher (MS only) (Automated)

Profile Applicability:

- Level 1 - Member Server

Description:

This policy setting controls the level of validation a computer with shared folders or printers (the server) performs on the service principal name (SPN) that is provided by the client computer when it establishes a session using the server message block (SMB) protocol.

The server message block (SMB) protocol provides the basis for file and print sharing and other networking operations, such as remote Windows administration. The SMB protocol supports validating the SMB server service principal name (SPN) within the authentication blob provided by a SMB client to prevent a class of attacks against SMB servers referred to as SMB relay attacks. This setting will affect both SMB1 and SMB2.

The recommended state for this setting is: `Accept if provided by client`. Configuring this setting to `Required from client` also conforms to the benchmark.

Note: Since the release of the MS KB3161561 security patch, this setting can cause significant issues (such as replication problems, group policy editing issues and blue screen crashes) on Domain Controllers when used *simultaneously* with UNC path hardening (i.e. Rule 18.5.14.1). **CIS therefore recommends against deploying this setting on Domain Controllers.**

Rationale:

The identity of a computer can be spoofed to gain unauthorized access to network resources.

Impact:

All Windows operating systems support both a client-side SMB component and a server-side SMB component. This setting affects the server SMB behavior, and its implementation should be carefully evaluated and tested to prevent disruptions to file and print serving capabilities.

If configured to `Accept if provided by client`, the SMB server will accept and validate the SPN provided by the SMB client and allow a session to be established if it matches the SMB server's list of SPN's for itself. If the SPN does NOT match, the session request for that SMB client will be denied.

If configured to `Required from client`, the SMB client MUST send a SPN name in session setup, and the SPN name provided MUST match the SMB server that is being requested to establish a connection. If no SPN is provided by client, or the SPN provided does not match, the session is denied.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1` or `2`.

```
HKLM\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters:SMBServerNameHardeningLevel
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Accept if provided by client` or `Required from client`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Server SPN target name validation level
```

Default Value:

Off. (The SPN is not required or validated by the SMB server from a SMB client.)

References:

1. GRID: MS-00000088

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

2.3.10 Network access

This section contains recommendations related to network access.

2.3.10.1 Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether an anonymous user can request security identifier (SID) attributes for another user, or use a SID to obtain its corresponding user name.

The recommended state for this setting is: `Disabled`.

Note: Certain policy settings must be configured in the **Default Domain Policy** to ensure they are applied globally. Exercise caution when modifying these policies, as improper changes can negatively impact the environment.

Only policies that are configured by Microsoft by default should reside in these baseline GPOs. Any additional or custom policy settings should be implemented through separate GPOs rather than modifying the default policies.

Rationale:

If this policy setting is enabled, a user with local access could use the well-known Administrator's SID to learn the real name of the built-in Administrator account, even if it has been renamed. That person could then use the account name to initiate a password guessing attack.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Network access: Allow anonymous SID/Name
translation
```

Default Value:

Disabled. (An anonymous user cannot request the SID attribute for another user.)

References:

1. GRID: MS-00000091

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.3.10.2 Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts' is set to 'Enabled' (MS only) (Automated)

Profile Applicability:

- Level 1 - Member Server

Description:

This policy setting controls the ability of anonymous users to enumerate the 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`.

Note: This policy has no effect on Domain Controllers.

Rationale:

An unauthorized user could anonymously list account names and use the information to attempt to guess passwords or perform social engineering attacks. (Social engineering attacks try to deceive users in some way to obtain passwords or some form of security information.)

Impact:

None - this is the default behavior. It will be impossible to establish trusts with Windows NT 4.0-based domains. Also, client computers that run older versions of the Windows operating system such as Windows NT 3.51 and Windows 95 will experience problems when they try to use resources on the server.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SYSTEM\CurrentControlSet\Control\Lsa:RestrictAnonymousSAM
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Network access: Do not allow anonymous enumeration
of SAM accounts
```

Default Value:

Enabled. (Do not allow anonymous enumeration of SAM accounts. This option replaces Everyone with Authenticated Users in the security permissions for resources.)

References:

1. GRID: MS-00000093

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.3.10.3 Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled' (MS only) (Automated)

Profile Applicability:

- Level 1 - Member Server

Description:

This policy setting controls the ability of anonymous users to enumerate SAM accounts as well as shares. If you enable this policy setting, anonymous users will not be able to enumerate domain account user names and network share names on the systems in your environment.

The recommended state for this setting is: `Enabled`.

Note: This policy has no effect on Domain Controllers.

Rationale:

An unauthorized user could anonymously list account names and shared resources and use the information to attempt to guess passwords or perform social engineering attacks. (Social engineering attacks try to deceive users in some way to obtain passwords or some form of security information.)

Impact:

It will be impossible to establish trusts with Windows NT 4.0-based domains. Also, client computers that run older versions of the Windows operating system such as Windows NT 3.51 and Windows 95 will experience problems when they try to use resources on the server. Users who access file and print servers anonymously will be unable to list the shared network resources on those servers; the users will have to authenticate before they can view the lists of shared folders and printers. However, even with this policy setting enabled, anonymous users will have access to resources with permissions that explicitly include the built-in group, `ANONYMOUS LOGON`.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SYSTEM\CurrentControlSet\Control\Lsa:RestrictAnonymous
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Network access: Do not allow anonymous enumeration
of SAM accounts and shares
```

Default Value:

Disabled. (Allow anonymous enumeration of SAM accounts and shares. No additional permissions can be assigned by the administrator for anonymous connections to the computer. Anonymous connections will rely on default permissions.)

References:

1. GRID: MS-00000092

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

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

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting determines whether Credential Manager (formerly called Stored User Names and Passwords) saves passwords or credentials for later use when it gains domain authentication.

The recommended state for this setting is: `Enabled`.

Note: Changes to this setting will not take effect until Windows is restarted.

Rationale:

Passwords that are cached can be accessed by the user when logged on to the computer. Although this information may sound obvious, a problem can arise if the user unknowingly executes hostile code that reads the passwords and forwards them to another, unauthorized user.

Impact:

Credential Manager will not store passwords and credentials on the computer. Users will be forced to enter passwords whenever they log on to their Passport account or other network resources that aren't accessible to their domain account. Testing has shown that clients running Windows Vista or Windows Server 2008 will be unable to connect to Distributed File System (DFS) shares in untrusted domains. Enabling this setting also makes it impossible to specify alternate credentials for scheduled tasks, this can cause a variety of problems. For example, some third-party backup products will no longer work. This policy setting should have no impact on users who access network resources that are configured to allow access with their Active Directory-based domain account.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SYSTEM\CurrentControlSet\Control\Lsa:DisableDomainCreds
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Network access: Do not allow storage of passwords
and credentials for network authentication
```

Default Value:

Disabled. (Credential Manager will store passwords and credentials on the computer for later use for domain authentication.)

References:

1. GRID: MS-00000094

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.3.10.5 Ensure 'Network access: Let Everyone permissions apply to anonymous users' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines what additional permissions are assigned for anonymous connections to the computer.

The recommended state for this setting is: `Disabled`.

Rationale:

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

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SYSTEM\CurrentControlSet\Control\Lsa:EveryoneIncludesAnonymous
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Network access: Let Everyone permissions apply to
anonymous users
```

Default Value:

Disabled. (Anonymous users can only access those resources for which the built-in group `ANONYMOUS LOGON` has been explicitly given permission.)

References:

1. GRID: MS-00000095

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.3.10.6 Ensure 'Network access: Named Pipes that can be accessed anonymously' is configured (DC only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This policy setting determines which communication sessions, or pipes, will have attributes and permissions that allow anonymous access.

The recommended state for this setting is: `LSARPC, NETLOGON, SAMR` and (when the legacy *Computer Browser* service is enabled) `BROWSER`.

Note: A Member Server that holds the *Remote Desktop Services* Role with *Remote Desktop Licensing* Role Service will require a special exception to this recommendation, to allow the `HydraLSPipe` and `TermServLicensing` Named Pipes to be accessed anonymously.

Rationale:

Limiting named pipes that can be accessed anonymously will reduce the attack surface of the system.

Impact:

Null session access over named pipes will be disabled unless they are included, and applications that rely on this feature or on unauthenticated access to named pipes will no longer function. The `BROWSER` named pipe may need to be added to this list if the *Computer Browser* service is needed for supporting legacy components. The *Computer Browser* service is disabled by default.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_MULTI_SZ` value of `LSARPC,NETLOGON,SAMR`.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters:
NullSessionPipes
```

Remediation:

To establish the recommended configuration via GP, configure the following UI path:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Network access: Named Pipes that can be accessed
anonymously
```

Default Value:

None.

References:

1. GRID: MS-00000096

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.3.10.7 Ensure 'Network access: Named Pipes that can be accessed anonymously' is configured (MS only) (Automated)

Profile Applicability:

- Level 1 - Member Server

Description:

This policy setting determines which communication sessions, or pipes, will have attributes and permissions that allow anonymous access.

The recommended state for this setting is: `<blank>` (i.e. None), or (when the legacy *Computer Browser* service is enabled) `BROWSER`.

Note: A Member Server that holds the *Remote Desktop Services* Role with *Remote Desktop Licensing* Role Service will require a special exception to this recommendation, to allow the `HydraLSPipe` and `TermServLicensing` Named Pipes to be accessed anonymously.

Rationale:

Limiting named pipes that can be accessed anonymously will reduce the attack surface of the system.

Impact:

Null session access over named pipes will be disabled unless they are included, and applications that rely on this feature or on unauthenticated access to named pipes will no longer function. The `BROWSER` named pipe may need to be added to this list if the *Computer Browser* service is needed for supporting legacy components. The *Computer Browser* service is disabled by default.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_MULTI_SZ` value of `blank` (i.e. None) or `BROWSER` (when the legacy *Computer Browser* service is enabled).

```
HKLM\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters:NullSessionPipes
```

Remediation:

To establish the recommended configuration via GP, configure the following UI path:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Network access: Named Pipes that can be accessed
anonymously
```

Default Value:

None.

References:

1. GRID: MS-00000096

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.3.10.8 Ensure 'Network access: Remotely accessible registry paths' is configured (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines which registry paths will be accessible over the network, regardless of the users or groups listed in the access control list (ACL) of the `winreg` registry key.

The recommended state for this setting is:

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

Note: When this setting is configured, a list of one or more objects needs to be specified. The delimiter used when entering the list is a line feed or carriage return, that is, type the first object on the list, press the Enter button, type the next object, press Enter again, etc. The setting value is stored as a comma-delimited list in group policy security templates. It is also rendered as a comma-delimited list in Group Policy Editor's display pane and the Resultant Set of Policy console. It is recorded in the registry as a line-feed delimited list in a `REG_MULTI_SZ` value.

Rationale:

The registry is a database that contains computer configuration information, and much of the information is sensitive. A threat actor could use this information to facilitate unauthorized activities. To reduce the risk of such an attack, suitable ACLs are assigned throughout the registry to help protect it from access by unauthorized users.

Impact:

None - this is the default behavior.

However, if the default registry paths from the list of accessible ones is removed, remote management tools such as the Microsoft Baseline Security Analyzer and Microsoft Systems Management Server could fail, as they require remote access to the registry to properly monitor and manage computers.

Note: If remote access is needed, this setting must also enable the Remote Registry service.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a REG_MULTI_SZ value of System\CurrentControlSet\Control\ProductOptions,System\CurrentControlSet\Control\Server Applications,Software\Microsoft\Windows NT\CurrentVersion.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\Winreg\AllowedExactPaths:Machine
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to: System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Control\Server Applications Software\Microsoft\Windows NT\CurrentVersion

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Remotely accessible registry paths
```

Default Value:

System\CurrentControlSet\Control\ProductOptions

System\CurrentControlSet\Control\Server Applications

Software\Microsoft\Windows NT\CurrentVersion

References:

1. GRID: MS-00000098

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.3.10.9 Ensure 'Network access: Remotely accessible registry paths and sub-paths' is configured (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines which registry paths and sub-paths will be accessible over the network, regardless of the users or groups listed in the access control list (ACL) of the `winreg` registry key.

The recommended state for this setting is:

```
System\CurrentControlSet\Control\Print\Printers
System\CurrentControlSet\Services\Eventlog
Software\Microsoft\OLAP Server
Software\Microsoft\Windows NT\CurrentVersion\Print
Software\Microsoft\Windows NT\CurrentVersion\Windows
System\CurrentControlSet\Control\ContentIndex
System\CurrentControlSet\Control\Terminal Server
System\CurrentControlSet\Control\Terminal Server\UserConfig
System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration
Software\Microsoft\Windows NT\CurrentVersion\Perflib
System\CurrentControlSet\Services\SysmonLog
```

Note: When this setting is configured, a list of one or more objects needs to be specified. The delimiter used when entering the list is a line feed or carriage return, that is, type the first object on the list, press the Enter button, type the next object, press Enter again, etc. The setting value is stored as a comma-delimited list in group policy security templates. It is also rendered as a comma-delimited list in Group Policy Editor's display pane and the Resultant Set of Policy console. It is recorded in the registry as a line-feed delimited list in a `REG_MULTI_SZ` value.

Rationale:

The registry contains sensitive computer configuration information that could be used by a threat actor to facilitate unauthorized activities. The fact that the default ACLs assigned throughout the registry are fairly restrictive and help to protect the registry from access by unauthorized users reduces the risk of such an attack.

Impact:

None - this is the default behavior.

However, if the default registry paths from the list of accessible ones is removed, remote management tools such as the Microsoft Baseline Security Analyzer and Microsoft Systems Management Server could fail, as they require remote access to the registry to properly monitor and manage computers.

Note: If remote access is needed, this setting must also enable the Remote Registry service.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a REG_MULTI_SZ value of System\CurrentControlSet\Control\Print\Printers,System\CurrentControlSet\Services\Eventlog,Software\Microsoft\OLAP Server,Software\Microsoft\Windows NT\CurrentVersion\Print,Software\Microsoft\Windows NT\CurrentVersion\Windows,System\CurrentControlSet\Control\ContentIndex,System\CurrentControlSet\Control\Terminal Server,System\CurrentControlSet\Control\Terminal Server\UserConfig,System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration,Software\Microsoft\Windows NT\CurrentVersion\Perflib,System\CurrentControlSet\Services\SysmonLog, System\CurrentControlSet\Services\CertSvc,System\CurrentControlSet\Services\WINS.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\Winreg\AllowedPaths:Machine
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to: System\CurrentControlSet\Control\Print\Printers System\CurrentControlSet\Services\Eventlog Software\Microsoft\OLAP Server Software\Microsoft\Windows NT\CurrentVersion\Print Software\Microsoft\Windows NT\CurrentVersion\Windows System\CurrentControlSet\Control\ContentIndex System\CurrentControlSet\Control\Terminal Server System\CurrentControlSet\Control\Terminal Server\UserConfig System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration Software\Microsoft\Windows NT\CurrentVersion\Perflib System\CurrentControlSet\Services\SysmonLog

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Remotely accessible registry paths and sub-paths
```

When a server holds the *Active Directory Certificate Services* Role with *Certification Authority* Role Service, the above list should also include: System\CurrentControlSet\Services\CertSvc.

When a server has the *WINS Server* Feature installed, the above list should also include:

System\CurrentControlSet\Services\WINS

Default Value:

System\CurrentControlSet\Control\Print\Printers
System\CurrentControlSet\Services\Eventlog Software\Microsoft\OLAP Server
Software\Microsoft\Windows NT\CurrentVersion\Print Software\Microsoft\Windows NT\CurrentVersion\Windows System\CurrentControlSet\Control\ContentIndex
System\CurrentControlSet\Control\Terminal Server
System\CurrentControlSet\Control\Terminal Server\UserConfig
System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration
Software\Microsoft\Windows NT\CurrentVersion\Perflib
System\CurrentControlSet\Services\SysmonLog

References:

1. GRID: MS-00000097

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.3.10.10 Ensure 'Network access: Restrict anonymous access to Named Pipes and Shares' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

When enabled, this policy setting restricts anonymous access to only those shares and pipes that are named in the `Network access: Named pipes that can be accessed anonymously` and `Network access: Shares that can be accessed anonymously` settings. This policy setting controls null session access to shares on your computers by adding `RestrictNullSessAccess` with the value `1` in the

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters`

registry key. This registry value toggles null session shares on or off to control whether the server service restricts unauthenticated clients' access to named resources.

The recommended state for this setting is: `Enabled`.

Rationale:

Null sessions are a weakness that can be exploited through shares (including the default shares) on computers in your environment.

Impact:

None - this is the default behavior. If you choose to enable this setting and are supporting Windows NT 4.0 domains, you should check if any of the named pipes are required to maintain trust relationships between the domains, and then add the pipe to the **Network access: Named pipes that can be accessed anonymously** list:

- COMNAP: SNA session access
- COMNODE: SNA session access
- SQL\QUERY: SQL instance access
- SPOOLSS: Spooler service
- LLSRPC: License Logging service
- NETLOGON: Net Logon service
- LSARPC: LSA access
- SAMR: Remote access to SAM objects
- BROWSER: Computer Browser service

Previous to the release of Windows Server 2003 with Service Pack 1 (SP1) these named pipes were allowed anonymous access by default, but with the increased hardening in Windows Server 2003 with SP1 these pipes must be explicitly added if needed.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters:RestrictNullSe
ssAccess
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Network access: Restrict anonymous access to Named
Pipes and Shares
```

Default Value:

Enabled. (Anonymous access is restricted to shares and pipes listed in the `Network access: Named pipes that can be accessed anonymously` and `Network access: Shares that can be accessed anonymously` settings.)

References:

1. GRID: MS-00000099

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.3.10.11 Ensure 'Network access: Restrict clients allowed to make remote calls to SAM' is set to 'Administrators: Remote Access: Allow' (MS only) (Automated)

Profile Applicability:

- Level 1 - Member Server

Description:

This policy setting allows you to restrict remote RPC connections to SAM.

The recommended state for this setting is: `Administrators: Remote Access: Allow`.

Note: A Windows 10 v1607, Server 2016 or newer OS is required to access and set this value in Group Policy.

Note #2: This setting was originally only supported on Windows Server 2016 or newer, then support for it was added to Windows Server 2008 R2 or newer via the March 2017 security patches.

Note #3: If your organization is using Microsoft Defender for Identity (formerly Azure Advanced Threat Protection (Azure ATP)), the (organization-named) Defender for Identity Directory Service Account (DSA), will also need to be granted the same `Remote Access: Allow` permission. For more information on adding the service account please see Configure SAM-R to enable lateral movement path detection in Microsoft Defender for Identity | Microsoft Docs.

Rationale:

To ensure that an unauthorized user cannot anonymously list local account names or groups and use the information to attempt to guess passwords or perform social engineering attacks. (Social engineering attacks try to deceive users in some way to obtain passwords or some form of security information.)

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_SZ` value of `O:BAG:BAD:(A;;RC;;;BA)`.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa:restrictremotesam
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Administrators: Remote Access: Allow`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Network access: Restrict clients allowed to make
remote calls to SAM
```

Default Value:

Administrators: Remote Access: Allow.

References:

1. GRID: MS-00000100

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.3.10.12 Ensure 'Network access: Shares that can be accessed anonymously' is set to 'None' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines which network shares can be accessed by anonymous users. The default configuration for this policy setting has little effect because all users have to be authenticated before they can access shared resources on the server.

The recommended state for this setting is: `<blank>` (i.e. None).

Rationale:

It is very dangerous to allow any values in this setting. Any shares that are listed can be accessed by any network user, which could lead to the exposure or corruption of sensitive data.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_MULTI_SZ` value that is `blank` i.e. no value in key.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters:
NullSessionShares
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `<blank>` (i.e. None):

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Network access: Shares that can be accessed
anonymously
```

Default Value:

None. (Only authenticated users will have access to all shared resources on the server.)

References:

1. GRID: MS-00000101

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines how network logons that use local accounts are authenticated. The Classic option allows precise control over access to resources, including the ability to assign different types of access to different users for the same resource. The Guest only option allows you to treat all users equally. In this context, all users authenticate as Guest only to receive the same access level to a given resource.

The recommended state for this setting is: `Classic - local users authenticate as themselves`.

Note: This setting does not affect interactive logons that are performed remotely by using such services as Telnet or Remote Desktop Services (formerly called Terminal Services).

Rationale:

With the Guest only model, any user who can authenticate to your computer over the network does so with guest privileges, which probably means that they will not have write access to shared resources on that computer. Although this restriction does increase security, it makes it more difficult for authorized users to access shared resources on those computers because ACLs on those resources must include access control entries (ACEs) for the Guest account. With the Classic model, local accounts should be password protected. Otherwise, if Guest access is enabled, anyone can use those user accounts to access shared system resources.

Impact:

None - this is the default configuration for domain-joined computers.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SYSTEM\CurrentControlSet\Control\Lsa:ForceGuest
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Classic - local users authenticate as themselves`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Network access: Sharing and security model for
local accounts
```

Default Value:

On domain-joined computers: Classic - local users authenticate as themselves. (Network logons that use local account credentials authenticate by using those credentials.)

On stand-alone computers: Guest only - local users authenticate as Guest. (Network logons that use local accounts are automatically mapped to the Guest account.)

References:

1. GRID: MS-00000102

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.3.11 Network security

This section contains recommendations related to network security.

2.3.11.1 Ensure 'Network security: Allow Local System to use computer identity for NTLM' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether Local System services that use Negotiate when reverting to NTLM authentication can use the computer identity. This policy is supported on at least Windows 7 or Windows Server 2008 R2.

The recommended state for this setting is: `Enabled`.

Rationale:

When connecting to computers running versions of Windows earlier than Windows Vista or Windows Server 2008 (non-R2), services running as Local System and using SPNEGO (Negotiate) that revert to NTLM use the computer identity. In Windows 7, if you are connecting to a computer running Windows Server 2008 or Windows Vista, then a system service uses either the computer identity or a NULL session. When connecting with a NULL session, a system-generated session key is created, which provides no protection but allows applications to sign and encrypt data without errors. When connecting with the computer identity, both signing and encryption is supported in order to provide data protection.

Impact:

Services running as Local System that use Negotiate when reverting to NTLM authentication will use the computer identity. This might cause some authentication requests between Windows operating systems to fail and log an error.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SYSTEM\CurrentControlSet\Control\Lsa:UseMachineId
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Network security: Allow Local System to use
computer identity for NTLM
```

Default Value:

Disabled. (Services running as Local System that use Negotiate when reverting to NTLM authentication will authenticate anonymously.)

References:

1. GRID: MS-00000103

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.3.11.2 Ensure 'Network security: Allow LocalSystem NULL session fallback' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether NTLM is allowed to fall back to a NULL session when used with LocalSystem.

The recommended state for this setting is: `Disabled`.

Rationale:

NULL sessions are less secure because by definition they are unauthenticated.

Impact:

Any applications that require NULL sessions for LocalSystem will not work as designed.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0:AllowNullSessionFallback
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Network security: Allow LocalSystem NULL session
fallback
```

Default Value:

On Windows Server 2008 (non-R2): Enabled. (NTLM will be permitted to fall back to a NULL session when used with LocalSystem.)

On Windows Server 2008 R2 or newer: Disabled. (NTLM will not be permitted to fall back to a NULL session when used with LocalSystem.)

References:

1. GRID: MS-00000104

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.3.11.3 Ensure 'Network Security: Allow PKU2U authentication requests to this computer to use online identities' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This setting determines if online identities are able to authenticate to this computer.

The Public Key Cryptography Based User-to-User (PKU2U) protocol introduced in Windows 7 and Windows Server 2008 R2 is implemented as a security support provider (SSP). The SSP enables peer-to-peer authentication, particularly through the Windows 7 media and file sharing feature called HomeGroup, which permits sharing between computers that are not members of a domain.

With PKU2U, a new extension was introduced to the Negotiate authentication package, `Spnego.dll`. In previous versions of Windows, Negotiate decided whether to use Kerberos or NTLM for authentication. The extension SSP for Negotiate, `Negoexts.dll`, which is treated as an authentication protocol by Windows, supports Microsoft SSPs including PKU2U.

When computers are configured to accept authentication requests by using online IDs, `Negoexts.dll` calls the PKU2U SSP on the computer that is used to log on. The PKU2U SSP obtains a local certificate and exchanges the policy between the peer computers. When validated on the peer computer, the certificate within the metadata is sent to the logon peer for validation and associates the user's certificate to a security token and the logon process completes.

The recommended state for this setting is: `Disabled`.

Note: If a hybrid environment is used, and PKU2U is `Disabled`, Remote Desktop connections from a hybrid joined system to a hybrid joined system will fail.

Note #2: If the failover clustering role is installed, and PKU2U is `Disabled`, failover clustering will not function properly.

Rationale:

The PKU2U protocol is a peer-to-peer authentication protocol - authentication should be managed centrally in most managed networks.

Impact:

None - this is the default configuration for domain-joined computers.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SYSTEM\CurrentControlSet\Control\Lsa\pku2u:AllowOnlineID
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Network Security: Allow PKU2U authentication
requests to this computer to use online identities
```

Default Value:

Disabled. (Online identities will not to be allowed to authenticate to a domain-joined machine.)

References:

1. https://learn.microsoft.com/en-us/windows-server/get-started/whats-new-in-windows-server-2019#failover-clustering
2. GRID: MS-00000105

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

2.3.11.4 Ensure 'Network security: Configure encryption types allowed for Kerberos' is set to 'AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to set the encryption types that Kerberos is allowed to use.

The recommended state for this setting is: `AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types`.

Note: Some legacy applications and OSes may still require `RC4_HMAC_MD5` - we recommend you test in your environment and verify whether you can safely remove it.

Rationale:

The strength of each encryption algorithm varies from one to the next, choosing stronger algorithms will reduce the risk of compromise however doing so may cause issues when the computer attempts to authenticate with systems that do not support them.

Impact:

If not selected, the encryption type will not be allowed. This setting may affect compatibility with client computers or services and applications. Multiple selections are permitted.

Note: Some legacy applications and OSes may still require `RC4_HMAC_MD5` - we recommend you test in your environment and verify whether you can safely remove it.

Note #2: Windows Server 2008 (non-R2) and below allow DES for Kerberos by default, but later OS versions do not.

Note #3: Some prerequisites might need to be met on Domain Controllers to support Kerberos AES 128 and 256 bit encryption types, as well as enabling support for Kerberos AES 128 and 256 bit on user accounts (in account options) for this recommendation to work correctly.

Note #4: If your organization uses Azure Files, please note that Microsoft did not introduce AES 256 Kerberos encryption support for it until AD DS authentication module v0.2.2. Please see this link for more information: Troubleshoot Azure Files identity-based authentication and authorization issues (SMB) - Azure | Microsoft Learn

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `2147483640`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\
Kerberos\Parameters:SupportedEncryptionTypes
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Network security: Configure encryption types
allowed for Kerberos
```

Default Value:

RC4_HMAC_MD5, AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types.

References:

1. GRID: MS-00000106

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	14.4 Encrypt All Sensitive Information in Transit Encrypt all sensitive information in transit.		●	●
v7	18.5 Use Only Standardized and Extensively Reviewed Encryption Algorithms Use only standardized and extensively reviewed encryption algorithms.		●	●

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether the LAN Manager (LM) hash value for the new password is stored when the password is changed. The LAN Manager (LM) hash is a legacy 16-byte hash of a user's password used in older authentication protocols. Tis hash is stored on the local system and is known for its weak security.

The recommended state for this setting is: `Enabled`.

Note: Certain policy settings must be configured in the **Default Domain Policy** to ensure they are applied globally. Exercise caution when modifying these policies, as improper changes can negatively impact the environment.

Only policies that are configured by Microsoft by default should reside in these baseline GPOs. Any additional or custom policy settings should be implemented through separate GPOs rather than modifying the default policies.

Rationale:

The SAM file can be targeted by threat actors who seek access to username and password hashes. Such attacks use special tools to crack passwords, which can then be used to impersonate users and gain access to resources on your network. These types of attacks will not be prevented if you enable this policy setting, but it will be much more difficult for these types of attacks to succeed.

The LM hash is relatively weak and prone to attack compared to the cryptographically stronger Microsoft Windows NT hash. Since LM hashes are stored on the local computer in the security database, passwords can then be easily compromised if the database is attacked.

Impact:

None - this is the default behavior.

However, older operating systems and some third-party applications may fail when this policy setting is enabled. Also, note that the password will need to be changed on all accounts after this setting is enabled to gain the proper benefit.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SYSTEM\CurrentControlSet\Control\Lsa:NoLMHash
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Network security: Do not store LAN Manager hash
value on next password change
```

Default Value:

Enabled. (LAN Manager hash values are not stored when passwords are changed.)

References:

1. GRID: MS-00000107

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 Encrypt Sensitive Data at Rest Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		●	●
v7	16.4 Encrypt or Hash all Authentication Credentials Encrypt or hash with a salt all authentication credentials when stored.		●	●

2.3.11.6 Ensure 'Network security: Force logoff when logon hours expire' is set to 'Enabled' (Manual)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether to disconnect users who are connected to the local computer outside their user account's valid logon hours. This setting affects the Server Message Block (SMB) component. If you enable this policy setting you should also enable *Microsoft network server: Disconnect clients when logon hours expire* (Rule 2.3.9.4).

The recommended state for this setting is: `Enabled`.

Note: Certain policy settings must be configured in the **Default Domain Policy** to ensure they are applied globally. Exercise caution when modifying these policies, as improper changes can negatively impact the environment.

Only policies that are configured by Microsoft by default should reside in these baseline GPOs. Any additional or custom policy settings should be implemented through separate GPOs rather than modifying the default policies.

Rationale:

If this setting is disabled, a user could remain connected to the computer outside of their allotted logon hours.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`.

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Network security: Force logoff when logon hours
expire
```

Default Value:

Enabled. (When a user's logon time expires, client sessions with the SMB server will be forcibly disconnected. The user will be unable to log on to the computer until their next scheduled access time commences.)

References:

1. GRID: MS-00000108

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	16.13 Alert on Account Login Behavior Deviation Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			●

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines which challenge or response authentication protocol is used for network logons. This choice affects the level of authentication protocol used by clients, the level of session security negotiated, and the level of authentication accepted by servers.

LAN Manager (LM) is a family of early Microsoft client/server software (predating Windows NT) that allowed users to link personal computers together on a single network. LM network capabilities included transparent file and print sharing, user security features, and network administration tools. In Active Directory domains, the Kerberos protocol is the default authentication protocol. However, if the Kerberos protocol is not negotiated for some reason, Active Directory will use LM, NTLM, or NTLMv2. LAN Manager authentication includes the LM, NTLM, and NTLM version 2 (NTLMv2) variants, and is the protocol that is used to authenticate all Windows clients when they perform the following operations:

- Join a domain
- Authenticate between Active Directory forests
- Authenticate to down-level domains
- Authenticate to computers that do not run Windows 2000, Windows Server 2003, or Windows XP
- Authenticate to computers that are not in the domain

The recommended state for this setting is: `Send NTLMv2 response only. Refuse LM & NTLM`.

Rationale:

Windows 2000 and Windows XP clients were configured by default to send LM and NTLM authentication responses (Windows 95-based and Windows 98-based clients only send LM). The default settings in OSes predating Windows Vista / Windows Server 2008 (non-R2) allowed all clients to authenticate with servers and use their resources. However, this meant that LM responses - the weakest form of authentication response - were sent over the network, and it was potentially possible for threat actors to sniff that traffic to more easily reproduce the user's password.

The Windows 95, Windows 98, and Windows NT operating systems cannot use the Kerberos version 5 protocol for authentication. For this reason, in a Windows Server 2003 domain, these computers authenticate by default with both the LM and NTLM protocols for network authentication. A more secure authentication protocol can be forced for Windows 95, Windows 98, and Windows NT by using NTLMv2. For the logon process, NTLMv2 uses a secure channel to protect the authentication process. Even if NTLMv2 is used for older clients and servers, Windows-based clients and servers that are members of the domain will use the Kerberos authentication protocol to authenticate with Windows Server 2003 or newer Domain Controllers. For these reasons, it is strongly preferred to restrict the use of LM & NTLM (non-v2) as much as possible.

Impact:

Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it; Domain Controllers refuse LM and NTLM (accept only NTLMv2 authentication). Clients that do not support NTLMv2 authentication will not be able to authenticate in the domain and access domain resources by using LM and NTLM.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `5`.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa:LmCompatibilityLevel
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to: `Send NTLMv2 response only. Refuse LM & NTLM`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Network security: LAN Manager authentication level
```

Default Value:

Send NTLMv2 response only. (Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it; Domain Controllers accept LM, NTLM & NTLMv2 authentication.)

References:

1. GRID: MS-00000109

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	18.5 Use Only Standardized and Extensively Reviewed Encryption Algorithms Use only standardized and extensively reviewed encryption algorithms.		●	●

2.3.11.8 Ensure 'Network security: LDAP client signing requirements' is set to 'Negotiate signing' or higher (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines the level of data signing that is requested on behalf of clients that issue LDAP BIND requests.

The recommended state for this setting is: `Negotiate signing`. Configuring this setting to `Require signing` also conforms to the benchmark.

Note: This policy setting does not have any impact on LDAP simple bind (`ldap_simple_bind`) or LDAP simple bind through SSL (`ldap_simple_bind_s`). No Microsoft LDAP clients that are included with Windows XP Professional use `ldap_simple_bind` or `ldap_simple_bind_s` to communicate with a Domain Controller.

Rationale:

Unsigned network traffic is susceptible to man-in-the-middle attacks in which an intruder captures the packets between the client and server, modifies them, and then forwards them to the server. For an LDAP server, this susceptibility means that a threat actor could cause a server to make decisions that are based on false or altered data from the LDAP queries. To lower this risk a network, implement strong physical security measures to protect the network infrastructure. Also, this can make all types of man-in-the-middle attacks extremely difficult if require digital signatures on all network packets by means of IPsec authentication headers is required.

Impact:

None - this is the default behavior.

However, if the option to *require* LDAP signatures tis selected, then the client must also be configured. If the client is not configured, it will not be able to communicate with the server, which could cause many features to fail, including user authentication, Group Policy, and logon scripts, because the caller will be told that the LDAP BIND command request failed.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1` or `2`.

```
HKLM\SYSTEM\CurrentControlSet\Services\LDAP:LDAPClientIntegrity
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Negotiate signing` or `Require signing`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Network security: LDAP client signing requirements
```

Default Value:

Negotiate signing. (If Transport Layer Security/Secure Sockets Layer (TLS/SSL) has not been started, the LDAP BIND request is initiated with the LDAP data signing option set in addition to the caller-specified options. If TLS/SSL has been started, the LDAP BIND request is initiated with the caller-specified options.)

References:

1. GRID: MS-00000110

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	18.5 Use Only Standardized and Extensively Reviewed Encryption Algorithms Use only standardized and extensively reviewed encryption algorithms.		●	●

2.3.11.9 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' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines which behaviors are allowed by clients for applications using the NTLM Security Support Provider (SSP). The SSP Interface (SSPI) is used by applications that need authentication services. The setting does not modify how the authentication sequence works but instead require certain behaviors in applications that use the SSPI.

The recommended state for this setting is: `Require NTLMv2 session security, Require 128-bit encryption`.

Note: These values are dependent on the *Network security: LAN Manager Authentication Level* (Rule 2.3.11.7) security setting value.

Rationale:

Enable both options for this policy setting to help protect network traffic that uses the NTLM Security Support Provider (NTLM SSP) from being exposed or tampered with by a threat actor who has gained access to the same network. These options help protect against man-in-the-middle attacks.

Impact:

NTLM connections will fail if NTLMv2 protocol and strong encryption (128-bit) are not **both** negotiated. Client applications that are enforcing these settings will be unable to communicate with older servers that do not support them.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `537395200`.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0:NTLMMinClientSec
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Require NTLMv2 session security, Require 128-bit encryption`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Minimum session security for NTLM SSP based (including secure RPC) clients
```

Default Value:

On Windows Server 2008 (non-R2): No requirements.

On Windows Server 2008 R2 or newer: Require 128-bit encryption. (NTLM connections will fail if strong encryption (128-bit) is not negotiated.)

References:

1. GRID: MS-00000111

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	18.5 Use Only Standardized and Extensively Reviewed Encryption Algorithms Use only standardized and extensively reviewed encryption algorithms.		●	●

2.3.11.10 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' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines which behaviors are allowed by servers for applications using the NTLM Security Support Provider (SSP). The SSP Interface (SSPI) is used by applications that need authentication services. The setting does not modify how the authentication sequence works but instead require certain behaviors in applications that use the SSPI.

The recommended state for this setting is: `Require NTLMv2 session security, Require 128-bit encryption`.

Note: These values are dependent on the *Network security: LAN Manager Authentication Level* (Rule 2.3.11.7) security setting value.

Rationale:

Enable all of the options for this policy setting to help protect network traffic that uses the NTLM Security Support Provider (NTLM SSP) from being exposed or tampered with by a threat actor who has gained access to the same network. These options help protect against man-in-the-middle attacks.

Impact:

NTLM connections will fail if NTLMv2 protocol and strong encryption (128-bit) are not **both** negotiated. Server applications that are enforcing these settings will be unable to communicate with older servers that do not support them.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `537395200`.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0:NTLMMinServerSec
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Require NTLMv2 session security, Require 128-bit encryption`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Minimum session security for NTLM SSP based (including secure RPC) servers
```

Default Value:

On Windows Server 2008 (non-R2): No requirements.

On Windows Server 2008 R2 or newer: Require 128-bit encryption. (NTLM connections will fail if strong encryption (128-bit) is not negotiated.)

References:

1. GRID: MS-00000112

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	18.5 Use Only Standardized and Extensively Reviewed Encryption Algorithms Use only standardized and extensively reviewed encryption algorithms.		●	●

2.3.11.11 Ensure 'Network security: Restrict NTLM: Audit Incoming NTLM Traffic' is set to 'Enable auditing for all accounts' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows the auditing of incoming NTLM traffic. Events for this setting are recorded in the operational event log (e.g. Applications and Services Log\Microsoft\Windows\NTLM).

The recommended state for this setting is: `Enable auditing for all accounts`.

Rationale:

Auditing and monitoring NTLM traffic can assist in identifying systems using this outdated authentication protocol, so they can be remediated to using a more secure protocol, such as Kerberos. The log information gathered can also assist in forensic investigations after a malicious attack.

NTLM and NTLMv2 authentication is vulnerable to various attacks, including SMB relay, man-in-the-middle, and brute force attacks. Reducing and eliminating NTLM authentication in an environment reduces the risk of a threat actor gaining access to systems on the network.

Impact:

The event log will contain information on incoming NTLM authentication traffic.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `2`.

```
HKLM\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0:AuditReceivingNTLMTraffic
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enable auditing for all accounts`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Network security: Restrict NTLM: Audit Incoming
NTLM Traffic
```

Default Value:

Disabled. (Incoming NTLM traffic is not logged.)

References:

1. https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-restrict-ntlm-audit-incoming-ntlm-traffic
2. https://learn.microsoft.com/en-us/defender-for-identity/configure-windows-event-collection#event-id-8004
3. GRID: MS-00000113

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●

2.3.11.12 Ensure 'Network security: Restrict NTLM: Audit NTLM authentication in this domain' is set to 'Enable all' (DC only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This policy setting allows auditing of NTLM authentication within the domain from the Domain Controller.

The recommended state for this setting is: `Enable all`.

Note: This setting is specific to each Domain Controller and will only log authentications made to that Domain Controller.

Rationale:

Auditing and monitoring NTLM traffic can assist in identifying systems using this outdated authentication protocol, so they can be remediated to using a more secure protocol, such as Kerberos. The log information gathered can also assist in forensic investigations after a malicious attack.

NTLM and NTLMv2 authentication is vulnerable to various attacks, including SMB relay, man-in-the-middle, and brute force attacks. Reducing and eliminating NTLM authentication in an environment reduces the risk of a threat actor gaining access to systems on the network.

Impact:

The event log will contain information on NTLM authentication traffic made to that Domain Controller.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `7`.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters:AuditNTLMInDomain
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enable all`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Network security: Restrict NTLM: Audit NTLM
authentication in this domain
```

Default Value:

Disabled. (The domain controller will not log events for NTLM authentication in this domain.)

References:

1. https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-restrict-ntlm-audit-ntlm-authentication-in-this-domain
2. https://learn.microsoft.com/en-us/defender-for-identity/what-is
3. GRID: MS-00000114

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●

2.3.11.13 Ensure 'Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers' is set to 'Audit all' or higher (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows the auditing of outgoing NTLM traffic. Events for this setting are recorded in the operational event log (e.g. Applications and Services Log\Microsoft\Windows\NTLM).

The recommended state for this setting is: `Audit all`. Configuring this setting to `Deny All` also conforms to the benchmark.

Note: Configuring this setting to `Deny All` is more secure, however it could have a negative impact on applications that still require NTLM. Test carefully before implementing the `Deny All` value.

Rationale:

Auditing and monitoring NTLM traffic can assist in identifying systems using this outdated authentication protocol, so they can be remediated to using a more secure protocol, such as Kerberos. The log information gathered can also assist in forensic investigations after a malicious attack.

NTLM and NTLMv2 authentication is vulnerable to various attacks, including SMB relay, man-in-the-middle, and brute force attacks. Reducing and eliminating NTLM authentication in an environment reduces the risk of a threat actor gaining access to systems on the network.

Impact:

The event log will contain information on outgoing NTLM authentication traffic.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1` or `2`.

```
HKLM\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0:RestrictSendingNTLMTraffic
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Audit all` or `Deny All`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Network security: Restrict NTLM: Outgoing NTLM
traffic to remote servers
```

Default Value:

Allow all. (The client can authenticate to remote servers by using NTLM authentication.)

References:

1. https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-restrict-ntlm-audit-incoming-ntlm-traffic
2. https://learn.microsoft.com/en-us/defender-for-identity/configure-windows-event-collection#event-id-8004
3. GRID: MS-00000115

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●

2.3.12 Recovery console

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

2.3.13 Shutdown

This section contains recommendations related to the Windows shutdown functionality.

2.3.13.1 Ensure 'Shutdown: Allow system to be shut down without having to log on' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether a computer can be shut down when a user is not logged on. If this policy setting is enabled, the shutdown command is available on the Windows logon screen. It is recommended to disable this policy setting to restrict the ability to shut down the computer to users with credentials on the system.

The recommended state for this setting is: `Disabled`.

Note: In Server 2008 R2 and older versions, this setting had no impact on Remote Desktop (RDP) / Terminal Services sessions - it only affected the local console. However, Microsoft changed the behavior in Windows Server 2012 (non-R2) and above, where if set to Enabled, RDP sessions are also allowed to shut down or restart the server.

Rationale:

Users who can access the console locally could shut down the computer. Threat actors could also walk to the local console and restart the server, which would cause a temporary denial-of-service (DoS) condition. Threat actors could also shut down the server and leave all of its applications and services unavailable. As noted in the Description above, the DoS risk of enabling this setting dramatically increases in Windows Server 2012 (non-R2) and above, as even remote users could then shut down or restart the server from the logon screen of an RDP session.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:ShutdownWithou
tLogon
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\Shutdown: Allow system to be shut down without
having to log on
```

Default Value:

Disabled. (Operators will have to log on to servers to shut them down or restart them.)

References:

1. GRID: MS-00000116

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.3.14 System cryptography

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

2.3.15 System objects

This section contains recommendations related to system objects.

2.3.15.1 Ensure 'System objects: Require case insensitivity for non-Windows subsystems' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether case insensitivity is enforced for all subsystems. The Microsoft Win32 subsystem is case insensitive. However, the kernel supports case sensitivity for other subsystems, such as the Portable Operating System Interface for UNIX (POSIX). Because Windows is case insensitive (but the POSIX subsystem will support case sensitivity), failure to enforce this policy setting makes it possible for a user of the POSIX subsystem to create a file with the same name as another file by using mixed case to label it. Such a situation can block access to these files by another user who uses typical Win32 tools, because only one of the files will be available.

The recommended state for this setting is: `Enabled`.

Rationale:

Because Windows is case-insensitive but the POSIX subsystem will support case sensitivity, failure to enable this policy setting would make it possible for a user of that subsystem to create a file with the same name as another file but with a different mix of upper and lower case letters. Such a situation could potentially confuse users when they try to access such files from normal Win32 tools because only one of the files will be available.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SYSTEM\CurrentControlSet\Control\Session
Manager\Kernel:ObCaseInsensitive
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\System objects: Require case insensitivity for non-
Windows subsystems
```

Default Value:

Enabled. (All subsystems will be forced to observe case insensitivity. This configuration may confuse users who are familiar with any UNIX-based operating systems that is case-sensitive.)

References:

1. GRID: MS-00000118

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines the strength of the default discretionary access control list (DACL) for objects. Active Directory maintains a global list of shared system resources, such as DOS device names, mutexes, and semaphores. In this way, objects can be located and shared among processes. Each type of object is created with a default DACL that specifies who can access the objects and what permissions are granted.

The recommended state for this setting is: `Enabled`.

Rationale:

This setting determines the strength of the default DACL for objects. Windows maintains a global list of shared computer resources so that objects can be located and shared among processes. Each type of object is created with a default DACL that specifies who can access the objects and with what permissions.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SYSTEM\CurrentControlSet\Control\Session Manager:ProtectionMode
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\System objects: Strengthen default permissions of
internal system objects (e.g. Symbolic Links)
```

Default Value:

Enabled. (The default DACL is stronger, allowing users who are not administrators to read shared objects but not allowing these users to modify shared objects that they did not create.)

References:

1. GRID: MS-00000119

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.3.16 System settings

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

2.3.17 User Account Control

This section contains recommendations related to User Account Control.

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

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

The recommended state for this setting is: `Enabled`.

Rationale:

One of the risks that the User Account Control feature introduced with Windows Vista is trying to mitigate is that of malicious software running under elevated credentials without the user or administrator being aware of its activity. An attack vector for these programs was to discover the password of the account named "Administrator" because that user account was created for all installations of Windows. To address this risk, in Windows Vista or newer, the built-in Administrator account is now disabled by default. In a default installation of a new computer, accounts with administrative control over the computer are initially set up in one of two ways:

- If the computer is not joined to a domain, the first user account you create has the equivalent permissions as a local administrator.
- If the computer is joined to a domain, no local administrator accounts are created. The Enterprise or Domain Administrator must log on to the computer and create one if a local administrator account is warranted.

Once Windows is installed, the built-in Administrator account may be manually enabled, but we strongly recommend that this account remain disabled.

Impact:

The built-in Administrator account uses Admin Approval Mode. Users that log on using the local Administrator account will be prompted for consent whenever a program requests an elevation in privilege, just like any other user would.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:FilterAdministratorToken
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Admin Approval Mode for the Built-in Administrator account
```

Default Value:

Disabled. (The built-in Administrator account runs all applications with full administrative privilege.)

References:

1. GRID: MS-00000120

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	4.3 Ensure the Use of Dedicated Administrative Accounts Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	●	●	●

2.3.17.2 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 (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

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

The recommended state for this setting is: `Prompt for consent on the secure desktop`. Configuring this setting to `Prompt for credentials on the secure desktop` also conforms to the benchmark.

Rationale:

One of the risks that the UAC feature introduced with Windows Vista is trying to mitigate is that of malicious software running under elevated credentials without the user or administrator being aware of its activity. This setting raises awareness to the administrator of elevated privilege operations and permits the administrator to prevent a malicious program from elevating its privilege when the program attempts to do so.

Impact:

When an operation (including execution of a Windows binary) requires elevation of privilege, the user is prompted on the secure desktop to select either Permit or Deny. If the user selects Permit, the operation continues with the user's highest available privilege.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1` or`2`.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:ConsentPromptBehaviorAdmin
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Prompt for consent on the secure desktop` or `Prompt for credentials on the secure desktop`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\User Account Control: Behavior of the elevation
prompt for administrators in Admin Approval Mode
```

Default Value:

Prompt for consent for non-Windows binaries. (When an operation for a non-Microsoft application requires elevation of privilege, the user is prompted on the secure desktop to select either Permit or Deny. If the user selects Permit, the operation continues with the user's highest available privilege.)

References:

1. GRID: MS-00000121

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls the behavior of the elevation prompt for standard users.

The recommended state for this setting is: `Automatically deny elevation requests`.

Rationale:

One of the risks that the User Account Control feature introduced with Windows Vista is trying to mitigate is that of malicious programs running under elevated credentials without the user or administrator being aware of their activity. This setting raises awareness to the user that a program requires the use of elevated privilege operations and requires that the user be able to supply administrative credentials in order for the program to run.

Impact:

When an operation requires elevation of privilege, a configurable access denied error message is displayed. An enterprise that is running desktops as standard user may choose this setting to reduce help desk calls.

Note: With this setting configured as recommended, the default error message displayed when a user attempts to perform an operation or run a program requiring privilege elevation (without Administrator rights) is "*This program will not run. This program is blocked by group policy. For more information, contact your system administrator.*" Some users who are not used to seeing this message may believe that the operation or program they attempted to run is specifically blocked by group policy, as that is what the message seems to imply. This message may therefore result in user questions as to why that specific operation/program is blocked, when in fact, the problem is that they need to perform the operation or run the program with an Administrative account (or "Run as Administrator" if it *is* already an Administrator account), and they are not doing that.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:ConsentPromptBehaviorUser
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Automatically deny elevation requests:`

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Behavior of the elevation prompt for standard users
```

Default Value:

Prompt for credentials. (When an operation requires elevation of privilege, the user is prompted to enter an administrative user name and password. If the user enters valid credentials, the operation continues with the applicable privilege.)

References:

1. GRID: MS-00000122

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.3.17.4 Ensure 'User Account Control: Detect application installations and prompt for elevation' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls the behavior of application installation detection for the computer.

The recommended state for this setting is: `Enabled`.

Rationale:

Some malicious software will attempt to install itself after being given permission to run. For example, malicious software with a trusted application shell. The user may have given permission for the program to run because the program is trusted, but if they are then prompted for installation of an unknown component this provides another way of trapping the software before it can do damage

Impact:

When an application installation package is detected that requires elevation of privilege, the user is prompted to enter an administrative user name and password. If the user enters valid credentials, the operation continues with the applicable privilege.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:EnableInstalle
rDetection
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\User Account Control: Detect application
installations and prompt for elevation
```

Default Value:

Disabled. (Default for enterprise. Application installation packages are not detected and prompted for elevation.)

References:

1. GRID: MS-00000123

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls whether applications that request to run with a User Interface Accessibility (UIAccess) integrity level must reside in a secure location in the file system. Secure locations are limited to the following:

- `…\Program Files\`, including subfolders
- `…\Windows\System32\`
- `…\Program Files (x86)\`, including subfolders (for 64-bit versions of Windows)

Note: Windows enforces a public key infrastructure (PKI) signature check on any interactive application that requests to run with a UIAccess integrity level regardless of the state of this security setting.

The recommended state for this setting is: `Enabled`.

Rationale:

UIAccess Integrity allows an application to bypass User Interface Privilege Isolation (UIPI) restrictions when an application is elevated in privilege from a standard user to an administrator. This is required to support accessibility features such as screen readers that are transmitting user interfaces to alternative forms. A process that is started with UIAccess rights has the following abilities:

- To set the foreground window.
- To drive any application window using SendInput function.
- To use read input for all integrity levels using low-level hooks, raw input, GetKeyState, GetAsyncKeyState, and GetKeyboardInput.
- To set journal hooks.
- To uses AttachThreadInput to attach a thread to a higher integrity input queue.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:EnableSecureUIAPaths
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Only elevate UIAccess applications that are installed in secure locations
```

Default Value:

Enabled. (If an application resides in a secure location in the file system, it runs only with UIAccess integrity.)

References:

1. GRID: MS-00000124

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.3.17.6 Ensure 'User Account Control: Run all administrators in Admin Approval Mode' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls the behavior of all User Account Control (UAC) policy settings for the computer. If you change this policy setting, you must restart your computer.

The recommended state for this setting is: `Enabled`.

Note: If this policy setting is disabled, the Security Center notifies you that the overall security of the operating system has been reduced.

Rationale:

This is the setting that turns on or off UAC. If this setting is disabled, UAC will not be used and any security benefits and risk mitigations that are dependent on UAC will not be present on the system.

Impact:

None - this is the default behavior. Users and administrators will need to learn to work with UAC prompts and adjust their work habits to use least privilege operations.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:EnableLUA
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\User Account Control: Run all administrators in
Admin Approval Mode
```

Default Value:

Enabled. (Admin Approval Mode is enabled. This policy must be enabled and related UAC policy settings must also be set appropriately to allow the built-in Administrator account and all other users who are members of the Administrators group to run in Admin Approval Mode.)

References:

1. GRID: MS-00000125

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.3.17.7 Ensure 'User Account Control: Switch to the secure desktop when prompting for elevation' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls whether the elevation request prompt is displayed on the interactive user's desktop or the secure desktop.

The recommended state for this setting is: `Enabled`.

Rationale:

Standard elevation prompt dialog boxes can be spoofed, which may cause users to disclose their passwords to malicious software. The secure desktop presents a very distinct appearance when prompting for elevation, where the user desktop dims, and the elevation prompt UI is more prominent. This increases the likelihood that users who become accustomed to the secure desktop will recognize a spoofed elevation prompt dialog box and not fall for the trick.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:PromptOnSecure
Desktop
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\User Account Control: Switch to the secure desktop
when prompting for elevation
```

Default Value:

Enabled. (All elevation requests go to the secure desktop regardless of prompt behavior policy settings for administrators and standard users.)

References:

1. GRID: MS-00000126

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls whether application write failures are redirected to defined registry and file system locations. This policy setting mitigates applications that run as administrator and write run-time application data to:

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

The recommended state for this setting is: `Enabled`.

Rationale:

This setting reduces vulnerabilities by ensuring that legacy applications only write data to permitted locations.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:EnableVirtualization
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local
Policies\Security Options\User Account Control: Virtualize file and registry
write failures to per-user locations
```

Default Value:

Enabled. (Application write failures are redirected at run time to defined user locations for both the file system and registry.)

References:

1. GRID: MS-00000127

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

3 Event Log

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

4 Restricted Groups

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

5 System Services

This section contains recommendations for system services.

5.1 Ensure 'Print Spooler (Spooler)' is set to 'Disabled' (DC only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This service spools print jobs and handles interaction with printers.

The recommended state for this setting is: `Disabled`.

Rationale:

Disabling the Print Spooler (Spooler) service mitigates the PrintNightmare vulnerability (CVE-2021-34527) and other attacks against the service.

Impact:

Domain Controllers will not be able to prune published printers from Active Directory. By default, Domain Controllers prune printer objects from Active Directory if the computer that published them doesn't respond to contact requests.

Domain Controllers will not be able to act as a print server, sharing printers for clients.

Applications on and users logged in at Domain Controllers will not be able to print, including printing to files (such as Adobe Portable Document Format (PDF)) which uses the Print Spooler service.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `4`.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Spooler:Start
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to: `Disabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\System
Services\Print Spooler
```

Default Value:

Automatic

References:

1. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527
2. GRID: MS-00000145

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

5.2 Ensure 'Print Spooler (Spooler)' is set to 'Disabled' (MS only) (Automated)

Profile Applicability:

- Level 2 - Member Server

Description:

This service spools print jobs and handles interaction with printers.

The recommended state for this setting is: `Disabled`.

Rationale:

Disabling the Print Spooler (Spooler) service mitigates the PrintNightmare vulnerability (CVE-2021-34527) and other attacks against the service.

Impact:

Member Servers will not be able to act as a print server, sharing printers for clients.

Applications on and users logged in to Member Servers will not be able to print, including printing to files (such as Adobe Portable Document Format (PDF)) which uses the Print Spooler service.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `4`.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Spooler:Start
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to: `Disabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\System
Services\Print Spooler
```

Default Value:

Automatic

References:

1. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527
2. GRID: MS-00000145

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

6 Registry

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

7 File System

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

8 Wired Network (IEEE 802.3) Policies

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

9 Windows Defender Firewall with Advanced Security (formerly Windows Firewall with Advanced Security)

This section contains recommendations for configuring the Windows Firewall.

Note: In older versions of Microsoft Windows, this section was named *Windows Firewall with Advanced Security*, but it was renamed to *Windows Defender Firewall with Advanced Security* starting with the Server 2019 release.

9.1 Domain Profile

This section contains recommendations for the Domain Profile of the Windows Firewall.

9.1.1 Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls whether the built-in Domain Firewall state is enabled or disabled.

The recommended state for this setting is: `On (recommended)`.

Rationale:

If the firewall is turned off all traffic will be able to access the system, and a threat actor may be able to remotely exploit a weakness in a network service.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile:EnableFirewall
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `On (recommended)`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Defender Firewall with Advanced Security\Windows Defender Firewall with
Advanced Security\Windows Defender Firewall Properties\Domain
Profile\Firewall state
```

Default Value:

On (recommended). (The Windows Firewall with Advanced Security will be active in this profile.)

References:

1. GRID: MS-00000173

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

9.1.2 Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines the behavior for inbound connections that do not match an inbound firewall rule.

The recommended state for this setting is: `Block (default)`.

Rationale:

If the firewall allows all traffic to access the system, then a threat actor may be able to remotely exploit a weakness in a network service.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile:DefaultInbound
Action
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Block (default)`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Defender Firewall with Advanced Security\Windows Defender Firewall with
Advanced Security\Windows Defender Firewall Properties\Domain Profile\Inbound
connections
```

Default Value:

Block (default). (The Windows Firewall with Advanced Security will block all inbound connections that do not match an inbound firewall rule in this profile.)

References:

1. GRID: MS-00000174

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	11.2 Document Traffic Configuration Rules All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.		●	●

9.1.3 Ensure 'Windows Firewall: Domain: Settings: Display a notification' is set to 'No' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Select this option to have Windows Firewall with Advanced Security display notifications to the user when a program is blocked from receiving inbound connections.

The recommended state for this setting is: `No`.

Note: When the `Apply local firewall rules` setting is configured to `No`, it's recommended to also configure the `Display a notification setting` to `No`. Otherwise, users will continue to receive messages that ask if they want to unblock a restricted inbound connection, but the user's response will be ignored.

Rationale:

Firewall notifications can be complex and may confuse the end users, who would not be able to address the alert.

Impact:

Windows Firewall will not display a notification when a program is blocked from receiving inbound connections.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile:DisableNotifications
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to No:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Defender Firewall with Advanced Security\Windows Defender Firewall with
Advanced Security\Windows Defender Firewall Properties\Domain
Profile\Settings Customize\Display a notification
```

Default Value:

Yes. (Windows Firewall with Advanced Security will display a notification when a program is blocked from receiving inbound connections.)

References:

1. GRID: MS-00000175

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	11.2 Document Traffic Configuration Rules All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.		●	●

9.1.4 Ensure 'Windows Firewall: Domain: Logging: Name' is configured (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting is used to specify the path and name of the file in which Windows Firewall will write its log information.

The recommended state for this setting is: `configured`.

Example: `%SystemRoot%\System32\logfiles\firewall\domainfw.log`.

Rationale:

If Windows Firewall events are not recorded it may be difficult or impossible for Administrators to analyze system issues or unauthorized activities of threat actors.

Microsoft stores all firewall events as one file on the system (`pfirewall.log`). To improve logging, separate each firewall profile (domain, private, public) into its own distinct log file (`domainfw.log`, `privatefw.log`, `publicfw.log`) for better organization and identification of specific issues within each profile.

Impact:

The log file will be stored in the location and file specified by the organization.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_SZ` value of `<path>\<filename>.log`. Where `<path>` is the location and `<file>` is the log name specified by the organization.

```
HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\Logging:LogFil
ePath
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `<path>\<file name>.log`:

Where `<path>` is the location and `<file>` is the log name specified by the organization.

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Defender Firewall with Advanced Security\Windows Defender Firewall with
Advanced Security\Windows Defender Firewall Properties\Domain Profile\Logging
Customize\Name
```

Default Value:

`%SystemRoot%\System32\logfiles\firewall\pfirewall.log`

References:

1. GRID: MS-00000176
2. https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/best-practices-configuring
3. https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/configure-the-windows-firewall-log

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	11.2 Document Traffic Configuration Rules All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.		●	●

9.1.5 Ensure 'Windows Firewall: Domain: Logging: Size limit (KB)' is set to '16,384 KB or greater' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Use this option to specify the size limit of the file in which Windows Firewall will write its log information.

The recommended state for this setting is: `16,384 KB or greater`.

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of threat actors.

Impact:

The log file size will be limited to the specified size, old events will be overwritten by newer ones when the limit is reached.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `16384`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\
Logging:LogFileSize
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `16,384 KB or greater`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Defender Firewall with Advanced Security\Windows Defender Firewall with
Advanced Security\Windows Defender Firewall Properties\Domain Profile\Logging
Customize\Size limit (KB)
```

Default Value:

4,096 KB.

References:

1. GRID: MS-00000177

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	11.2 Document Traffic Configuration Rules All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.		●	●

9.1.6 Ensure 'Windows Firewall: Domain: Logging: Log dropped packets' is set to 'Yes' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Use this option to log when Windows Firewall with Advanced Security discards an inbound packet for any reason. The log records why and when the packet was dropped. Look for entries with the word `DROP` in the action column of the log.

The recommended state for this setting is: `Yes`.

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of threat actors.

Impact:

Information about dropped packets will be recorded in the firewall log file.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\Logging:LogDroppedPackets
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Yes`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows Defender Firewall with Advanced Security\Windows Defender Firewall with Advanced Security\Windows Defender Firewall Properties\Domain Profile\Logging Customize\Log dropped packets
```

Default Value:

No (default). (Information about dropped packets will not be recorded in the firewall log file.)

References:

1. GRID: MS-00000178

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v8	4.5 Implement and Manage a Firewall on End-User Devices Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	11.2 Document Traffic Configuration Rules All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.		●	●

9.1.7 Ensure 'Windows Firewall: Domain: Logging: Log successful connections' is set to 'Yes' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Use this option to log when Windows Firewall with Advanced Security allows an inbound connection. The log records why and when the connection was formed. Look for entries with the word `ALLOW` in the action column of the log.

The recommended state for this setting is: `Yes`.

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of threat actors.

Impact:

Information about successful connections will be recorded in the firewall log file.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\Logging:LogSuc
cessfulConnections
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Yes`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Defender Firewall with Advanced Security\Windows Defender Firewall with
Advanced Security\Windows Defender Firewall Properties\Domain Profile\Logging
Customize\Log successful connections
```

Default Value:

No (default). (Information about successful connections will not be recorded in the firewall log file.)

References:

1. GRID: MS-00000179

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	11.2 Document Traffic Configuration Rules All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.		●	●

9.2 Private Profile

This section contains recommendations for the Private Profile of the Windows Firewall.

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls whether the built-in Private Firewall state is enabled or disabled.

The recommended state for this setting is: `On (recommended)`.

Rationale:

If the firewall is turned off all traffic will be able to access the system, and a threat actor may be more easily able to remotely exploit a weakness in a network service.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\PrivateProfile:EnableFirewal
l
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `On (recommended)`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Defender Firewall with Advanced Security\Windows Defender Firewall with
Advanced Security\Windows Defender Firewall Properties\Private
Profile\Firewall state
```

Default Value:

On (recommended). (The Windows Firewall with Advanced Security will be active in this profile.)

References:

1. GRID: MS-00000180

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines the behavior for inbound connections that do not match an inbound firewall rule.

The recommended state for this setting is: `Block (default)`.

Rationale:

If the firewall allows all traffic to access the system, then a threat actor may be able to remotely exploit a weakness in a network service.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\PrivateProfile:DefaultInboun
dAction
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Block (default)`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Defender Firewall with Advanced Security\Windows Defender Firewall with
Advanced Security\Windows Defender Firewall Properties\Private
Profile\Inbound connections
```

Default Value:

Block (default). (The Windows Firewall with Advanced Security will block all inbound connections that do not match an inbound firewall rule in this profile.)

References:

1. GRID: MS-00000181

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	11.2 Document Traffic Configuration Rules All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.		●	●

9.2.3 Ensure 'Windows Firewall: Private: Settings: Display a notification' is set to 'No' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Select this option to have Windows Firewall with Advanced Security display notifications to the user when a program is blocked from receiving inbound connections.

The recommended state for this setting is: `No`.

Note: When the `Apply local firewall rules` setting is configured to `No`, it's recommended to also configure the `Display a notification` setting to `No`. Otherwise, users will continue to receive messages that ask if they want to unblock a restricted inbound connection, but the user's response will be ignored.

Rationale:

Firewall notifications can be complex and may confuse the end users, who would not be able to address the alert.

Impact:

Windows Firewall will not display a notification when a program is blocked from receiving inbound connections.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\PrivateProfile:DisableNotifi
cations
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to No:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Defender Firewall with Advanced Security\Windows Defender Firewall with
Advanced Security\Windows Defender Firewall Properties\Private
Profile\Settings Customize\Display a notification
```

Default Value:

Yes. (Windows Firewall with Advanced Security will display a notification when a program is blocked from receiving inbound connections.)

References:

1. GRID: MS-00000182

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	11.2 Document Traffic Configuration Rules All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.		●	●

9.2.4 Ensure 'Windows Firewall: Private: Logging: Name' is configured (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting is used to specify the path and name of the file in which Windows Firewall will write its log information.

The recommended state for this setting is: `configured`.

Example: `%SystemRoot%\System32\logfiles\firewall\privatefw.log`.

Rationale:

If Windows Firewall events are not recorded it may be difficult or impossible for Administrators to analyze system issues or unauthorized activities of threat actors.

Microsoft stores all firewall events as one file on the system (`pfirewall.log`). To improve logging, separate each firewall profile (domain, private, public) into its own distinct log file (`domainfw.log`, `privatefw.log`, `publicfw.log`) for better organization and identification of specific issues within each profile.

Impact:

The log file will be stored in the location and file specified by the organization.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_SZ` value of `<path>\<filename>.log`. Where `<path>` is the location and `<file>` is the log name specified by the organization.

```
HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\PrivateProfile\Logging:LogFi
lePath
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `<path>\<file name>.log`:

Where `<path>` is the location and `<file>` is the log name specified by the organization.

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Defender Firewall with Advanced Security\Windows Defender Firewall with
Advanced Security\Windows Defender Firewall Properties\Private
Profile\Logging Customize\Name
```

Default Value:

`%SystemRoot%\System32\logfiles\firewall\pfirewall.log`

References:

1. GRID: MS-00000183
2. https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/best-practices-configuring
3. https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/configure-the-windows-firewall-log

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	11.2 Document Traffic Configuration Rules All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.		●	●

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Use this option to specify the size limit of the file in which Windows Firewall will write its log information.

The recommended state for this setting is: `16,384 KB or greater`.

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of threat actors.

Impact:

The log file size will be limited to the specified size, old events will be overwritten by newer ones when the limit is reached.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `16384`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PrivateProfile
\Logging:LogFileSize
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `16,384 KB or greater`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Defender Firewall with Advanced Security\Windows Defender Firewall with
Advanced Security\Windows Defender Firewall Properties\Private
Profile\Logging Customize\Size limit (KB)
```

Default Value:

4,096 KB.

References:

1. GRID: MS-00000184

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	11.2 Document Traffic Configuration Rules All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.		●	●

9.2.6 Ensure 'Windows Firewall: Private: Logging: Log dropped packets' is set to 'Yes' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Use this option to log when Windows Firewall with Advanced Security discards an inbound packet for any reason. The log records why and when the packet was dropped. Look for entries with the word `DROP` in the action column of the log.

The recommended state for this setting is: `Yes`.

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities ofthreat actors.

Impact:

Information about dropped packets will be recorded in the firewall log file.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\PrivateProfile\Logging:LogDr
oppedPackets
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Yes`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Defender Firewall with Advanced Security\Windows Defender Firewall with
Advanced Security\Windows Defender Firewall Properties\Private
Profile\Logging Customize\Log dropped packets
```

Default Value:

No (default). (Information about dropped packets will not be recorded in the firewall log file.)

References:

1. GRID: MS-00000185

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	11.2 Document Traffic Configuration Rules All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.		●	●

9.2.7 Ensure 'Windows Firewall: Private: Logging: Log successful connections' is set to 'Yes' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Use this option to log when Windows Firewall with Advanced Security allows an inbound connection. The log records why and when the connection was formed. Look for entries with the word `ALLOW` in the action column of the log.

The recommended state for this setting is: `Yes`.

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of threat actors.

Impact:

Information about successful connections will be recorded in the firewall log file.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\PrivateProfile\Logging:LogSuccessfulConnections
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Yes`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows Defender Firewall with Advanced Security\Windows Defender Firewall with Advanced Security\Windows Defender Firewall Properties\Private Profile\Logging Customize\Log successful connections
```

Default Value:

No (default). (Information about successful connections will not be recorded in the firewall log file.)

References:

1. GRID: MS-00000186

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	11.2 Document Traffic Configuration Rules All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.		●	●

9.3 Public Profile

This section contains recommendations for the Public Profile of the Windows Firewall.

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls whether the built-in Public Firewall state is enabled or disabled.

The recommended state for this setting is: `On (recommended)`.

Rationale:

If the firewall is turned off all traffic will be able to access the system, and a threat actor may be able to remotely exploit a weakness in a network service.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile:EnableFirewall
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `On (recommended):`

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Defender Firewall with Advanced Security\Windows Defender Firewall with
Advanced Security\Windows Defender Firewall Properties\Public
Profile\Firewall state
```

Default Value:

On (recommended). (The Windows Firewall with Advanced Security will be active in this profile.)

References:

1. GRID: MS-00000187

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This setting determines the behavior for inbound connections that do not match an inbound firewall rule.

The recommended state for this setting is: `Block (default)`.

Rationale:

If the firewall allows all traffic to access the system, then a threat actor may be more easily able to remotely exploit a weakness in a network service.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile:DefaultInbound
Action
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Block (default)`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Defender Firewall with Advanced Security\Windows Defender Firewall with
Advanced Security\Windows Defender Firewall Properties\Public Profile\Inbound
connections
```

Default Value:

Block (default). (The Windows Firewall with Advanced Security will block all inbound connections that do not match an inbound firewall rule in this profile.)

References:

1. GRID: MS-00000188

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	11.2 Document Traffic Configuration Rules All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.		●	●

9.3.3 Ensure 'Windows Firewall: Public: Settings: Display a notification' is set to 'No' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Select this option to have Windows Firewall with Advanced Security display notifications to the user when a program is blocked from receiving inbound connections.

The recommended state for this setting is: `No`.

Rationale:

Some organizations may prefer to avoid alarming users when firewall rules block certain types of network activity. However, notifications can be helpful when troubleshooting network issues involving the firewall.

Impact:

Windows Firewall will not display a notification when a program is blocked from receiving inbound connections.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile:DisableNotific
ations
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to 'No':

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Defender Firewall with Advanced Security\Windows Defender Firewall with
Advanced Security\Windows Defender Firewall Properties\Public
Profile\Settings Customize\Display a notification
```

Default Value:

Yes. (Windows Firewall with Advanced Security will display a notification when a program is blocked from receiving inbound connections.)

References:

1. GRID: MS-00000189

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	11.2 Document Traffic Configuration Rules All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.		●	●

9.3.4 Ensure 'Windows Firewall: Public: Settings: Apply local firewall rules' is set to 'No' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This setting controls whether local administrators are allowed to create local firewall rules that apply together with firewall rules configured by Group Policy.

The recommended state for this setting is: `No`.

Note: When the `Apply local firewall rules` setting is configured to `No`, it's recommended to also configure the `Display a notification` setting to `No`. Otherwise, users will continue to receive messages that ask if they want to unblock a restricted inbound connection, but the user's response will be ignored.

Rationale:

When in the Public profile, there should be no special local firewall exceptions per computer. These settings should be managed by a centralized policy.

Impact:

Administrators can still create firewall rules, but the rules will not be applied.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile:AllowLocalPoli
cyMerge
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `No`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Defender Firewall with Advanced Security\Windows Defender Firewall with
Advanced Security\Windows Defender Firewall Properties\Public
Profile\Settings Customize\Apply local firewall rules
```

Default Value:

Yes (default). (Firewall rules created by administrators will be applied.)

References:

1. GRID: MS-00000190

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	11.2 Document Traffic Configuration Rules All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.		●	●

9.3.5 Ensure 'Windows Firewall: Public: Settings: Apply local connection security rules' is set to 'No' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This setting controls whether local administrators are allowed to create connection security rules that apply together with connection security rules configured by Group Policy.

The recommended state for this setting is: `No`.

Rationale:

Users with administrative privileges might create firewall rules that expose the system to remote attack.

Impact:

Administrators can still create local connection security rules, but the rules will not be applied.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile:AllowLocalIPse
cPolicyMerge
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `No`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Defender Firewall with Advanced Security\Windows Defender Firewall with
Advanced Security\Windows Defender Firewall Properties\Public
Profile\Settings Customize\Apply local connection security rules
```

Default Value:

Yes (default). (Local connection security rules created by administrators will be applied.)

References:

1. GRID: MS-00000191

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	11.2 Document Traffic Configuration Rules All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.		●	●

9.3.6 Ensure 'Windows Firewall: Public: Logging: Name' is configured (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting is used to specify the path and name of the file in which Windows Firewall will write its log information.

The recommended state for this setting is: `configured`.

Example: `%SystemRoot%\System32\logfiles\firewall\publicfw.log`.

Rationale:

If Windows Firewall events are not recorded it may be difficult or impossible for Administrators to analyze system issues or unauthorized activities of threat actors.

Microsoft stores all firewall events as one file on the system (`pfirewall.log`). To improve logging, separate each firewall profile (domain, private, public) into its own distinct log file (`domainfw.log`, `privatefw.log`, `publicfw.log`) for better organization and identification of specific issues within each profile.

Impact:

The log file will be stored in the location and file specified by the organization.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_SZ` value of `<path>\<filename>.log`. Where `<path>` is the location and `<file>` is the log name specified by the organization.

```
HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile\Logging:LogFil
ePath
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `<path>\<file name>.log`:

Where `<path>` is the location and `<file>` is the log name specified by the organization.

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Defender Firewall with Advanced Security\Windows Defender Firewall with
Advanced Security\Windows Defender Firewall Properties\Public Profile\Logging
Customize\Name
```

Default Value:

`%SystemRoot%\System32\logfiles\firewall\pfirewall.log`

References:

1. GRID: MS-00000192
2. https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/configure-the-windows-firewall-log
3. https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/best-practices-configuring

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	11.2 Document Traffic Configuration Rules All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.		●	●

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Use this option to specify the size limit of the file in which Windows Firewall will write its log information.

The recommended state for this setting is: `16,384 KB or greater`.

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of threat actors.

Impact:

The log file size will be limited to the specified size, old events will be overwritten by newer ones when the limit is reached.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `16384`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile\
Logging:LogFileSize
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `16,384 KB or greater`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Defender Firewall with Advanced Security\Windows Defender Firewall with
Advanced Security\Windows Defender Firewall Properties\Public Profile\Logging
Customize\Size limit (KB)
```

Default Value:

4,096 KB.

References:

1. GRID: MS-00000193

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	11.2 Document Traffic Configuration Rules All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.		●	●

9.3.8 Ensure 'Windows Firewall: Public: Logging: Log dropped packets' is set to 'Yes' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Use this option to log when Windows Firewall with Advanced Security discards an inbound packet for any reason. The log records why and when the packet was dropped. Look for entries with the word `DROP` in the action column of the log.

The recommended state for this setting is: `Yes`.

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of threat actors.

Impact:

Information about dropped packets will be recorded in the firewall log file.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile\Logging:LogDro
ppedPackets
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Yes`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows
Defender Firewall with Advanced Security\Windows Defender Firewall with
Advanced Security\Windows Defender Firewall Properties\Public Profile\Logging
Customize\Log dropped packets
```

Default Value:

No (default). (Information about dropped packets will not be recorded in the firewall log file.)

References:

1. GRID: MS-00000194

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	11.2 Document Traffic Configuration Rules All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.		●	●

9.3.9 Ensure 'Windows Firewall: Public: Logging: Log successful connections' is set to 'Yes' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Use this option to log when Windows Firewall with Advanced Security allows an inbound connection. The log records why and when the connection was formed. Look for entries with the word `ALLOW` in the action column of the log.

The recommended state for this setting is: `Yes`.

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of threat actors.

Impact:

Information about successful connections will be recorded in the firewall log file.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile\Logging:LogSuccessfulConnections
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Yes`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows Defender Firewall with Advanced Security\Windows Defender Firewall with Advanced Security\Windows Defender Firewall Properties\Public Profile\Logging Customize\Log successful connections
```

Default Value:

No (default). (Information about successful connections will not be recorded in the firewall log file.)

References:

1. GRID: MS-00000195

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	11.2 Document Traffic Configuration Rules All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.		●	●

10 Network List Manager Policies

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

11 Wireless Network (IEEE 802.11) Policies

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

12 Public Key Policies

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

13 Software Restriction Policies

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

14 Network Access Protection NAP Client Configuration

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

15 Application Control Policies

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

16 IP Security Policies

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

17 Advanced Audit Policy Configuration

This section contains recommendations for configuring the Windows audit facilities.

17.1 Account Logon

This section contains recommendations for configuring the Account Logon audit policy.

17.1.1 Ensure 'Audit Credential Validation' is set to 'Success and Failure' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports the results of validation tests on credentials submitted for a user account logon request. These events occur on the computer that is authoritative for the credentials. For domain accounts, the Domain Controller is authoritative, whereas for local accounts, the local computer is authoritative. In domain environments, most of the Account Logon events occur in the Security log of the Domain Controllers that are authoritative for the domain accounts. However, these events can occur on other computers in the organization when local accounts are used to log on. Events for this subcategory include:

- 4774: An account was mapped for logon.
- 4775: An account could not be mapped for logon.
- 4776: The Domain Controller attempted to validate the credentials for an account.
- 4777: The Domain Controller failed to validate the credentials for an account.

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

Rationale:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected.

Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Impact:

Advanced audit logging will generate additional events when this feature is enabled.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using `auditpol.exe`, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce923f-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Success and Failure`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Account Logon\Audit Credential
Validation
```

Default Value:

Success.

References:

1. GRID: MS-00000196

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●
v7	16.12 Monitor Attempts to Access Deactivated Accounts Monitor attempts to access deactivated accounts through audit logging.		●	●

17.1.2 Ensure 'Audit Kerberos Authentication Service' is set to 'Success and Failure' (DC Only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This subcategory reports the results of events generated after a Kerberos authentication TGT request. Kerberos is a distributed authentication service that allows a client running on behalf of a user to prove its identity to a server without sending data across the network.

- 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`.

Rationale:

If no audit settings are configured, or if audit settings are too lax on the computers in the organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Impact:

Advanced audit logging will generate additional events when this feature is enabled.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using `auditpol.exe`, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce9242-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Success and Failure`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Logon\Audit Kerberos Authentication Service
```

Default Value:

Success.

References:

1. GRID: MS-00000197

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

17.1.3 Ensure 'Audit Kerberos Service Ticket Operations' is set to 'Success and Failure' (DC Only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This subcategory reports the results of events generated by Kerberos authentication ticket-granting ticket (TGT) requests. Kerberos Service Ticket requests (TGS requests) occur as part of service use and access requests by specific accounts. Auditing these events will record the IP address from which the account requested TGS, when TGS was requested, and which encryption type was used.

- 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`.

Rationale:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Impact:

Advanced audit logging will generate additional events when this feature is enabled.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using `auditpol.exe`, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce9240-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Success and Failure`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Account Logon\Audit Kerberos
Service Ticket Operations
```

Default Value:

Success.

References:

1. GRID: MS-00000198

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

17.2 Account Management

This section contains recommendations for configuring the Account Management audit policy.

17.2.1 Ensure 'Audit Application Group Management' is set to 'Success and Failure' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to audit events generated by changes to application groups such as the following:

- Application group is created, changed, or deleted.
- Member is added or removed from an application group.

Application groups are utilized by Windows Authorization Manager, which is a flexible framework created by Microsoft for integrating role-based access control (RBAC) into applications. More information on Windows Authorization Manager is available at MSDN - Windows Authorization Manager.

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

Note: Although Microsoft "Deprecated" Windows Authorization Manager (AzMan) in Windows Server 2012 and 2012 R2, this feature still exists in the OS (unimproved), and therefore should still be audited.

Rationale:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Impact:

Advanced audit logging will generate additional events when this feature is enabled.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using `auditpol.exe`, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce9239-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Success and Failure`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Account Management\Audit
Application Group Management
```

Default Value:

No Auditing.

References:

1. GRID: MS-00000199

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

17.2.2 Ensure 'Audit Computer Account Management' is set to include 'Success' (DC only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This subcategory reports each event of computer account management, such as when a computer account is created, changed, deleted, renamed, disabled, or enabled. Events for this subcategory 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 to include: `Success`.

Rationale:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Impact:

Advanced audit logging will generate additional events when this feature is enabled.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using `auditpol.exe`, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce9236-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to include `Success`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Computer Account Management
```

Default Value:

Success.

References:

1. GRID: MS-00000200

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

17.2.3 Ensure 'Audit Distribution Group Management' is set to include 'Success' (DC only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This subcategory reports each event of distribution group management, such as when a distribution group is created, changed, or deleted or when a member is added to or removed from a distribution group. If you enable this Audit policy setting, administrators can track events to detect malicious, accidental, and authorized creation of group accounts. Events for this subcategory include:

- 4744: A security-disabled local group was created.
- 4745: A security-disabled local group was changed.
- 4746: A member was added to a security-disabled local group.
- 4747: A member was removed from a security-disabled local group.
- 4748: A security-disabled local group was deleted.
- 4749: A security-disabled global group was created.
- 4750: A security-disabled global group was changed.
- 4751: A member was added to a security-disabled global group.
- 4752: A member was removed from a security-disabled global group.
- 4753: A security-disabled global group was deleted.
- 4759: A security-disabled universal group was created.
- 4760: A security-disabled universal group was changed.
- 4761: A member was added to a security-disabled universal group.
- 4762: A member was removed from a security-disabled universal group.
- 4763: A security-disabled universal group was deleted.

The recommended state for this setting is to include: `Success`.

Rationale:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Impact:

Advanced audit logging will generate additional events when this feature is enabled.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using `auditpol.exe`, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce9238-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to include `Success`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Account Management\Audit
Distribution Group Management
```

Default Value:

No Auditing.

References:

1. GRID: MS-00000201

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

17.2.4 Ensure 'Audit Other Account Management Events' is set to include 'Success' (DC only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This subcategory reports other account management events. Events for this subcategory include:

- 4782: The password hash an account was accessed.
- 4793: The Password Policy Checking API was called.

The recommended state for this setting is to include: `Success`.

Rationale:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Impact:

Advanced audit logging will generate additional events when this feature is enabled.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using `auditpol.exe`, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce923a-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to include `Success`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Other Account Management Events
```

Default Value:

No Auditing.

References:

1. GRID: MS-00000202

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

17.2.5 Ensure 'Audit Security Group Management' is set to include 'Success' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports each event of security group management, such as when a security group is created, changed, or deleted or when a member is added to or removed from a security group. If you enable this Audit policy setting, administrators can track events to detect malicious, accidental, and authorized creation of security group accounts. Events for this subcategory include:

- 4727: A security-enabled global group was created.
- 4728: A member was added to a security-enabled global group.
- 4729: A member was removed from a security-enabled global group.
- 4730: A security-enabled global group was deleted.
- 4731: A security-enabled local group was created.
- 4732: A member was added to a security-enabled local group.
- 4733: A member was removed from a security-enabled local group.
- 4734: A security-enabled local group was deleted.
- 4735: A security-enabled local group was changed.
- 4737: A security-enabled global group was changed.
- 4754: A security-enabled universal group was created.
- 4755: A security-enabled universal group was changed.
- 4756: A member was added to a security-enabled universal group.
- 4757: A member was removed from a security-enabled universal group.
- 4758: A security-enabled universal group was deleted.
- 4764: A group's type was changed.

The recommended state for this setting is to include: `Success`.

Rationale:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Impact:

Advanced audit logging will generate additional events when this feature is enabled.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using `auditpol.exe`, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce9237-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to include `Success`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Account Management\Audit Security
Group Management
```

Default Value:

Success.

References:

1. GRID: MS-00000203

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●
v7	16.6 Maintain an Inventory of Accounts Maintain an inventory of all accounts organized by authentication system.		●	●

17.2.6 Ensure 'Audit User Account Management' is set to 'Success and Failure' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports each event of user account management, such as when a user account is created, changed, or deleted; a user account is renamed, disabled, or enabled; or a password is set or changed. If you enable this Audit policy setting, administrators can track events to detect malicious, accidental, and authorized creation of user accounts. Events for this subcategory include:

- 4720: A user account was created.
- 4722: A user account was enabled.
- 4723: An attempt was made to change an account's password.
- 4724: An attempt was made to reset an account's password.
- 4725: A user account was disabled.
- 4726: A user account was deleted.
- 4738: A user account was changed.
- 4740: A user account was locked out.
- 4765: SID History was added to an account.
- 4766: An attempt to add SID History to an account failed.
- 4767: A user account was unlocked.
- 4780: The ACL was set on accounts which are members of administrators groups.
- 4781: The name of an account was changed:
- 4794: An attempt was made to set the Directory Services Restore Mode.
- 5376: Credential Manager credentials were backed up.
- 5377: Credential Manager credentials were restored from a backup.

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

Rationale:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Impact:

Advanced audit logging will generate additional events when this feature is enabled.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using `auditpol.exe`, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce9235-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Success and Failure`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Account Management\Audit User
Account Management
```

Default Value:

Success.

References:

1. GRID: MS-00000204

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

17.3 Detailed Tracking

This section contains recommendations for configuring the Detailed Tracking audit policy.

17.3.1 Ensure 'Audit PNP Activity' is set to include 'Success' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to audit when plug and play detects an external device.

The recommended state for this setting is to include: `Success`.

Note: A Windows 10, Server 2016 or newer OS is required to access and set this value in Group Policy.

Rationale:

Enabling this setting will allow a user to audit events when a device is plugged into a system. This can help alert IT staff if unapproved devices are plugged in.

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Impact:

Advanced audit logging will generate additional events when this feature is enabled.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using `auditpol.exe`, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce9248-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to include `Success`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Detailed Tracking\Audit PNP Activity
```

Default Value:

No Auditing.

References:

1. GRID: MS-00000205

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

17.3.2 Ensure 'Audit Process Creation' is set to include 'Success' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports the creation of a process and the name of the program or user that created it. Events for this subcategory include:

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

Refer to Microsoft Knowledge Base article 947226: Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting.

The recommended state for this setting is to include: `Success`.

Rationale:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Impact:

Advanced audit logging will generate additional events when this feature is enabled.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using `auditpol.exe`, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce922b-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to include `Success`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Detailed Tracking\Audit Process
Creation
```

Default Value:

No Auditing.

References:

1. GRID: MS-00000206

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

17.4 DS Access

This section contains recommendations for configuring the Directory Services Access audit policy.

17.4.1 Ensure 'Audit Directory Service Access' is set to include 'Failure' (DC only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This subcategory reports when an AD DS object is accessed. Only objects with SACLs cause audit events to be generated, and only when they are accessed in a manner that matches their SACL. These events are similar to the directory service access events in previous versions of Windows Server. This subcategory applies only to Domain Controllers. Events for this subcategory include:

- 4662: An operation was performed on an object.

The recommended state for this setting is to include: `Failure`.

Rationale:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Impact:

Advanced audit logging will generate additional events when this feature is enabled.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using `auditpol.exe`, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce923b-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to include `Failure`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\DS Access\Audit Directory Service Access
```

Default Value:

Success.

References:

1. GRID: MS-00000207

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

17.4.2 Ensure 'Audit Directory Service Changes' is set to include 'Success' (DC only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This subcategory reports changes to objects in Active Directory Domain Services (AD DS). The types of changes that are reported are create, modify, move, and undelete operations that are performed on an object. DS Change auditing, where appropriate, indicates the old and new values of the changed properties of the objects that were changed. Only objects with SACLs cause audit events to be generated, and only when they are accessed in a manner that matches their SACL. Some objects and properties do not cause audit events to be generated due to settings on the object class in the schema. This subcategory applies only to Domain Controllers. Events for this subcategory 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 state for this setting is to include: `Success`.

Rationale:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Impact:

Advanced audit logging will generate additional events when this feature is enabled.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using `auditpol.exe`, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce923c-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to include `Success`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\DS Access\Audit Directory Service
Changes
```

Default Value:

No Auditing.

References:

1. GRID: MS-00000208

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

17.5 Logon/Logoff

This section contains recommendations for configuring the Logon/Logoff audit policy.

17.5.1 Ensure 'Audit Account Lockout' is set to include 'Failure' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports when a user's account is locked out as a result of too many failed logon attempts. Events for this subcategory include:

- 4625: An account failed to log on.

The recommended state for this setting is to include: `Failure`.

Rationale:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Impact:

Advanced audit logging will generate additional events when this feature is enabled.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using `auditpol.exe`, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce9217-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to include `Failure`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Account Lockout
```

Default Value:

Success.

References:

1. GRID: MS-00000209

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●
v7	16.6 Maintain an Inventory of Accounts Maintain an inventory of all accounts organized by authentication system.		●	●

17.5.2 Ensure 'Audit Group Membership' is set to include 'Success' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy allows you to audit the group membership information in the user's logon token. Events in this subcategory are generated on the computer on which a logon session is created. For an interactive logon, the security audit event is generated on the computer that the user logged on to. For a network logon, such as accessing a shared folder on the network, the security audit event is generated on the computer hosting the resource.

The recommended state for this setting is to include: `Success`.

Note: A Windows 10, Server 2016 or newer OS is required to access and set this value in Group Policy.

Rationale:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Impact:

Advanced audit logging will generate additional events when this feature is enabled.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using `auditpol.exe`, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce9249-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to include `Success`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Group Membership
```

Default Value:

No Auditing.

References:

1. GRID: MS-00000210

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

17.5.3 Ensure 'Audit Logoff' is set to include 'Success' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports when a user logs off from the system. These events occur on the accessed computer. For interactive logons, the generation of these events occurs on the computer that is logged on to. If a network logon takes place to access a share, these events generate on the computer that hosts the accessed resource. If you configure this setting to No auditing, it is difficult or impossible to determine which user has accessed or attempted to access organization computers. Events for this subcategory include:

- 4634: An account was logged off.
- 4647: User initiated logoff.

The recommended state for this setting is to include: `Success`.

Rationale:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Impact:

Advanced audit logging will generate additional events when this feature is enabled.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using `auditpol.exe`, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce9216-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to include `Success`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Logoff
```

Default Value:

Success.

References:

1. GRID: MS-00000211

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●
v7	16.13 Alert on Account Login Behavior Deviation Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			●

17.5.4 Ensure 'Audit Logon' is set to 'Success and Failure' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports when a user attempts to log on to the system. These events occur on the accessed computer. For interactive logons, the generation of these events occurs on the computer that is logged on to. If a network logon takes place to access a share, these events generate on the computer that hosts the accessed resource. If you configure this setting to No auditing, it is difficult or impossible to determine which user has accessed or attempted to access organization computers. Events for this subcategory include:

- 4624: An account was successfully logged on.
- 4625: An account failed to log on.
- 4648: A logon was attempted using explicit credentials.
- 4675: SIDs were filtered.

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

Rationale:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Impact:

Advanced audit logging will generate additional events when this feature is enabled.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using `auditpol.exe`, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce9215-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Success and Failure`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Logon
```

Default Value:

Success and Failure.

References:

1. GRID: MS-00000212

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●
v7	16.13 Alert on Account Login Behavior Deviation Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			●

17.5.5 Ensure 'Audit Other Logon/Logoff Events' is set to 'Success and Failure' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports other logon/logoff-related events, such as Remote Desktop Services session disconnects and reconnects, using RunAs to run processes under a different account, and locking and unlocking a workstation. Events for this subcategory include:

- 4649: A replay attack was detected.
- 4778: A session was reconnected to a Window Station.
- 4779: A session was disconnected from a Window Station.
- 4800: The workstation was locked.
- 4801: The workstation was unlocked.
- 4802: The screen saver was invoked.
- 4803: The screen saver was dismissed.
- 5378: The requested credentials delegation was disallowed by policy.
- 5632: A request was made to authenticate to a wireless network.
- 5633: A request was made to authenticate to a wired network.

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

Rationale:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Impact:

Advanced audit logging will generate additional events when this feature is enabled.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using `auditpol.exe`, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce921c-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Success and Failure`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Other
Logon/Logoff Events
```

Default Value:

No Auditing.

References:

1. GRID: MS-00000213

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●
v7	16.13 Alert on Account Login Behavior Deviation Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			●

17.5.6 Ensure 'Audit Special Logon' is set to include 'Success' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports when a special logon is used. A special logon is a logon that has administrator-equivalent privileges and can be used to elevate a process to a higher level. Events for this subcategory include:

- 4964: Special groups have been assigned to a new logon.

The recommended state for this setting is to include: `Success`.

Rationale:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Impact:

Advanced audit logging will generate additional events when this feature is enabled.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using `auditpol.exe`, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce921b-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to include `Success`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Special Logon
```

Default Value:

Success.

References:

1. GRID: MS-00000214

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●
v7	16.13 Alert on Account Login Behavior Deviation Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			●

17.6 Object Access

This section contains recommendations for configuring the Object Access audit policy.

17.6.1 Ensure 'Audit Detailed File Share' is set to include 'Failure' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory allows you to audit attempts to access files and folders on a shared folder. Events for this subcategory include:

- 5145: network share object was checked to see whether client can be granted desired access.

The recommended state for this setting is to include: `Failure`

Rationale:

Auditing the Failures will log which unauthorized users attempted (and failed) to get access to a file or folder on a network share on this computer, which could possibly be an indication of malicious intent.

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Impact:

Advanced audit logging will generate additional events when this feature is enabled.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using `auditpol.exe`, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce9244-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to include `Failure`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Object Access\Audit Detailed File
Share
```

Default Value:

No Auditing.

References:

1. GRID: MS-00000215

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

17.6.2 Ensure 'Audit File Share' is set to 'Success and Failure' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to audit attempts to access a shared folder.

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

Note: There are no system access control lists (SACLs) for shared folders. If this policy setting is enabled, access to all shared folders on the system is audited.

Rationale:

In an enterprise managed environment, it's important to track deletion, creation, modification, and access events for network shares. Any unusual file sharing activity may be useful in an investigation of potentially malicious activity.

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Impact:

Advanced audit logging will generate additional events when this feature is enabled.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using `auditpol.exe`, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce9224-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Success and Failure`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Object Access\Audit File Share
```

Default Value:

No Auditing.

References:

1. GRID: MS-00000216

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

17.6.3 Ensure 'Audit Other Object Access Events' is set to 'Success and Failure' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to audit events generated by the management of task scheduler jobs or COM+ objects.

For scheduler jobs, the following are audited:

- Job created.
- Job deleted.
- Job enabled.
- Job disabled.
- Job updated.

For COM+ objects, the following are audited:

- Catalog object added.
- Catalog object updated.
- Catalog object deleted.

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

Rationale:

The unexpected creation of scheduled tasks and COM+ objects could potentially be an indication of malicious activity. Since these types of actions are generally low volume, it may be useful to capture them in the audit logs for use during an investigation.

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Impact:

Advanced audit logging will generate additional events when this feature is enabled.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using `auditpol.exe`, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce9227-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Success and Failure`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Object Access\Audit Other Object
Access Events
```

Default Value:

No Auditing.

References:

1. GRID: MS-00000217

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

17.6.4 Ensure 'Audit Removable Storage' is set to 'Success and Failure' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to audit user attempts to access file system objects on a removable storage device. A security audit event is generated only for all objects for all types of access requested. If you configure this policy setting, an audit event is generated each time an account accesses a file system object on a removable storage. Success audits record successful attempts and Failure audits record unsuccessful attempts. If you do not configure this policy setting, no audit event is generated when an account accesses a file system object on a removable storage.

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

Note: A Windows 8.0, Server 2012 (non-R2) or newer OS is required to access and set this value in Group Policy.

Rationale:

Auditing removable storage may be useful when investigating an incident. For example, if an individual is suspected of copying sensitive information onto a USB drive.

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Impact:

Advanced audit logging will generate additional events when this feature is enabled.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using `auditpol.exe`, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce9245-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Success and Failure`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Object Access\Audit Removable
Storage
```

Default Value:

No Auditing.

References:

1. GRID: MS-00000218

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

17.7 Policy Change

This section contains recommendations for configuring the Policy Change audit policy.

17.7.1 Ensure 'Audit Audit Policy Change' is set to include 'Success' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports changes in audit policy including SACL changes. Events for this subcategory include:

- 4715: The audit policy (SACL) on an object was changed.
- 4719: System audit policy was changed.
- 4902: The Per-user audit policy table was created.
- 4904: An attempt was made to register a security event source.
- 4905: An attempt was made to unregister a security event source.
- 4906: The CrashOnAuditFail value has changed.
- 4907: Auditing settings on object were changed.
- 4908: Special Groups Logon table modified.
- 4912: Per User Audit Policy was changed.

The recommended state for this setting is include: `Success`.

Rationale:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Impact:

Advanced audit logging will generate additional events when this feature is enabled.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using `auditpol.exe`, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce922f-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to include `Success`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Policy Change\Audit Audit Policy
Change
```

Default Value:

Success.

References:

1. GRID: MS-00000219

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	5.5 Implement Automated Configuration Monitoring Systems Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

17.7.2 Ensure 'Audit Authentication Policy Change' is set to include 'Success' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports changes in authentication policy. Events for this subcategory include:

- 4706: A new trust was created to a domain.
- 4707: A trust to a domain was removed.
- 4713: Kerberos policy was changed.
- 4716: Trusted domain information was modified.
- 4717: System security access was granted to an account.
- 4718: System security access was removed from an account.
- 4739: Domain Policy was changed.
- 4864: A namespace collision was detected.
- 4865: A trusted forest information entry was added.
- 4866: A trusted forest information entry was removed.
- 4867: A trusted forest information entry was modified.

The recommended state for this setting is to include: `Success`.

Rationale:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Impact:

Advanced audit logging will generate additional events when this feature is enabled.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using `auditpol.exe`, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce9230-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to include `Success`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Policy Change\Audit Authentication
Policy Change
```

Default Value:

Success.

References:

1. GRID: MS-00000220

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	5.5 Implement Automated Configuration Monitoring Systems Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

17.7.3 Ensure 'Audit Authorization Policy Change' is set to include 'Success' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports changes in authorization policy. Events for this subcategory include:

- 4703: A user right was adjusted.
- 4704: A user right was assigned.
- 4705: A user right was removed.
- 4670: Permissions on an object were changed.
- 4911: Resource attributes of the object were changed.
- 4913: Central Access Policy on the object was changed.

The recommended state for this setting is to include: `Success`.

Rationale:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Impact:

Advanced audit logging will generate additional events when this feature is enabled.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using `auditpol.exe`, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce9231-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to include `Success`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Policy Change\Audit Authorization
Policy Change
```

Default Value:

Success.

References:

1. GRID: MS-00000221

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	5.5 Implement Automated Configuration Monitoring Systems Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

17.7.4 Ensure 'Audit MPSSVC Rule-Level Policy Change' is set to 'Success and Failure' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory determines whether the operating system generates audit events when changes are made to policy rules for the Microsoft Protection Service (MPSSVC.exe). Events for this subcategory include:

- 4944: The following policy was active when the Windows Firewall started.
- 4945: A rule was listed when the Windows Firewall started.
- 4946: A change has been made to Windows Firewall exception list. A rule was added.
- 4947: A change has been made to Windows Firewall exception list. A rule was modified.
- 4948: A change has been made to Windows Firewall exception list. A rule was deleted.
- 4949: Windows Firewall settings were restored to the default values.
- 4950: A Windows Firewall setting has changed.
- 4951: A rule has been ignored because its major version number was not recognized by Windows Firewall.
- 4952: Parts of a rule have been ignored because its minor version number was not recognized by Windows Firewall. The other parts of the rule will be enforced.
- 4953: A rule has been ignored by Windows Firewall because it could not parse the rule.
- 4954: Windows Firewall Group Policy settings have changed. The new settings have been applied.
- 4956: Windows Firewall has changed the active profile.
- 4957: Windows Firewall did not apply the following rule.
- 4958: Windows Firewall did not apply the following rule because the rule referred to items not configured on this computer.

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

Rationale:

Changes to firewall rules are important for understanding the security state of the computer and how well it is protected against network attacks.

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Impact:

Advanced audit logging will generate additional events when this feature is enabled.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using `auditpol.exe`, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce9232-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Success and Failure`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Policy Change\Audit MPSSVC Rule-
Level Policy Change
```

Default Value:

No Auditing.

References:

1. GRID: MS-00000222

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

17.7.5 Ensure 'Audit Other Policy Change Events' is set to include 'Failure' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory contains events about EFS Data Recovery Agent policy changes, changes in Windows Filtering Platform filter, status on Security policy settings updates for local Group Policy settings, Central Access Policy changes, and detailed troubleshooting events for Cryptographic Next Generation (CNG) operations.

- 5063: A cryptographic provider operation was attempted.
- 5064: A cryptographic context operation was attempted.
- 5065: A cryptographic context modification was attempted.
- 5066: A cryptographic function operation was attempted.
- 5067: A cryptographic function modification was attempted.
- 5068: A cryptographic function provider operation was attempted.
- 5069: A cryptographic function property operation was attempted.
- 5070: A cryptographic function property modification was attempted.
- 6145: One or more errors occurred while processing security policy in the group policy objects.

The recommended state for this setting is to include: `Failure`.

Rationale:

This setting can help detect errors in applied Security settings which came from Group Policy, and failure events related to Cryptographic Next Generation (CNG) functions.

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Impact:

Advanced audit logging will generate additional events when this feature is enabled.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using `auditpol.exe`, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce9234-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to include `Failure`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Policy Change\Audit Other Policy
Change Events
```

Default Value:

No Auditing.

References:

1. GRID: MS-00000223

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

17.8 Privilege Use

This section contains recommendations for configuring the Privilege Use audit policy.

17.8.1 Ensure 'Audit Sensitive Privilege Use' is set to 'Success' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports when a user account or service uses a sensitive privilege. A sensitive privilege includes the following user rights:

- Act as part of the operating system
- Back up files and directories
- Create a token object
- Debug programs
- Enable computer and user accounts to be trusted for delegation
- Generate security audits
- Impersonate a client after authentication
- Load and unload device drivers
- Manage auditing and security log
- Modify firmware environment values
- Replace a process-level token
- Restore files and directories
- Take ownership of files or other objects

Auditing this subcategory will create a high volume of events. Events for this subcategory include:

- 4672: Special privileges assigned to new logon.
- 4673: A privileged service was called.
- 4674: An operation was attempted on a privileged object.

The recommended state for this setting is: `Success`.

Rationale:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Impact:

Advanced audit logging will generate additional events when this feature is enabled.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using `auditpol.exe`, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce9228-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Success`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\Privilege Use\Audit Sensitive
Privilege Use
```

Default Value:

No Auditing.

References:

1. GRID: MS-00000224

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

17.9 System

This section contains recommendations for configuring the System audit policy.

17.9.1 Ensure 'Audit IPsec Driver' is set to 'Success and Failure' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports on the activities of the Internet Protocol security (IPsec) driver. Events for this subcategory include:

- 4960: IPsec dropped an inbound packet that failed an integrity check. If this problem persists, it could indicate a network issue or that packets are being modified in transit to this computer. Verify that the packets sent from the remote computer are the same as those received by this computer. This error might also indicate interoperability problems with other IPsec implementations.
- 4961: IPsec dropped an inbound packet that failed a replay check. If this problem persists, it could indicate a replay attack against this computer.
- 4962: IPsec dropped an inbound packet that failed a replay check. The inbound packet had too low a sequence number to ensure it was not a replay.
- 4963: IPsec dropped an inbound clear text packet that should have been secured. This is usually due to the remote computer changing its IPsec policy without informing this computer. This could also be a spoofing attack attempt.
- 4965: IPsec received a packet from a remote computer with an incorrect Security Parameter Index (SPI). This is usually caused by malfunctioning hardware that is corrupting packets. If these errors persist, verify that the packets sent from the remote computer are the same as those received by this computer. This error may also indicate interoperability problems with other IPsec implementations. In that case, if connectivity is not impeded, then these events can be ignored.
- 5478: IPsec Services has started successfully.
- 5479: IPsec Services has been shut down successfully. The shutdown of IPsec Services can put the computer at greater risk of network attack or expose the computer to potential security risks.
- 5480: IPsec Services failed to get the complete list of network interfaces on the computer. This poses a potential security risk because some of the network interfaces may not get the protection provided by the applied IPsec filters. Use the IP Security Monitor snap-in to diagnose the problem.
- 5483: IPsec Services failed to initialize RPC server. IPsec Services could not be started.
- 5484: IPsec Services has experienced a critical failure and has been shut down. The shutdown of IPsec Services can put the computer at greater risk of network attack or expose the computer to potential security risks.
- 5485: IPsec Services failed to process some IPsec filters on a plug-and-play event for network interfaces. This poses a potential security risk because some

of the network interfaces may not get the protection provided by the applied IPsec filters. Use the IP Security Monitor snap-in to diagnose the problem.

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

Rationale:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Impact:

Advanced audit logging will generate additional events when this feature is enabled.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using `auditpol.exe`, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce9213-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Success and Failure`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\System\Audit IPsec Driver
```

Default Value:

No Auditing.

References:

1. GRID: MS-00000225

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

17.9.2 Ensure 'Audit Other System Events' is set to 'Success and Failure' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports on other system events. Events for this subcategory include:

- 5024: The Windows Firewall Service has started successfully.
- 5025: The Windows Firewall Service has been stopped.
- 5027: The Windows Firewall Service was unable to retrieve the security policy from the local storage. The service will continue enforcing the current policy.
- 5028: The Windows Firewall Service was unable to parse the new security policy. The service will continue with currently enforced policy.
- 5029: The Windows Firewall Service failed to initialize the driver. The service will continue to enforce the current policy.
- 5030: The Windows Firewall Service failed to start.
- 5032: Windows Firewall was unable to notify the user that it blocked an application from accepting incoming connections on the network.
- 5033: The Windows Firewall Driver has started successfully.
- 5034: The Windows Firewall Driver has been stopped.
- 5035: The Windows Firewall Driver failed to start.
- 5037: The Windows Firewall Driver detected critical runtime error. Terminating.
- 5058: Key file operation.
- 5059: Key migration operation.

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

Rationale:

Capturing these audit events may be useful for identifying when the Windows Firewall is not performing as expected.

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Impact:

Advanced audit logging will generate additional events when this feature is enabled.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using `auditpol.exe`, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce9214-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Success and Failure`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\System\Audit Other System Events
```

Default Value:

Success and Failure.

References:

1. GRID: MS-00000226

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

17.9.3 Ensure 'Audit Security State Change' is set to include 'Success' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports changes in security state of the system, such as when the security subsystem starts and stops. Events for this subcategory include:

- 4608: Windows is starting up.
- 4609: Windows is shutting down.
- 4616: The system time was changed.
- 4621: Administrator recovered system from CrashOnAuditFail. Users who are not administrators will now be allowed to log on. Some auditable activity might not have been recorded.

The recommended state for this setting is to include: `Success`.

Rationale:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Impact:

Advanced audit logging will generate additional events when this feature is enabled.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using `auditpol.exe`, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce9210-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to include `Success`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\System\Audit Security State Change
```

Default Value:

Success.

References:

1. GRID: MS-00000227

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

17.9.4 Ensure 'Audit Security System Extension' is set to include 'Success' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports the loading of extension code such as authentication packages by the security subsystem. Events for this subcategory include:

- 4610: An authentication package has been loaded by the Local Security Authority.
- 4611: A trusted logon process has been registered with the Local Security Authority.
- 4614: A notification package has been loaded by the Security Account Manager.
- 4622: A security package has been loaded by the Local Security Authority.
- 4697: A service was installed in the system.

The recommended state for this setting is to include: `Success`.

Rationale:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Impact:

Advanced audit logging will generate additional events when this feature is enabled.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using `auditpol.exe`, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce9211-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to include `Success`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\System\Audit Security System
Extension
```

Default Value:

No Auditing.

References:

1. GRID: MS-00000228

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

17.9.5 Ensure 'Audit System Integrity' is set to 'Success and Failure' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This subcategory reports on violations of integrity of the security subsystem. Events for this subcategory include:

- 4612: Internal resources allocated for the queuing of audit messages have been exhausted, leading to the loss of some audits.
- 4615: Invalid use of LPC port.
- 4618: A monitored security event pattern has occurred.
- 4816: RPC detected an integrity violation while decrypting an incoming message.
- 5038: Code integrity determined that the image hash of a file is not valid. The file could be corrupt due to unauthorized modification or the invalid hash could indicate a potential disk device error.
- 5056: A cryptographic self test was performed.
- 5057: A cryptographic primitive operation failed.
- 5060: Verification operation failed.
- 5061: Cryptographic operation.
- 5062: A kernel-mode cryptographic self test was performed.

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

Rationale:

If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected, or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Impact:

Advanced audit logging will generate additional events when this feature is enabled.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

OR

To audit the system using `auditpol.exe`, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"{0cce9212-69ae-11d9-bed3-505054503030}"
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Success and Failure:`

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced
Audit Policy Configuration\Audit Policies\System\Audit System Integrity
```

Default Value:

Success and Failure.

References:

1. GRID: MS-00000229

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

18 Administrative Templates (Computer)

This section contains computer-based recommendations from Group Policy Administrative Templates (ADMX).

18.1 Control Panel

This section contains recommendations for Control Panel settings.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.1.1 Personalization

This section contains recommendations for Control Panel personalization settings.

This Group Policy section is provided by the Group Policy template `ControlPanelDisplay.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.1.1.1 Ensure 'Prevent enabling lock screen camera' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Disables the lock screen camera toggle switch in PC Settings and prevents a camera from being invoked on the lock screen.

The recommended state for this setting is: `Enabled`.

Rationale:

Disabling the lock screen camera extends the protection afforded by the lock screen to camera features.

Impact:

If you enable this setting, users will no longer be able to enable or disable lock screen camera access in PC Settings, and the camera cannot be invoked on the lock screen.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\Personalization:NoLockScreenCamera
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Control
Panel\Personalization\Prevent enabling lock screen camera
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `ControlPanelDisplay.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Default Value:

Disabled. (Users can enable invocation of an available camera on the lock screen.)

References:

1. GRID: MS-00000231

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

18.1.1.2 Ensure 'Prevent enabling lock screen slide show' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Disables the lock screen slide show settings in PC Settings and prevents a slide show from playing on the lock screen.

The recommended state for this setting is: `Enabled`.

Rationale:

Disabling the lock screen slide show extends the protection afforded by the lock screen to slide show contents.

Impact:

If you enable this setting, users will no longer be able to modify slide show settings in PC Settings, and no slide show will ever start.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\Personalization:NoLockScreenSlidesho
w
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Control
Panel\Personalization\Prevent enabling lock screen slide show
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `ControlPanelDisplay.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Default Value:

Disabled. (Users can enable a slide show that will run after they lock the machine.)

References:

1. GRID: MS-00000232

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

18.1.2 Regional and Language Options

This section contains recommendation settings for Regional and Language Options.

This Group Policy section is provided by the Group Policy template `Globalization.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.1.2.1 Handwriting personalization

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Globalization.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.1.2.2 Ensure 'Allow users to enable online speech recognition services' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy enables the automatic learning component of input personalization that includes speech, inking, and typing. Automatic learning enables the collection of speech and handwriting patterns, typing history, contacts, and recent calendar information. It is required for the use of Cortana. Some of this collected information may be stored on the user's OneDrive, in the case of inking and typing; some of the information will be uploaded to Microsoft to personalize speech.

The recommended state for this setting is: `Disabled`.

Rationale:

If this setting is Enabled sensitive information could be stored in the cloud or sent to Microsoft.

Impact:

Automatic learning of speech, inking, and typing stops and users cannot change its value via PC Settings.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\InputPersonalization:AllowInputPersonalizati
on
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Control
Panel\Regional and Language Options\Allow users to enable online speech
recognition services
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `Globalization.admx/adml` that is included with the Microsoft Windows 10 RTM (version 1507) Administrative Templates (or newer).

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Allow input personalization*. It was renamed to *Allow users to enable online speech recognition services* starting with the Windows 10 v1809 & Server 2019 Administrative Templates.

Default Value:

Enabled. (Automatic learning of speech, inking and typing is enabled, but users may change this value via PC Settings.)

References:

1. GRID: MS-00000233

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

18.1.3 Ensure 'Allow Online Tips' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting configures the retrieval of online tips and help for the Settings app.

The recommended state for this setting is: `Disabled`.

Rationale:

In high-security environments, data must never be shared with third-parties without explicit consent, as it may contain sensitive information.

Impact:

Settings will not contact Microsoft content services to retrieve tips and help content.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer:AllowOnlineTips
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Control Panel\Allow Online Tips
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `ControlPanel.admx/adml` that is included with the Microsoft Windows 10 version 1709 Administrative Templates (or newer).

Default Value:

Enabled. (Settings will contact Microsoft content services to retrieve tips and help content.)

References:

1. GRID: MS-00000230

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●
v7	9.3 Perform Regular Automated Port Scans Perform automated port scans on a regular basis against all systems and alert if unauthorized ports are detected on a system.		●	●

18.2 Desktop

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Desktop.admx/adml` that is included with the Microsoft Windows 11 version 22H2 Administrative Templates v1.0 (or newer).

18.3 LAPS (legacy)

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This older version of LAPS is still applicable to Windows Server 2016, which is not supported by the newer Windows LAPS.

This Group Policy section is provided by the Group Policy template `AdmPwd.admx/adml` that is included with older versions of the Microsoft Security Compliance Toolkit and Baselines. Regardless of Windows Operating System version, download the Security Baseline for Windows 11 22H2, which is the last Security Baseline to obtain the template.

Legacy Microsoft LAPS can be downloaded from Download LAPS from Official Microsoft Download Center.

18.4 MS Security Guide

This section contains recommendations for configuring additional settings from the MS Security Guide.

This Group Policy section is provided by the Group Policy template `SecGuide.admx/adml` that is available for download from the Microsoft Security Compliance Toolkit and Baselines website. Regardless of Windows Operating System version, download the latest Windows 11 Security Baseline to obtain the template.

18.4.1 Ensure 'Apply UAC restrictions to local accounts on network logons' is set to 'Enabled' (MS only) (Automated)

Profile Applicability:

- Level 1 - Member Server

Description:

This setting controls whether local accounts can be used for remote administration via network logon (e.g., NET USE, connecting to C$, etc.). Local accounts are at high risk for credential theft when the same account and password is configured on multiple systems. Enabling this policy significantly reduces that risk.

Enabled: Applies UAC token-filtering to local accounts on network logons. Membership in powerful group such as Administrators is disabled and powerful privileges are removed from the resulting access token. This configures the `LocalAccountTokenFilterPolicy` registry value to `0`. This is the default behavior for Windows.

Disabled: Allows local accounts to have full administrative rights when authenticating via network logon, by configuring the `LocalAccountTokenFilterPolicy` registry value to `1`.

For more information about local accounts and credential theft, review the "Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques" documents.

For more information about `LocalAccountTokenFilterPolicy`, see Microsoft Knowledge Base article 951016: Description of User Account Control and remote restrictions in Windows Vista.

The recommended state for this setting is: `Enabled`.

Rationale:

Local accounts are at high risk for credential theft when the same account and password is configured on multiple systems. Ensuring this policy is Enabled significantly reduces that risk.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:LocalAccountTo
kenFilterPolicy
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\MS Security
Guide\Apply UAC restrictions to local accounts on network logons
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`SecGuide.admx/adml`) is required - it is available from Microsoft at this link.

Default Value:

Enabled. (UAC token-filtering is applied to local accounts on network logons. Membership in powerful groups such as Administrators and disabled and powerful privileges are removed from the resulting access token.)

References:

1. GRID: MS-00000240

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	4.3 Ensure the Use of Dedicated Administrative Accounts Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	●	●	●

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This setting configures the start type for the Server Message Block version 1 (SMBv1) client driver service (`MRxSmb10`), which is recommended to be disabled.

The recommended state for this setting is: `Enabled: Disable driver (recommended)`.

Note: Do not, *under any circumstances*, configure this overall setting as `Disabled`, as doing so will delete the underlying registry entry altogether, which will cause serious problems.

Rationale:

Since September 2016, Microsoft has strongly encouraged that SMBv1 be disabled and no longer used on modern networks, as it is a 30 year old design that is much more vulnerable to attacks then much newer designs such as SMBv2 and SMBv3.

More information on this can be found at the following links:

Stop using SMB1 | Storage at Microsoft

Disable SMB v1 in Managed Environments with Group Policy – "Stay Safe" Cyber Security Blog

Disabling SMBv1 through Group Policy – Microsoft Security Guidance blog

Impact:

Some legacy OSes (e.g. Windows XP, Server 2003 or older), applications and appliances may no longer be able to communicate with the system once SMBv1 is disabled. We recommend careful testing be performed to determine the impact prior to configuring this as a widespread control, and where possible, remediate any incompatibilities found with the vendor of the incompatible system. Microsoft is also maintaining a thorough (although not comprehensive) list of known SMBv1 incompatibilities at this link: SMB1 Product Clearinghouse | Storage at Microsoft

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `4`.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\mrxsmb10:Start
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Disable driver (recommended)`:

```
Computer Configuration\Policies\Administrative Templates\MS Security
Guide\Configure SMB v1 client driver
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`SecGuide.admx/adml`) is required - it is available from Microsoft at this link.

Default Value:

On Windows Server 2008 (non-R2), 2008 R2, and 2012 (non-R2): Enabled: Manual start.

On Windows Server 2012 R2 and Server 2016 (up to v1607): Enabled: Automatic start.

On Windows Server 2016 v1709 or newer: Enabled: Disable driver.

References:

1. GRID: MS-00000242

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●
v7	14.3 Disable Workstation to Workstation Communication Disable all workstation to workstation communication to limit an attacker's ability to move laterally and compromise neighboring systems, through technologies such as Private VLANs or microsegmentation.		●	●

18.4.3 Ensure 'Configure SMB v1 server' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This setting configures the server-side processing of the Server Message Block version 1 (SMBv1) protocol.

The recommended state for this setting is: `Disabled`.

Rationale:

Since September 2016, Microsoft has strongly encouraged that SMBv1 be disabled and no longer used on modern networks, as it is a 30 year old design that is much more vulnerable to attacks then much newer designs such as SMBv2 and SMBv3.

More information on this can be found at the following links:

Stop using SMB1 | Storage at Microsoft

Disable SMB v1 in Managed Environments with Group Policy – "Stay Safe" Cyber Security Blog

Disabling SMBv1 through Group Policy – Microsoft Security Guidance blog

Impact:

Some legacy OSes (e.g. Windows XP, Server 2003 or older), applications and appliances may no longer be able to communicate with the system once SMBv1 is disabled. We recommend careful testing be performed to determine the impact prior to configuring this as a widespread control, and where possible, remediate any incompatibilities found with the vendor of the incompatible system. Microsoft is also maintaining a thorough (although not comprehensive) list of known SMBv1 incompatibilities at this link: SMB1 Product Clearinghouse | Storage at Microsoft

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters:SMB1
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\MS Security
Guide\Configure SMB v1 server
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`SecGuide.admx/adml`) is required - it is available from Microsoft at this link.

Default Value:

On Windows Server 2016 v1607 and older: Enabled.

On Windows Server 2016 v1709 or newer: Disabled.

References:

1. GRID: MS-00000243

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●
v7	14.3 Disable Workstation to Workstation Communication Disable all workstation to workstation communication to limit an attacker's ability to move laterally and compromise neighboring systems, through technologies such as Private VLANs or microsegmentation.		●	●

18.4.4 Ensure 'Enable Certificate Padding' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting configures whether the WinVerifyTrust function performs strict Windows Authenticode signature verification for Portable Executable files (PE files). If enabled, PE files will be considered "unsigned" if Windows identifies content in them that does not conform to the Authenticode specification.

The recommended state for this setting is: `Enabled`.

Rationale:

A remote code execution vulnerability exists in the way that the WinVerifyTrust function handles Windows Authenticode signature verification for portable executable (PE) files. For more information on this vulnerability, visit CVE-2013-3900 - Security Update Guide - Microsoft - WinVerifyTrust Signature Validation Vulnerability.

Impact:

Microsoft recommends that installers are built to only extract content from validated portions of signed files. Some installers do not follow this guidance and therefore may be negatively impacted by this setting.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` or `REG_SZ` value of `1`.

```
HKLM\SOFTWARE\Microsoft\Cryptography\Wintrust\Config:EnableCertPaddingCheck
```

32-bit subsystem on 64-bit OS

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` or `REG_SZ` value of `1`.

```
HKLM\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Wintrust\Config:EnableCertPaddingCheck
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\MS Security Guide\Enable Certificate Padding
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`SecGuide.admx/adml`) is required - it is available from Microsoft at this link.

Default Value:

Disabled. (The WinVerifyTrust function does not perform strict Windows Authenticode signature verification for Portable Executable files (PE files).)

References:

1. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2013-3900
2. https://learn.microsoft.com/en-us/windows/win32/api/wintrust/nf-wintrust-winverifytrust
3. https://aaron-margosis.medium.com/enable-certificate-padding-check-reg-sz-or-reg-dword-675603f0790b
4. https://msrc.microsoft.com/update-guide/advisory/ADV2915720
5. GRID: MS-00000244

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Windows includes support for Structured Exception Handling Overwrite Protection (SEHOP). We recommend enabling this feature to improve the security profile of the computer.

The recommended state for this setting is: `Enabled`.

Rationale:

This feature is designed to block exploits that use the Structured Exception Handler (SEH) overwrite technique. This protection mechanism is provided at run-time. Therefore, it helps protect applications regardless of whether they have been compiled with the latest improvements, such as the /SAFESEH option.

Impact:

After you enable SEHOP, existing versions of Cygwin, Skype, and Armadillo-protected applications may not work correctly.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SYSTEM\CurrentControlSet\Control\Session
Manager\kernel:DisableExceptionChainValidation
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\MS Security
Guide\Enable Structured Exception Handling Overwrite Protection (SEHOP)
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`SecGuide.admx/adml`) is required - it is available from Microsoft at this link.

More information is available at MSKB 956607: How to enable Structured Exception Handling Overwrite Protection (SEHOP) in Windows operating systems

Default Value:

Disabled for 32-bit processes.

References:

1. GRID: MS-00000245

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

18.4.6 Ensure 'NetBT NodeType configuration' is set to 'Enabled: P-node (recommended)' (Automated)

Profile Applicability:

- Level 1 - Member Server
- Level 1 - Domain Controller

Description:

This setting determines which method NetBIOS over TCP/IP (NetBT) uses to register and resolve names. The available methods are:

- The B-node (broadcast) method only uses broadcasts.
- The P-node (point-to-point) method only uses name queries to a name server (WINS).
- The M-node (mixed) method broadcasts first, then queries a name server (WINS) if broadcast failed.
- The H-node (hybrid) method queries a name server (WINS) first, then broadcasts if the query failed.

The recommended state for this setting is: `Enabled: P-node (recommended)` (point-to-point).

Note: Resolution through LMHOSTS or DNS follows these methods. If the `NodeType` registry value is present, it overrides any `DhcpNodeType` registry value. If neither `NodeType` nor `DhcpNodeType` is present, the computer uses B-node (broadcast) if there are no WINS servers configured for the network, or H-node (hybrid) if there is at least one WINS server configured.

Rationale:

In order to help mitigate the risk of NetBIOS Name Service (NBT-NS) poisoning attacks, setting the node type to P-node (point-to-point) will prevent the system from sending out NetBIOS broadcasts.

Impact:

NetBIOS name resolution queries will require a defined and available WINS server for external NetBIOS name resolution. If a WINS server is not defined or not reachable, and the desired hostname is not defined in the local cache, local LMHOSTS or HOSTS files, NetBIOS name resolution will fail.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `2`.

```
HKLM\SYSTEM\CurrentControlSet\Services\NetBT\Parameters:NodeType
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: P-node (recommended)`:

```
Computer Configuration\Policies\Administrative Templates\MS Security
Guide\NetBT NodeType configuration
```

Note: This change does not take effect until the computer has been restarted.

Note #2: This Group Policy path does not exist by default. An additional Group Policy template (`SecGuide.admx/adml`) is required - it is available from Microsoft at this link. Please note that this setting is **only** available in the *Security baseline (FINAL) for Windows 10 v1903 and Windows Server v1903* (or newer) release of `SecGuide.admx/adml`, so if you previously downloaded this template, you may need to update it from a newer Microsoft baseline to get this new *NetBT NodeType configuration* setting.

Default Value:

If a WINS server is not configured in NIC properties: B-node (broadcast only)

If a WINS server is configured in NIC properties: H-node (hybrid - point-to-point first, then broadcast)

References:

1. GRID: MS-00000247

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

18.5 MSS (Legacy)

This section contains recommendations for the Microsoft Solutions for Security (MSS) settings.

This Group Policy section is provided by the Group Policy template `MSS-legacy.admx/adml` that is available for download from the Microsoft Security Compliance Toolkit and Baselines website. Regardless of Windows Operating System version, download the latest Windows 11 Security Baseline to obtain the template.

18.5.1 Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This setting is separate from the Welcome screen feature in Windows XP and Windows Vista; if that feature is disabled, this setting is not disabled. If you configure a computer for automatic logon, anyone who can physically gain access to the computer can also gain access to everything that is on the computer, including any network or networks to which the computer is connected. Also, if you enable automatic logon, the password is stored in the registry in plaintext, and the specific registry key that stores this value is remotely readable by the Authenticated Users group.

For additional information, see Microsoft Knowledge Base article 324737: How to turn on automatic logon in Windows.

The recommended state for this setting is: `Disabled`.

Rationale:

If you configure a computer for automatic logon, anyone who can physically gain access to the computer can also gain access to everything that is on the computer, including any network or networks that the computer is connected to. Also, if you enable automatic logon, the password is stored in the registry in plaintext. The specific registry key that stores this setting is remotely readable by the Authenticated Users group. As a result, this entry is appropriate only if the computer is physically secured and if you ensure that untrusted users cannot remotely see the registry.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_SZ` value of `0`.

```
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon:AutoAdminLogon
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS:
(AutoAdminLogon) Enable Automatic Logon
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`MSS-legacy.admx/adml`) is required - it is available from this TechNet blog post: The MSS settings – Microsoft Security Guidance blog

Default Value:

Disabled.

References:

1. GRID: MS-00000249

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 Encrypt Sensitive Data at Rest Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		●	●
v7	16.4 Encrypt or Hash all Authentication Credentials Encrypt or hash with a salt all authentication credentials when stored.		●	●

18.5.2 Ensure 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level' is set to 'Enabled: Highest protection, source routing is completely disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

IP source routing is a mechanism that allows the sender to determine the IP route that a datagram should follow through the network.

The recommended state for this setting is: `Enabled: Highest protection, source routing is completely disabled`.

Rationale:

A threat actor could use source routed packets to obscure their identity and location. Source routing allows a computer that sends a packet to specify the route that the packet takes.

Impact:

All incoming source routed packets will be dropped.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `2`.

```
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters:DisableIPSourceRouting
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Highest protection, source routing is completely disabled`:

```
Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (DisableIPSourceRouting IPv6) IP source routing protection level
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`MSS-legacy.admx/adml`) is required - it is available from this TechNet blog post: [The MSS settings – Microsoft Security Guidance blog]

Default Value:

No additional protection, source routed packets are allowed.

References:

1. GRID: MS-00000250

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

18.5.3 Ensure 'MSS: (DisableIPSourceRouting) IP source routing protection level' is set to 'Enabled: Highest protection, source routing is completely disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

IP source routing is a mechanism that allows the sender to determine the IP route that a datagram should take through the network. It is recommended to configure this setting to Not Defined for enterprise environments and to Highest Protection for high security environments to completely disable source routing.

The recommended state for this setting is: `Enabled: Highest protection, source routing is completely disabled`.

Rationale:

A threat actor could use source routed packets to obscure their identity and location. Source routing allows a computer that sends a packet to specify the route that the packet takes.

Impact:

All incoming source routed packets will be dropped.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `2`.

```
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters:DisableIPSourceRoutin
g
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Highest protection, source routing is completely disabled`:

```
Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS:
(DisableIPSourceRouting) IP source routing protection level
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`MSS-legacy.admx/adml`) is required - it is available from this TechNet blog post: The MSS settings – Microsoft Security Guidance blog

Default Value:

Medium, source routed packets ignored when IP forwarding is enabled.

References:

1. GRID: MS-00000251

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Internet Control Message Protocol (ICMP) redirects cause the IPv4 stack to plumb host routes. These routes override the Open Shortest Path First (OSPF) generated routes.

The recommended state for this setting is: `Disabled`.

Rationale:

This behavior is expected. The problem is that the 10 minute time-out period for the ICMP redirect-plumbed routes temporarily creates a network situation in which traffic will no longer be routed properly for the affected host. Ignoring such ICMP redirects will limit the system's exposure to attacks that will impact its ability to participate on the network.

Impact:

When Routing and Remote Access Service (RRAS) is configured as an autonomous system boundary router (ASBR), it does not correctly import connected interface subnet routes. Instead, this router injects host routes into the OSPF routes. However, the OSPF router cannot be used as an ASBR router, and when connected interface subnet routes are imported into OSPF the result is confusing routing tables with strange routing paths.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters:EnableICMPRedirect
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS:
(EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`MSS-legacy.admx/adml`) is required - it is available from this TechNet blog post: The MSS settings – Microsoft Security Guidance blog

Default Value:

Enabled. (ICMP redirects can override OSPF-generated routes.)

References:

1. GRID: MS-00000253

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

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

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This value controls how often TCP attempts to verify that an idle connection is still intact by sending a keep-alive packet. If the remote computer is still reachable, it acknowledges the keep-alive packet.

The recommended state for this setting is: `Enabled: 300,000 or 5 minutes`.

Rationale:

A threat actor who is able to connect to network applications could establish numerous connections to cause a DoS condition.

Impact:

Keep-alive packets are not sent by default by Windows. However, some applications may configure the TCP stack flag that requests keep-alive packets. For such configurations, you can lower this value from the default setting of two hours to five minutes to disconnect inactive sessions more quickly.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `300000`.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters:KeepAliveTime
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: 300,000 or 5 minutes`:

```
Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`MSS-legacy.admx/adml`) is required - it is available from this TechNet blog post: [The MSS settings – Microsoft Security Guidance blog]

Default Value:

7,200,000 milliseconds or 120 minutes.

References:

1. GRID: MS-00000254

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

NetBIOS over TCP/IP is a network protocol that among other things provides a way to easily resolve NetBIOS names that are registered on Windows-based systems to the IP addresses that are configured on those systems. This setting determines whether the computer releases its NetBIOS name when it receives a name-release request.

The recommended state for this setting is: `Enabled`.

Rationale:

The NetBT protocol is designed not to use authentication, and is therefore vulnerable to spoofing. Spoofing makes a transmission appear to come from a user other than the user who performed the action. A threat actor could exploit the unauthenticated nature of the protocol to send a name-conflict datagram to a target computer, which would cause the computer to relinquish its name and not respond to queries.

A threat actor could send a request over the network and query a computer to release its NetBIOS name. As with any change that could affect applications, it is recommended that you test this change in a non-production environment before you change the production environment.

The result of such an attack could be to cause intermittent connectivity issues on the target computer, or even to prevent the use of Network Neighborhood, domain logons, the NET SEND command, or additional NetBIOS name resolution.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SYSTEM\CurrentControlSet\Services\NetBT\Parameters:NoNameReleaseOnDemand
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS:
(NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release
requests except from WINS servers
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`MSS-legacy.admx/adml`) is required - it is available from this TechNet blog post: The MSS settings – Microsoft Security Guidance blog

Default Value:

Enabled.

References:

1. GRID: MS-00000255

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

18.5.7 Ensure 'MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This setting is used to enable or disable the Internet Router Discovery Protocol (IRDP), which allows the system to detect and configure default gateway addresses automatically as described in RFC 1256 on a per-interface basis.

The recommended state for this setting is: `Disabled`.

Rationale:

A threat actor who has gained control of a computer on the same network segment could configure a computer on the network to impersonate a router. Other computers with IRDP enabled would then attempt to route their traffic through the already compromised computer.

Impact:

Windows will not automatically detect and configure default gateway addresses on the computer.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters:PerformRouterDiscover
y
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS:
(PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway
addresses
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`MSS-legacy.admx/adml`) is required - it is available from this TechNet blog post: [The MSS settings – Microsoft Security Guidance blog]

Default Value:

Enable only if DHCP sends the Perform Router Discovery option.

References:

1. GRID: MS-00000256

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

The DLL search order can be configured to search for DLLs that are requested by running processes in one of two ways:

- Search folders specified in the system path first, and then search the current working folder.
- Search current working folder first, and then search the folders specified in the system path.

When enabled, the registry value is set to 1. With a setting of 1, the system first searches the folders that are specified in the system path and then searches the current working folder. When disabled the registry value is set to 0 and the system first searches the current working folder and then searches the folders that are specified in the system path.

Applications will be forced to search for DLLs in the system path first. For applications that require unique versions of these DLLs that are included with the application, this entry could cause performance or stability problems.

The recommended state for this setting is: `Enabled`.

Note: More information on how Safe DLL search mode works is available at this link: Dynamic-Link Library Search Order - Windows applications | Microsoft Docs

Rationale:

If a user unknowingly executes hostile code that was packaged with additional files that include modified versions of system DLLs, the hostile code could load its own versions of those DLLs and potentially increase the type and degree of damage the code can render.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SYSTEM\CurrentControlSet\Control\Session Manager:SafeDllSearchMode
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS:
(SafeDllSearchMode) Enable Safe DLL search mode
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`MSS-legacy.admx/adml`) is required - it is available from this TechNet blog post: The MSS settings – Microsoft Security Guidance blog

Default Value:

Enabled.

References:

1. GRID: MS-00000257

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

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

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This setting controls the number of times that TCP retransmits an individual data segment (non-connect segment) before the connection is aborted. The retransmission time-out is doubled with each successive retransmission on a connection. It is reset when responses resume. The base time-out value is dynamically determined by the measured round-trip time on the connection.

The recommended state for this setting is: `Enabled: 3`.

Rationale:

A threat actor could exhaust a target computer's resources if it never sent any acknowledgment messages for data that was transmitted by the target computer.

Impact:

TCP starts a retransmission timer when each outbound segment is passed to the IP. If no acknowledgment is received for the data in a given segment before the timer expires, then the segment is retransmitted up to three times.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `3`.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TCPIP6\Parameters:TcpMax
DataRetransmissions
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: 3`:

```
Computer Configuration\Policies\Administrative Templates\MSS
(Legacy)\MSS:(TcpMaxDataRetransmissions IPv6) How many times unacknowledged
data is retransmitted
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`MSS-legacy.admx/adml`) is required - it is available from this TechNet blog post: The MSS settings – Microsoft Security Guidance blog

Default Value:

5 times.

References:

1. GRID: MS-00000259

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	11.1 Maintain Standard Security Configurations for Network Devices Maintain standard, documented security configuration standards for all authorized network devices.		●	●

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

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This setting controls the number of times that TCP retransmits an individual data segment (non-connect segment) before the connection is aborted. The retransmission time-out is doubled with each successive retransmission on a connection. It is reset when responses resume. The base time-out value is dynamically determined by the measured round-trip time on the connection.

The recommended state for this setting is: `Enabled: 3`.

Rationale:

A threat actor could exhaust a target computer's resources if it never sent any acknowledgment messages for data that was transmitted by the target computer.

Impact:

TCP starts a retransmission timer when each outbound segment is passed to the IP. If no acknowledgment is received for the data in a given segment before the timer expires, then the segment is retransmitted up to three times.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `3`.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters:TcpMaxDataRetransmissions
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: 3`:

```
Computer Configuration\Policies\Administrative Templates\MSS
(Legacy)\MSS:(TcpMaxDataRetransmissions) How many times unacknowledged data
is retransmitted
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`MSS-legacy.admx/adml`) is required - it is available from this TechNet blog post: The MSS settings – Microsoft Security Guidance blog

Default Value:

5 times.

References:

1. GRID: MS-00000260

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.5.11 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' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This setting can generate a security audit in the Security event log when the log reaches a user-defined threshold.

The recommended state for this setting is: `Enabled: 90% or less`.

Note: If log settings are configured to Overwrite events as needed or Overwrite events older than x days, this event will not be generated.

Rationale:

If the Security log reaches 90 percent of its capacity and the computer has not been configured to overwrite events as needed, more recent events will not be written to the log. If the log reaches its capacity and the computer has been configured to shut down when it can no longer record events to the Security log, the computer will shut down and will no longer be available to provide network services.

Impact:

An audit event will be generated when the Security log reaches the 90% percent full threshold (or whatever lower value may be set) unless the log is configured to overwrite events as needed.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `90`.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Security:Warnin
gLevel
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: 90% or less`:

```
Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`MSS-legacy.admx/adml`) is required - it is available from this TechNet blog post: The MSS settings – Microsoft Security Guidance blog

Default Value:

0%. (No warning event is generated.)

References:

1. GRID: MS-00000261

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 Ensure Adequate Audit Log Storage Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	●	●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●
v7	6.4 Ensure adequate storage for logs Ensure that all systems that store logs have adequate storage space for the logs generated.		●	●

18.6 Network

This section contains recommendations for network settings.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.6.1 Background Intelligent Transfer Service (BITS)

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Bits.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.6.2 BranchCache

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `PeerToPeerCaching.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.6.3 DirectAccess Client Experience Settings

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `nca.admx/adml` that is included with the Microsoft 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.6.4 DNS Client

This section contains recommendations related to DNS Client.

This Group Policy section is provided by the Group Policy template `DnsClient.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.6.4.1 Ensure 'Configure multicast DNS (mDNS) protocol' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines if the DNS client will perform name resolution over Multicast DNS (mDNS). mDNS performs local network name and service discoveries without the need for central DNS.

The recommended state for this setting is: `Disabled`.

Rationale:

A threat actor can listen on a network over UDP port 5353 and respond to them, tricking the host into thinking that it knows the location of the requested system.

Impact:

In the event DNS is unavailable a system will be unable to request it from other systems on the same subnet.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\DNSClient:EnableMDNS
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Network\DNS
Client\Configure multicast DNS (mDNS) protocol
```

Note: This Group Policy path is provided by the Group Policy template `DnsClient.admx/adml` that is included with the Microsoft Windows 11 version 24H2 Administrative Templates (or newer).

Default Value:

Disabled. (The system will use locally configured settings.)

References:

1. https://techcommunity.microsoft.com/blog/networkingblog/mdns-in-the-enterprise/3275777
2. https://www.wolfandco.com/resources/blog/penetration-testers-best-friend dns-llmnr-netbios-ns/
3. GRID: MS-00000574

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

18.6.4.2 Ensure 'Configure NetBIOS settings' is set to 'Enabled: Disable NetBIOS name resolution on public networks' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting specifies if the Domain Name System (DNS) client will perform name resolution over Network Basic Input/Output System (NetBIOS). NetBIOS is a legacy name resolution method for internal Microsoft networking that predates the use of DNS for that purpose (pre–Active Directory). Some legacy applications still require the use of NetBIOS for full functionality.

The recommended state for this setting is: `Enabled: Disable NetBIOS name resolution on public networks`. Configuring this setting to `Enabled: Disable NetBIOS name resolution` also conforms to the benchmark.

Rationale:

NetBIOS does not perform authentication and can allow remote threat actors to cause a denial-of-service by sending spoofed Name Conflicts or Name Release datagrams. This is also known as "NetBIOS Name Server Protocol Spoofing". Preventing the use of NetBIOS on public networks reduces the attack surface.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0` or `2`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\DNSClient:EnableNetbios
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Disable NetBIOS name resolution on public networks`:

```
Computer Configuration\Policies\Administrative Templates\Network\DNS
Client\Configure NetBIOS settings
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `DnsClient.admx/adml` that is included with the Microsoft Windows 11 version 22H2 Administrative Templates v1.0 (or newer).

Default Value:

Enabled. (The DNS client will disable NetBIOS name resolution on public networks.)

References:

1. GRID: MS-00000263

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●

18.6.4.3 Ensure 'Turn off default IPv6 DNS Servers' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting controls whether the DNS client will use the default IPv6 DNS server addresses provided by Windows.

The recommended state for this setting is: `Enabled`.

Rationale:

Since the vast majority of private enterprise managed networks have no need to utilize IPv6 (because they have access to private IPv4 addressing), disabling the use of IPv6 DNS server addresses removes a possible attack surface that is also harder to monitor the traffic on.

It is not recommended to use DNS servers that are controlled by an external entity without input from the organization's IT department.

Impact:

Default IPv6 DNS server addresses will not be utilized by Windows.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows
NT\DNSClient:DisableIPv6DefaultDnsServers
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Network\DNS
Client\Turn off default IPv6 DNS Servers
```

Note: This Group Policy path is provided by the Group Policy template `DnsClient.admx/adml` that is included with the Microsoft Windows 11 version 24H2 Administrative Templates (or newer).

Default Value:

Disabled. (The default IPv6 DNS server addresses provided by Windows will be utilized.)

References:

1. GRID: MS-00000575

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.6.4.4 Ensure 'Turn off multicast name resolution' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Member Server
- Level 1 - Domain Controller

Description:

Link-Local Multicast Name Resolution (LLMNR) is a secondary name resolution protocol. With LLMNR, queries are sent using multicast over a local network link on a single subnet from a client computer to another client computer on the same subnet that also has LLMNR enabled. LLMNR does not require a DNS server or DNS client configuration and provides name resolution in scenarios in which conventional DNS name resolution is not possible.

The recommended state for this setting is: `Enabled`.

Rationale:

A threat actors can listen on a network for these LLMNR (UDP/5355) or NBT-NS (UDP/137) broadcasts and respond to them, tricking the host into thinking that it knows the location of the requested system.

Note: To completely mitigate local name resolution poisoning, in addition to this setting, the properties of each installed NIC should also be set to `Disable NetBIOS over TCP/IP` (on the WINS tab in the NIC properties). Unfortunately, there is no global setting to achieve this that automatically applies to all NICs - it is a per-NIC setting that varies with different NIC hardware installations.

Impact:

In the event DNS is unavailable a system will be unable to request it from other systems on the same subnet.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\DNSClient:EnableMulticast
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Network\DNS
Client\Turn off multicast name resolution
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `DnsClient.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Disabled. (LLMNR will be enabled on all available network adapters.)

References:

1. GRID: MS-00000264

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.6.5 Fonts

This section contains recommendations related to Fonts.

This Group Policy section is provided by the Group Policy template `GroupPolicy.admx/adml` that is included with the Microsoft Windows 10 version 1607 & Server 2016 Administrative Templates (or newer).

18.6.5.1 Ensure 'Enable Font Providers' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting determines whether Windows is allowed to download fonts and font catalog data from an online font provider.

The recommended state for this setting is: `Disabled`.

Rationale:

In an enterprise managed environment the IT department should be managing the changes to the system configuration, to ensure all changes are tested and approved.

Impact:

Windows will not connect to an online font provider and will only enumerate locally-installed fonts.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\System:EnableFontProviders
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Network\Fonts\Enable
Font Providers
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `GroupPolicy.admx/adml` that is included with the Microsoft Windows 10 version 1607 & Server 2016 Administrative Templates (or newer).

Default Value:

Enabled. (Fonts that are included in Windows but that are not stored locally will be downloaded on demand from an online font provider.)

References:

1. GRID: MS-00000265

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	18.4 Only Use Up-to-date And Trusted Third-Party Components Only use up-to-date and trusted third-party components for the software developed by the organization.		●	●

18.6.6 Hotspot Authentication

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `hotspotauth.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.6.7 Lanman Server

This section contains recommendations related to Lanman Server.

This Group Policy section is provided by the Group Policy template `LanmanServer.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.6.7.1 Ensure 'Mandate the minimum version of SMB' is set to 'Enabled: 3.1.1' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy settings controls the minimum version of Server Message Block (SMB) protocol that can be used on the system.

The recommended state for this setting is: `Enabled: 3.1.1`.

Note: This group policy setting does not prevent the use of SMBv1 if it is installed and enabled on the system. If the following recommendations are configured as prescribed in this benchmark, SMBv1 will be disabled on the system: *Configure SMB v1 client driver* and *Configure SMB v1 server*.

Rationale:

The newer, more modern version of SMB (v3) is supported and available on all currently supported Microsoft Windows OSes. SMBv1 is no longer enabled by default due to its security risks, and although SMBv2 is more robust than v1, it does not support encryption like its successor.

Impact:

If older legacy (unsupported) Windows OSes that do not support SMB v3.1.1 are present in the environment, this setting may affect backward compatibility with them. For example, Windows 8.1 and Windows Server 2012 R2 and older. This setting may also prevent third-party clients that do not support SMB v3.1.1 from connecting.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `785`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\LanmanServer:MinSmb2Dialect
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: 3.1.1`:

```
Computer Configuration\Policies\Administrative Templates\Network\Lanman Server\Mandate the minimum version of SMB
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `LanmanServer.admx/adml` that is included with the Microsoft Windows 11 version 24H2 Administrative Templates (or newer).

Default Value:

Disabled. (SMB v2.0 or higher are enabled by default.)

References:

1. GRID: MS-00000581

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.6.8 Lanman Workstation

This section contains recommendations related to Lanman Workstation.

This Group Policy section is provided by the Group Policy template `LanmanWorkstation.admx/adml` that is included with the Microsoft Windows 10 RTM (version 1507) Administrative Templates (or newer).

18.6.8.1 Ensure 'Enable insecure guest logons' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines if the SMB client will allow insecure guest logons to an SMB server.

The recommended state for this setting is: `Disabled`.

Rationale:

Insecure guest logons are used by file servers to allow unauthenticated access to shared folders.

Impact:

The SMB client will reject insecure guest logons. This was not originally the default behavior in older versions of Windows, but Microsoft changed the default behavior starting with Windows Server 2016 v1709: Guest access in SMB2 disabled by default in Windows 10 and Windows Server 2016

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\LanmanWorkstation:AllowInsecureGuestAuth
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled:`

```
Computer Configuration\Policies\Administrative Templates\Network\Lanman Workstation\Enable insecure guest logons
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `LanmanWorkstation.admx/adml` that is included with the Microsoft Windows 10 version 1511 Administrative Templates (or newer).

Default Value:

On Server 2016 RTM (v1607) or older: Enabled. (The SMB client will allow insecure guest logons.)

On Server 2016 v1709, Server 2019 or newer: Disabled. (The SMB client will reject insecure guest logons.)

References:

1. GRID: MS-00000266

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.6.8.2 Ensure 'Require Encryption' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls whether the SMB client will require encryption.

The recommended state for this setting is: `Enabled`.

Warning: The SMB server must support and have SMB encryption enabled (requires SMB v3.0 or newer).

Rationale:

The newer, more modern version of SMB (v3) is supported and available on all currently supported Microsoft Windows OSes. SMBv1 is no longer enabled by default due to its security risks, and although SMBv2 is more robust than v1, it does not support encryption like its successor.

Impact:

If older legacy (unsupported) Windows OSes that do not support encryption are present in the environment, this setting may affect backward compatibility with them. For example, Windows 7 and Windows Server 2008 R2 and older. This setting may also affect connecting to third-party devices and appliances that do not support SMB v3.0.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\LanmanWorkstation:RequireEncryption
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Network\Lanman
Workstation\Require Encryption
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `LanmanWorkstation.admx/adml` that is included with the Microsoft Windows 11 version 24H2 Administrative Templates (or newer).

Default Value:

Disabled. (The SMB client will not require encryption. However, SMB encryption may still be required by the server.)

References:

1. GRID: MS-00000613

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	14.4 Encrypt All Sensitive Information in Transit Encrypt all sensitive information in transit.		●	●

18.6.9 Link-Layer Topology Discovery

This section contains recommendations for Link-Layer Topology Discovery settings.

This Group Policy section is provided by the Group Policy template `LinkLayerTopologyDiscovery.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

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

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting changes the operational behavior of the Mapper I/O network protocol driver.

LLTDIO allows a computer to discover the topology of a network it's connected to. It also allows a computer to initiate Quality-of-Service requests such as bandwidth estimation and network health analysis.

The recommended state for this setting is: `Disabled`.

Rationale:

To help protect from potentially discovering and connecting to unauthorized devices, this setting should be disabled to prevent responding to network traffic for network topology discovery.

Impact:

Some real-time applications could have issues with short network disconnections. For more information visit: Network disconnection after configuring the LLTDIO and RSPNDR group policy objects - Windows Server | Microsoft Learn.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry locations with a `REG_DWORD` value of `0`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\LLTD:AllowLLTDIOOnDoma
in
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\LLTD:AllowLLTDIOOnPubl
icNet
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\LLTD:EnableLLTDIO
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\LLTD:ProhibitLLTDIOOnP
rivateNet
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Network\Link-Layer
Topology Discovery\Turn on Mapper I/O (LLTDIO) driver
```

Note: This Group Policy path is provided by the Group Policy template `LinkLayerTopologyDiscovery.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (The Mapper I/O (LLTDIO) network protocol driver is turned off.)

References:

1. GRID: MS-00000267

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

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

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting changes the operational behavior of the Responder network protocol driver.

The Responder allows a computer to participate in Link Layer Topology Discovery requests so that it can be discovered and located on the network. It also allows a computer to participate in Quality-of-Service activities such as bandwidth estimation and network health analysis.

The recommended state for this setting is: `Disabled`.

Rationale:

To help protect from potentially discovering and connecting to unauthorized devices, this setting should be disabled to prevent responding to network traffic for network topology discovery.

Impact:

Some real-time applications could have issues with short network disconnections. For more information visit: Network disconnection after configuring the LLTDIO and RSPNDR group policy objects - Windows Server | Microsoft Learn.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry locations with a `REG_DWORD` value of `0`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\LLTD:AllowRspndrOnDoma
in
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\LLTD:AllowRspndrOnPubl
icNet
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\LLTD:EnableRspndr
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\LLTD:ProhibitRspndrOnP
rivateNet
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Network\Link-Layer Topology Discovery\Turn on Responder (RSPNDR) driver
```

Note: This Group Policy path is provided by the Group Policy template `LinkLayerTopologyDiscovery.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (The Responder (RSPNDR) network protocol driver is turned off.)

References:

1. GRID: MS-00000268

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

18.6.10 Microsoft Peer-to-Peer Networking Services

This section contains recommendations for Microsoft Peer-to-Peer Networking Services settings.

This Group Policy section is provided by the Group Policy template `P2P-pnrp.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.6.10.1 Peer Name Resolution Protocol

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `P2P-pnrp.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.6.10.2 Ensure 'Turn off Microsoft Peer-to-Peer Networking Services' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

The Peer Name Resolution Protocol (PNRP) allows for distributed resolution of a name to an IPv6 address and port number. The protocol operates in the context of *clouds*. A cloud is a set of peer computers that can communicate with each other by using the same IPv6 scope.

Peer-to-Peer protocols allow for applications in the areas of RTC, collaboration, content distribution and distributed processing.

The recommended state for this setting is: `Enabled`.

Rationale:

This setting enhances the security of the environment and reduces the overall risk exposure related to peer-to-peer networking.

Impact:

Microsoft Peer-to-Peer Networking Services are turned off in their entirety, and all applications dependent on them will stop working.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Peernet:Disabled
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Network\Microsoft
Peer-to-Peer Networking Services\Turn off Microsoft Peer-to-Peer Networking
Services
```

Note: This Group Policy path is provided by the Group Policy template `P2P-pnrp.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Peer-to-peer protocols are turned on.)

References:

1. GRID: MS-00000269

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.6.11 Network Connections

This section contains recommendations for Network Connections settings.

This Group Policy section is provided by the Group Policy template `NetworkConnections.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.6.11.1 Windows Defender Firewall (formerly Windows Firewall)

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsFirewall.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note: This section was initially named *Windows Firewall* but was renamed by Microsoft to *Windows Defender Firewall* starting with the Microsoft Windows 10 version 1709 Administrative Templates.

18.6.11.2 Ensure 'Prohibit installation and configuration of Network Bridge on your DNS domain network' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

You can use this procedure to control a user's ability to install and configure a Network Bridge.

The recommended state for this setting is: `Enabled`.

Rationale:

The Network Bridge setting, if enabled, allows users to create a Layer 2 Media Access Control (MAC) bridge, enabling them to connect two or more physical network segments together. A Network Bridge thus allows a computer that has connections to two different networks to share data between those networks.

In an enterprise managed environment, where there is a need to control network traffic to only authorized paths, allowing users to create a Network Bridge increases the risk and attack surface from the bridged network.

Impact:

Users cannot create or configure a Network Bridge.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\Network
Connections:NC_AllowNetBridge_NLA
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Network\Network
Connections\Prohibit installation and configuration of Network Bridge on your
DNS domain network
```

Note: This Group Policy path is provided by the Group Policy template `NetworkConnections.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Users are able create and modify the configuration of Network Bridges. Membership in the local Administrators group, or equivalent, is the minimum required to complete this procedure.)

References:

1. GRID: MS-00000270

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	11.3 Use Automated Tools to Verify Standard Device Configurations and Detect Changes Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviations are discovered.		●	●

18.6.11.3 Ensure 'Prohibit use of Internet Connection Sharing on your DNS domain network' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Although this "legacy" setting traditionally applied to the use of Internet Connection Sharing (ICS) in Windows 2000, Windows XP & Server 2003, this setting now freshly applies to the Mobile Hotspot feature in Windows 10 & Server 2016.

The recommended state for this setting is: `Enabled`.

Rationale:

Non-administrators should not be able to turn on the Mobile Hotspot feature and open their Internet connectivity up to nearby mobile devices.

Impact:

Mobile Hotspot cannot be enabled or configured by Administrators and non-Administrators alike.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\Network
Connections:NC_ShowSharedAccessUI
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Network\Network
Connections\Prohibit use of Internet Connection Sharing on your DNS domain
network
```

Note: This Group Policy path is provided by the Group Policy template `NetworkConnections.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (All users are allowed to turn on Mobile Hotspot.)

References:

1. GRID: MS-00000271

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.6.11.4 Ensure 'Require domain users to elevate when setting a network's location' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether to require domain users to elevate when setting a network's location.

The recommended state for this setting is: `Enabled`.

Rationale:

Allowing regular users to set a network location increases the risk and attack surface.

Impact:

Domain users must elevate when setting a network's location.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\Network
Connections:NC_StdDomainUserSetLocation
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Network\Network
Connections\Require domain users to elevate when setting a network's location
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `NetworkConnections.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Default Value:

Disabled. (Users can set a network's location without elevating.)

References:

1. GRID: MS-00000272

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

18.6.12 Network Connectivity Status Indicator

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `NCSI.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.6.13 Network Isolation

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `NetworkIsolation.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.6.14 Network Provider

This section contains recommendations for Network Provider settings.

This Group Policy section is provided by the Group Policy template `NetworkProvider.admx/adml` that is included with the MS15-011 / MSKB 3000483 security update and the Microsoft Windows 10 RTM (version 1507) Administrative Templates (or newer).

18.6.14.1 Ensure 'Hardened UNC Paths' is set to 'Enabled, with "Require Mutual Authentication", "Require Integrity", and "Require Privacy" set for all NETLOGON and SYSVOL shares' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting configures secure access to Universal Naming Convention (UNC) paths. UNC paths identify network resources using a specific notation. These names consist of three parts: a host device name, a share name, and an optional file path.

The recommended state for this setting is: `Enabled, with "Require Mutual Authentication", "Require Integrity", and "Require Privacy" set for all NETLOGON and SYSVOL shares`.

Rationale:

In February 2015, Microsoft released a new control mechanism to mitigate a remote code execution vulnerability (MS15-011 / MSKB 3000483) in how Group Policy receives and applies connection data when a domain-joined system connects to a domain controller. A threat actor who successfully exploits this vulnerability could take complete control of the affected system. They could then install programs, view, change, or delete data, or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate with administrative user rights.

MS15-011 / MSKB 3000483 requires both the installation of the new security update and also the deployment of specific group policy settings to all computers on the domain from Windows Vista / Server 2008 (non-R2) or newer (the associated security patch to enable this feature was not released for Server 2003). A new group policy template (`NetworkProvider.admx/adml`) was also provided with the security update.

Once the new GPO template is in place, the following are the minimum requirements to remediate the Group Policy security risk:

```
\\*\NETLOGON RequireMutualAuthentication=1, RequireIntegrity=1, RequirePrivacy=1
```

```
\\*\SYSVOL RequireMutualAuthentication=1, RequireIntegrity=1, RequirePrivacy=1
```

Note: A reboot may be required after the setting is applied to a client machine to access the above paths.

Additional guidance on the deployment of this security setting is available from the Microsoft Premier Field Engineering (PFE) Platforms TechNet Blog here: Guidance on Deployment of MS15-011 and MS15-014.

Impact:

Windows only allows access to the specified UNC paths after fulfilling additional security requirements.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry locations with a `REG_SZ` value of `RequireMutualAuthentication=1, RequireIntegrity=1, RequirePrivacy=1`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths:\\*\NETLOGON
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths:\\*\SYSVOL
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled` with the following paths configured, at a minimum:

`\\*\NETLOGON RequireMutualAuthentication=1, RequireIntegrity=1, RequirePrivacy=1 \\*\SYSVOL RequireMutualAuthentication=1, RequireIntegrity=1, RequirePrivacy=1`

```
Computer Configuration\Policies\Administrative Templates\Network\Network Provider\Hardened UNC Paths
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`NetworkProvider.admx/adml`) is required - it is included with the MS15-011 / MSKB 3000483 security update or with the Microsoft Windows 10 RTM (version 1507) Administrative Templates (or newer).

Default Value:

Disabled. (No UNC paths are hardened.)

References:

1. GRID: MS-00000273

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

18.6.15 Offline Files

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `OfflineFiles.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.6.16 QoS Packet Scheduler

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `QOS.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.6.17 SNMP

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Snmp.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.6.18 SSL Configuration Settings

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `CipherSuiteOrder.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.6.19 TCPIP Settings

This section contains TCP/IP configuration settings.

This Group Policy section is provided by the Group Policy template `tcpip.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.6.19.1 IPv6 Transition Technologies

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `tcpip.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.6.19.2 Parameters

This section contains TCP/IP parameter configuration settings.

This Group Policy section is provided by the Group Policy template `tcpip.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.6.19.2.1 Disable IPv6 (Ensure TCPIP6 Parameter 'DisabledComponents' is set to '0xff (255)') (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

Internet Protocol version 6 (IPv6) is a set of protocols that computers use to exchange information over the Internet and over home and business networks. IPv6 allows for many more IP addresses to be assigned than IPv4 did. Older networking, hosts and operating systems may not support IPv6 natively.

The recommended state for this setting is: `DisabledComponents - 0xff (255)`.

Rationale:

Since the vast majority of private enterprise managed networks have no need to utilize IPv6 (because they have access to private IPv4 addressing), disabling IPv6 components removes a possible attack surface that is also harder to monitor the traffic on. As a result, we recommend configuring IPv6 to a Disabled state when it is not needed.

Configuring this recommendation to the CIS suggested state mitigates CVE-2024-38063, a TCP/IP Remote Code Execution Vulnerability.

Impact:

Connectivity to other systems using IPv6 will no longer operate, and software that depends on IPv6 will cease to function. Examples of Microsoft applications that may use IPv6 include: Remote Assistance, HomeGroup, DirectAccess, Windows Mail.

This registry change is documented in Microsoft Knowledge Base article 929852: How to disable IPv6 or its components in Windows.

Note: This registry change does not take effect until the next reboot.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `255`.

```
HKLM\SYSTEM\CurrentControlSet\Services\TCPIP6\Parameters:DisabledComponents
```

Remediation:

To establish the recommended configuration, set the following Registry value to `0xff (255) (DWORD)`:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TCPIP6\Parameters:Disabl
edComponents
```

Note: This change does not take effect until the computer has been restarted.

Note #2: Although Microsoft does not provide ADMX/ADML templates to configure this registry value, custom templates (`Configure-IPv6-Components-KB929852.ADMX/ADML`) are provided in the CIS Benchmark Build Kit to facilitate its configuration. Be aware though that simply turning off (not configured) the group policy setting with the template will not "undo" the change once applied. Instead, the opposite setting must be applied to change the registry value to the opposite state.

Default Value:

All IPv6 components are enabled and Windows prefers IPv6 over IPv4.

References:

1. https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-38063
2. GRID: MS-00000275

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.6.20 Windows Connect Now

This section contains recommendations for Windows Connect Now settings.

This Group Policy section is provided by the Group Policy template `WindowsConnectNow.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.6.20.1 Ensure 'Configuration of wireless settings using Windows Connect Now' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting allows the configuration of wireless settings using Windows Connect Now (WCN). The WCN Registrar enables the discovery and configuration of devices over Ethernet (UPnP) over in-band 802.11 Wi-Fi through the Windows Portable Device API (WPD) and via USB Flash drives. Additional options are available to allow discovery and configuration over a specific medium.

The recommended state for this setting is: `Disabled`.

Rationale:

This setting enhances the security of the environment and reduces the overall risk exposure related to user configuration of wireless settings. Additionally, according to Microsoft, Windows Connect Now was created as a solution for home networking and small businesses and is not intended for enterprise scenarios.

Impact:

WCN operations are disabled over all media.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry locations with a `REG_DWORD` value of `0`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WCN\Registrars:EnableR
egistrars
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WCN\Registrars:Disable
UPnPRegistrar
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WCN\Registrars:Disable
InBand802DOT11Registrar
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WCN\Registrars:Disable
FlashConfigRegistrar
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WCN\Registrars:Disable
WPDRegistrar
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Network\Windows
Connect Now\Configuration of wireless settings using Windows Connect Now
```

Note: This Group Policy path is provided by the Group Policy template `WindowsConnectNow.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

WCN operations are enabled and allowed over all media.

References:

1. https://learn.microsoft.com/en-us/windows/win32/wcn/about-windows-connect-now
2. GRID: MS-00000276

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	15.4 Disable Wireless Access on Devices if Not Required Disable wireless access on devices that do not have a business purpose for wireless access.			●
v7	15.5 Limit Wireless Access on Client Devices Configure wireless access on client machines that do have an essential wireless business purpose, to allow access only to authorized wireless networks and to restrict access to other wireless networks.			●

18.6.20.2 Ensure 'Prohibit access of the Windows Connect Now wizards' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting prohibits access to Windows Connect Now (WCN) wizards.

The recommended state for this setting is: `Enabled`.

Rationale:

Allowing standard users to access the Windows Connect Now wizard increases the risk and attack surface. Additionally, according to Microsoft, Windows Connect Now was created as a solution for home networking and small businesses and is not intended for enterprise scenarios.

Impact:

The WCN wizards are turned off and users have no access to any of the wizard tasks. All the configuration related tasks including "Set up a wireless router or access point" and "Add a wireless device" are disabled.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\WCN\UI:DisableWcnUi
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Network\Windows
Connect Now\Prohibit access of the Windows Connect Now wizards
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WindowsConnectNow.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Disabled. (Users can access all WCN wizard tasks.)

References:

1. https://learn.microsoft.com/en-us/windows/win32/wcn/about-windows-connect-now
2. GRID: MS-00000277

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.6.21 Windows Connection Manager

This section contains recommendations for Windows Connection Manager settings.

This Group Policy section is provided by the Group Policy template `WCM.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.6.21.1 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' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting prevents computers from establishing multiple simultaneous connections to either the Internet or to a Windows domain.

The recommended state for this setting is: `Enabled: 3 = Prevent Wi-Fi when on Ethernet`.

Rationale:

Preventing bridged network connections can help prevent a user unknowingly allowing traffic to route between internal and external networks, which risks exposure to sensitive internal data.

Impact:

While connected to an Ethernet connection, Windows won't allow use of a WLAN (automatically *or* manually) until Ethernet is disconnected. However, if a cellular data connection is available, it will always stay connected for services that require it, but no Internet traffic will be routed over cellular if an Ethernet or WLAN connection is present.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `3`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WcmSvc\GroupPolicy:fMinimizeConnections
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: 3 = Prevent Wi-Fi when on Ethernet`:

```
Computer Configuration\Policies\Administrative Templates\Network\Windows
Connection Manager\Minimize the number of simultaneous connections to the
Internet or a Windows Domain
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WCM.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates. It was updated with a new *Minimize Policy Options* sub-setting starting with the Windows 10 version 1903 Administrative Templates.

Default Value:

Enabled: 1 = Minimize simultaneous connections. (Any new automatic internet connection is blocked when the computer has at least one active internet connection to a preferred type of network. The order of preference (from most preferred to least preferred) is: Ethernet, WLAN, then cellular. Ethernet is always preferred when connected. Users can still manually connect to any network.)

References:

1. GRID: MS-00000278

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	15.5 Limit Wireless Access on Client Devices Configure wireless access on client machines that do have an essential wireless business purpose, to allow access only to authorized wireless networks and to restrict access to other wireless networks.			●

18.6.21.2 Ensure 'Prohibit connection to non-domain networks when connected to domain authenticated network' is set to 'Enabled' (MS only) (Automated)

Profile Applicability:

- Level 2 - Member Server

Description:

This policy setting prevents computers from connecting to both a domain based network and a non-domain based network at the same time.

The recommended state for this setting is: `Enabled`.

Rationale:

The potential concern is that a user would unknowingly allow network traffic to flow between the insecure public network and the enterprise managed network.

Impact:

The computer responds to automatic and manual network connection attempts based on the following circumstances:

Automatic connection attempts - When the computer is already connected to a domain based network, all automatic connection attempts to non-domain networks are blocked. - When the computer is already connected to a non-domain based network, automatic connection attempts to domain based networks are blocked.

Manual connection attempts - When the computer is already connected to either a non-domain based network or a domain based network over media other than Ethernet, and a user attempts to create a manual connection to an additional network in violation of this policy setting, the existing network connection is disconnected and the manual connection is allowed. - When the computer is already connected to either a non-domain based network or a domain based network over Ethernet, and a user attempts to create a manual connection to an additional network in violation of this policy setting, the existing Ethernet connection is maintained and the manual connection attempt is blocked.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\WcmSvc\GroupPolicy:fBlockNonDomain
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Network\Windows
Connection Manager\Prohibit connection to non-domain networks when connected
to domain authenticated network
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WCM.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Disabled. (Connections to both domain and non-domain networks are simultaneously allowed.)

References:

1. GRID: MS-00000279

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	12.4 Deny Communication over Unauthorized Ports Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.	●	●	●

18.7 Printers

This section contains recommendations for printer settings.

This Group Policy section is provided by the Group Policy template `Printing.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.7.1 Ensure 'Allow Print Spooler to accept client connections' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls whether the Print Spooler service will accept client connections.

The recommended state for this setting is: `Disabled`.

Note: The Print Spooler service must be restarted for changes to this policy to take effect.

Warning: An exception to this recommendation must be made for print servers in order for them to function properly. Users will not be able to print to the server when client connections are disabled.

Rationale:

Disabling the ability for the Print Spooler service to accept client connections mitigates **remote** attacks against the PrintNightmare vulnerability (CVE-2021-34527) and other **remote** Print Spooler attacks. However, this recommendation *does not* mitigate against **local** attacks on the Print Spooler service.

Impact:

Provided that the Print Spooler service is not disabled, applications on and users logged in to servers will continue to be able to print *from the server*. However, the Print Spooler service will not accept client connections or allow users to share printers. Note that all printers that were already shared will continue to be shared.

Warning: An exception to this recommendation must be made for print servers in order for them to function properly. Users will not be able to print to the server when client connections are disabled.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `2`.

```
HKLM\Software\Policies\Microsoft\Windows
NT\Printers:RegisterSpoolerRemoteRpcEndPoint
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Printers:Allow Print
Spooler to accept client connections
```

Note: This Group Policy path is provided by the Group Policy template `Printing2.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Enabled. (The Print Spooler will always accept client connections.)

References:

1. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527
2. GRID: MS-00000281

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●

18.7.2 Ensure 'Configure Redirection Guard' is set to 'Enabled: Redirection Guard Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether Redirection Guard is enabled for the print spooler. Redirection Guard can prevent file redirections from being used within the print spooler.

The recommended state for this setting is: `Enabled: Redirection Guard Enabled`.

Rationale:

This setting prevents non-administrators from redirecting files within the print spooler process.

Impact:

None - this is default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Printers:RedirectionguardPolicy
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Redirection Guard Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Printers\Configure
Redirection Guard
```

Note: This Group Policy path is provided by the Group Policy template `Printing.admx/adml` that is included with the Microsoft Windows 11 version 22H2 Administrative Templates v1.0 (or newer).

Default Value:

Disabled. (Redirection Guard will default to being "Enabled".)

References:

1. https://techcommunity.microsoft.com/t5/microsoft-security-baselines/windows-11-version-22h2-security-baseline/ba-p/3632520
2. GRID: MS-00000282

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●

18.7.3 Ensure 'Configure RPC connection settings: Protocol to use for outgoing RPC connections' is set to 'Enabled: RPC over TCP' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls which protocol and protocol settings to use for outgoing Remote Procedure Call (RPC) connections to a remote print spooler.

The recommended state for this setting is: `Enabled: RPC over TCP`

Rationale:

This setting prevents the use of named pipes for RPC connections to the print spooler and forces the use of TCP which is a more secure communication method.

Impact:

Warning: Many existing print configurations may be using the older named pipes protocol and therefore will cease to function.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows
NT\Printers\RPC:RpcUseNamedPipeProtocol
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: RPC over TCP`:

```
Computer Configuration\Policies\Administrative Templates\Printers\Configure
RPC connection settings: Protocol to use for outgoing RPC connections
```

Note: This Group Policy path is provided by the Group Policy template `Printing.admx/adml` that is included with the Microsoft Windows 11 version 22H2 Administrative Templates v1.0 (or newer).

Default Value:

Disabled. (By default, RPC over TCP is used. For RPC over named pipes, authentication is always enabled for domain joined machines but disabled for non-domain joined machines.)

References:

1. https://learn.microsoft.com/en-us/troubleshoot/windows-client/printing/windows-11-rpc-connection-updates-for-print#allow-rpc-over-tcp-communication
2. GRID: MS-00000283

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

18.7.4 Ensure 'Configure RPC connection settings: Use authentication for outgoing RPC connections' is set to 'Enabled: Default' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls which protocol and protocol settings to use for outgoing Remote Procedure Call (RPC) connections to a remote print spooler.

The recommended state for this setting is: `Enabled: Default`

Rationale:

This setting can prevent the use of named pipes for RPC connections to the print spooler and forces the use of TCP which is a more secure communication method.

Impact:

Warning: Many existing print configurations may be using the older named pipes protocol and therefore will cease to function.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Printers\RPC:RpcAuthentication
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Default`:

```
Computer Configuration\Policies\Administrative Templates\Printers\Configure
RPC connection settings: Use authentication for outgoing RPC connections
```

Note: This Group Policy path is provided by the Group Policy template `Printing.admx/adml` that is included with the Microsoft Windows 11 version 22H2 Administrative Templates v1.0 (or newer).

Default Value:

Disabled. (By default, RPC over TCP is used. For RPC over named pipes, authentication is always enabled for domain joined machines but disabled for non-domain joined machines.)

References:

1. https://learn.microsoft.com/en-us/troubleshoot/windows-client/printing/windows-11-rpc-connection-updates-for-print#allow-rpc-over-tcp-communication
2. GRID: MS-00000284

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

18.7.5 Ensure 'Configure RPC listener settings: Protocols to allow for incoming RPC connections' is set to 'Enabled: RPC over TCP' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls which protocols incoming Remote Procedure Call (RPC) connections to the print spooler are allowed to use.

The recommended state for this setting is: `Enabled: RPC over TCP`.

Rationale:

This setting can prevent the use of named pipes for RPC connections to the print spooler and forces the use of TCP which is a more secure communication method.

Impact:

Warning: Many existing print configurations may be using the older named pipes protocol and therefore will cease to function.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `5`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows
NT\Printers\RPC:RpcProtocols
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: RCP over TCP`:

```
Computer Configuration\Policies\Administrative Templates\Printers\Configure
RPC listener settings: Configure protocol options for incoming RPC
connections
```

Note: This Group Policy path is provided by the Group Policy template `Printing.admx/adml` that is included with the Microsoft Windows 11 version 22H2 Administrative Templates v1.0 (or newer).

Default Value:

Enabled. (RPC over TCP is enabled and Negotiate is used for the authentication protocol.)

References:

1. GRID: MS-00000285

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

18.7.6 Ensure 'Configure RPC listener settings: Authentication protocol to use for incoming RPC connections:' is set to 'Enabled: Negotiate' or higher (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls which protocols incoming Remote Procedure Call (RPC) connections to the print spooler are allowed to use.

The recommended state for this setting is: `Enabled: Negotiate` or `Enabled: Kerberos`.

Rationale:

This setting can prevent the use of named pipes for RPC connections to the print spooler and forces the use of TCP which is a more secure communication method.

Impact:

Warning: Many existing print configurations may be using the older named pipes protocol and therefore will cease to function.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0` or `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Printers\RPC:ForceKerberosForRpc
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Negotiate` or `Enabled: Kerberos`:

```
Computer Configuration\Policies\Administrative Templates\Printers\Configure
RPC listener settings: Configure protocol options for incoming RPC
connections
```

Note: This Group Policy path is provided by the Group Policy template `Printing.admx/adml` that is included with the Microsoft Windows 11 version 22H2 Administrative Templates v1.0 (or newer).

Default Value:

Enabled. (RPC over TCP is enabled and Negotiate is used for the authentication protocol.)

References:

1. GRID: MS-00000286

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

18.7.7 Ensure 'Configure RPC over TCP port' is set to 'Enabled: 0' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls which port is used for RPC over TCP for incoming connections to the print spooler and outgoing connections to remote print spoolers.

The recommended state for this setting is: `Enabled: 0`.

Rationale:

Using dynamic ports for printing makes it more difficult for a threat actor to know which port is being used and therefore which port to attack.

Impact:

If your current print environment is configured for a specific TCP port, this setting may require a firewall change (if applicable) for continued printing.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Printers\RPC:RpcTcpPort
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: 0`:

```
Computer Configuration\Policies\Administrative Templates\Printers\Configure
RPC over TCP port
```

Note: This Group Policy path is provided by the Group Policy template `Printing.admx/adml` that is included with the Microsoft Windows 11 version 22H2 Administrative Templates v1.0 (or newer).

Default Value:

Disabled. (Dynamic TCP ports are used)

References:

1. GRID: MS-00000287

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

18.7.8 Ensure 'Configure RPC packet level privacy setting for incoming connections' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls packet level privacy for Remote Procedure Call (RPC) incoming connections.

The recommended state for this setting is: `Enabled`.

Rationale:

A security bypass vulnerability (CVE-2021-1678 | Windows Print Spooler Spoofing Vulnerability) exists in the way the Printer RPC binding handles authentication for the remote Winspool interface. Enabling the RPC packet level privacy setting for incoming connections enforces the server-side to increase the authentication level to minimize this vulnerability.

Impact:

None - this is default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SYSTEM\CurrentControlSet\Control\Print:RpcAuthnLevelPrivacyEnabled
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\MS Security
Guide\Configure RPC packet level privacy setting for incoming connections
```

Note: This Group Policy path is provided by the Group Policy template `Printing.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Enabled. (Packet level privacy is enabled for RPC for incoming connections.)

References:

1. https://support.microsoft.com/en-us/topic/managing-deployment-of-printer-rpc-binding-changes-for-cve-2021-1678-kb4599464-12a69652-30b9-3d61-d9f7-7201623a8b25
2. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-1678
3. GRID: MS-00000241

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

18.7.9 Ensure 'Limits print driver installation to Administrators' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls whether users who aren't Administrators can install print drivers on the system.

The recommended state for this setting is: `Enabled`.

Note: On August 10, 2021, Microsoft announced a Point and Print Default Behavior Change which modifies the default Point and Print driver installation and update behavior to require Administrator privileges. This is documented in KB5005652—Manage new Point and Print default driver installation behavior (CVE-2021-34481).

Rationale:

Restricting the installation of print drives to Administrators can help mitigate the PrintNightmare vulnerability (CVE-2021-34527) and other Print Spooler attacks.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows
NT\Printers\PointAndPrint:RestrictDriverInstallationToAdministrators
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`.

```
Computer Configuration\Policies\Administrative Templates\Printers\Limits
print driver installation to Administrators
```

Note: This Group Policy path is provided by the Group Policy template `Printing.admx/adml` that is included with the Microsoft Windows 10 version 21H2 Administrative Templates (or newer).

Default Value:

Enabled. (The system will limit installation of print drivers to Administrators of the computer.)

References:

1. https://support.microsoft.com/en-us/topic/kb5005010-restricting-installation-of-new-printer-drivers-after-applying-the-july-6-2021-updates-31b91c02-05bc-4ada-a7ea-183b129578a7
2. https://support.microsoft.com/en-gb/topic/kb5005652-manage-new-point-and-print-default-driver-installation-behavior-cve-2021-34481-873642bf-2634-49c5-a23b-6d8e9a302872
3. GRID: MS-00000288

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

18.7.10 Ensure 'Manage processing of Queue-specific files' is set to 'Enabled: Limit Queue-specific files to Color profiles' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting manages how queue-specific files are processed during printer installation. At printer installation time, a vendor-supplied installation application can specify a set of files, of any type, to be associated with a particular print queue. The files are downloaded to each client that connects to the print server.

The recommended state for this setting is: `Enabled: Limit Queue-specific files to Color profiles`.

Rationale:

A Windows Print Spooler Remote Code Execution Vulnerability (CVE-2021-36958) exists when the Windows Print Spooler service improperly performs privileged file operations. A threat actor who successfully exploits this vulnerability could run arbitrary code with SYSTEM privileges and then install programs; view, change, or delete data; or create new accounts with full user rights.

Impact:

None - this is default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Printers:CopyFilesPolicy
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Limit Queue-specific files to Color profiles`:

```
Computer Configuration\Policies\Administrative Templates\Printers\Manage
processing of Queue-specific files
```

Note: This Group Policy path is provided by the Group Policy template `Printing.admx/adml` that is included with the Microsoft Windows 11 version 22H2 Administrative Templates v1.0 (or newer).

Default Value:

Disabled. (Queue-specific files will be limited to Color profiles.)

References:

1. https://learn.microsoft.com/en-us/windows-hardware/drivers/print/installing-queue-specific-files
2. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36958
3. GRID: MS-00000289

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●

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

Profile Applicability:

- Level 1 - Member Server
- Level 1 - Domain Controller

Description:

This policy setting controls whether computers will show a warning and a security elevation prompt when users create a new printer connection using Point and Print.

The recommended state for this setting is: `Enabled: Show warning and elevation prompt`.

Note: On August 10, 2021, Microsoft announced a Point and Print Default Behavior Change which modifies the default Point and Print driver installation and update behavior to require Administrator privileges. This is documented in KB5005652—Manage new Point and Print default driver installation behavior (CVE-2021-34481). This change overrides all Point and Print Group Policy settings and ensures that only Administrators can install printer drivers from a print server using Point and Print.

Rationale:

Enabling Windows User Account Control (UAC) for the installation of new print drivers can help mitigate the PrintNightmare vulnerability (CVE-2021-34527) and other Print Spooler attacks.

Although the Point and Print default driver installation behavior overrides this setting, it is important to configure this as a backstop in the event that behavior is reversed.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\Software\Policies\Microsoft\Windows
NT\Printers\PointAndPrint:NoWarningNoElevationOnInstall
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Show warning and elevation prompt`:

```
Computer Configuration\Policies\Administrative Templates\Printers\Point and
Print Restrictions: When installing drivers for a new connection
```

Note: This Group Policy path is provided by the Group Policy template `Printing.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Enabled. (Windows computers will show a warning and a security elevation prompt when users create a new printer connection using Point and Print.)

References:

1. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-1675
2. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34481
3. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527
4. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36958
5. https://msrc-blog.microsoft.com/2021/08/10/point-and-print-default-behavior-change/
6. https://support.microsoft.com/en-us/topic/kb5005652-manage-new-point-and-print-default-driver-installation-behavior-cve-2021-34481-873642bf-2634-49c5-a23b-6d8e9a302872
7. GRID: MS-00000290

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

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

Profile Applicability:

- Level 1 - Member Server
- Level 1 - Domain Controller

Description:

This policy setting controls whether computers will show a warning and a security elevation prompt when users are updating drivers for an existing connection using Point and Print.

The recommended state for this setting is: `Enabled: Show warning and elevation prompt`.

Note: On August 10, 2021, Microsoft announced a Point and Print Default Behavior Change which modifies the default Point and Print driver installation and update behavior to require Administrator privileges. This is documented in KB5005652—Manage new Point and Print default driver installation behavior (CVE-2021-34481). This change overrides all Point and Print Group Policy settings and ensures that only Administrators can install printer drivers from a print server using Point and Print.

Rationale:

Enabling Windows User Account Control (UAC) for updating existing print drivers can help mitigate the PrintNightmare vulnerability (CVE-2021-34527) and other Print Spooler attacks.

Although the Point and Print default driver installation behavior overrides this setting, it is important to configure this as a backstop in the event that behavior is reversed.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\Software\Policies\Microsoft\Windows
NT\Printers\PointAndPrint:UpdatePromptSettings
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Show warning and elevation prompt`:

```
Computer Configuration\Policies\Administrative Templates\Printers\Point and
Print Restrictions: When updating drivers for an existing connection
```

Note: This Group Policy path is provided by the Group Policy template `Printing.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Enabled. (Windows computers will show a warning and a security elevation prompt when users are updating drivers for an existing connection using Point and Print.)

References:

1. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-1675
2. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34481
3. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527
4. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36958
5. https://msrc-blog.microsoft.com/2021/08/10/point-and-print-default-behavior-change/
6. https://support.microsoft.com/en-us/topic/kb5005652-manage-new-point-and-print-default-driver-installation-behavior-cve-2021-34481-873642bf-2634-49c5-a23b-6d8e9a302872
7. GRID: MS-00000291

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

18.8 Start Menu and Taskbar

This section contains recommendations for Start Menu and Taskbar.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.8.1 Notifications

This section contains recommendations for Start Menu and Taskbar Notifications.

This Group Policy section is provided by the Group Policy template `WPN.admx/adml` that is included with the Microsoft 10 version 1803 Administrative Templates (or newer).

18.8.1.1 Ensure 'Turn off notifications network usage' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting blocks applications from using the network to send notifications to update tiles, tile badges, toast, or raw notifications. This policy setting turns off the connection between Windows and the Windows Push Notification Service (WNS). This policy setting also stops applications from being able to poll application services to update tiles.

The recommended state for this setting is: `Enabled`.

Rationale:

Windows Push Notification Services (WNS) is a mechanism to receive third-party notifications and updates from the cloud/Internet. In a high security environment, external systems, especially those hosted outside the organization, should be prevented from having an impact on the secure workstations.

Impact:

Applications and system features will not be able receive notifications from the network from WNS or via notification polling APIs.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\PushNotifications:NoC
loudApplicationNotification
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Start Menu and
Taskbar\Turn off notifications network usage
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WPN.admx/adml` that is included with the Microsoft Windows 10 version 1607 & Server 2016 Administrative Templates (or newer).

Default Value:

Disabled.

References:

1. GRID: MS-00000293

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.9 System

This section contains recommendations for System settings.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.1 Access-Denied Assistance

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `srm-fci.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.9.2 App-V

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `appv.admx/adml` that is included with the Microsoft Windows 10 version 1607 & Server 2016 Administrative Templates (or newer).

18.9.3 Audit Process Creation

This section contains settings related to auditing of process creation events.

This Group Policy section is provided by the Group Policy template `AuditSettings.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.9.3.1 Ensure 'Include command line in process creation events' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls whether the process creation command line text is logged in security audit events when a new process has been created.

The recommended state for this setting is: `Enabled`.

Note: This feature that this setting controls was not originally supported in server OSes older than Windows Server 2012 R2. However, in February 2015 Microsoft added support for the feature to Windows Server 2008 R2 and Windows Server 2012 (non-R2) via an update - KB3004375. Therefore, this setting is also important to set on those older OSes.

Rationale:

Capturing process command line information in event logs can be very valuable when performing forensic investigations of attack incidents.

Impact:

Process command line information will be included in the event logs, which can contain sensitive or private information such as passwords or user data.

Warning: There are potential risks of capturing credentials and sensitive information which could be exposed to users who have read-access to event logs. Microsoft provides a feature called "Protected Event Logging" to better secure event log data. For assistance with protecting event logging, visit: About Logging Windows - PowerShell | Microsoft Docs.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\Audit:ProcessC
reationIncludeCmdLine_Enabled
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\System\Audit Process Creation\Include command line in process creation events
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `AuditSettings.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Default Value:

Disabled. (The process's command line information will not be included in Audit Process Creation events.)

References:

1. https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_logging_windows?view=powershell-7.2#protected-event-logging
2. GRID: MS-00000294

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.8 Collect Command-Line Audit Logs Collect command-line audit logs. Example implementations include collecting audit logs from PowerShell®, BASH™, and remote administrative terminals.		●	●
v7	8.8 Enable Command-line Audit Logging Enable command-line audit logging for command shells, such as Microsoft Powershell and Bash.		●	●

18.9.4 Credentials Delegation

This section contains settings related to Credential Delegation.

This Group Policy section is provided by the Group Policy template `CredSsp.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.4.1 Ensure 'Encryption Oracle Remediation' is set to 'Enabled: Force Updated Clients' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Some versions of the CredSSP protocol that is used by some applications (such as Remote Desktop Connection) are vulnerable to an encryption oracle attack against the client. This policy controls compatibility with vulnerable clients and servers and allows you to set the level of protection desired for the encryption oracle vulnerability.

The recommended state for this setting is: `Enabled: Force Updated Clients`.

Rationale:

This setting is important to mitigate the CredSSP encryption oracle vulnerability, for which information was published by Microsoft on 03/13/2018 in CVE-2018-0886 | CredSSP Remote Code Execution Vulnerability. All versions of Windows Server from Server 2008 (non-R2) onwards are affected by this vulnerability, and will be compatible with this recommendation provided that they have been patched up through May 2018 (or later).

Impact:

Client applications which use CredSSP will not be able to fall back to the insecure versions and services using CredSSP will not accept unpatched clients. This setting should not be deployed until all remote hosts support the newest version, which is achieved by ensuring that all Microsoft security updates at least through May 2018 are installed.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\CredSSP\Parame
ters:AllowEncryptionOracle
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Force Updated Clients`:

```
Computer Configuration\Policies\Administrative Templates\System\Credentials
Delegation\Encryption Oracle Remediation
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `CredSsp.admx/adml` that is included with the Microsoft Windows 10 version 1803 Administrative Templates (or newer).

Default Value:

Without the May 2018 security update: Enabled: Vulnerable (Client applications which use CredSSP will expose the remote servers to attacks by supporting fall back to the insecure versions and services using CredSSP will accept unpatched clients.)

With the May 2018 security update: Enabled: Mitigated (Client applications which use CredSSP will not be able to fall back to the insecure version but services using CredSSP will accept unpatched clients.)

References:

1. GRID: MS-00000295

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	3.4 Deploy Automated Operating System Patch Management Tools Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.	●	●	●

18.9.4.2 Ensure 'Remote host allows delegation of non-exportable credentials' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

When using credential delegation, devices provide an exportable version of credentials to the remote host. This exposes users to the risk of credential theft from threat actors on the remote host. The Restricted Admin Mode and Windows Defender Remote Credential Guard features are two options to help protect against this risk.

The recommended state for this setting is: `Enabled`.

Note: More detailed information on Windows Defender Remote Credential Guard and how it compares to Restricted Admin Mode can be found at this link: Protect Remote Desktop credentials with Windows Defender Remote Credential Guard (Windows 10) | Microsoft Docs

Rationale:

Restricted Admin Mode was designed to help protect administrator accounts by ensuring that reusable credentials are not stored in memory on remote devices that could potentially be compromised. *Windows Defender Remote Credential Guard* helps you protect your credentials over a Remote Desktop connection by redirecting Kerberos requests back to the device that is requesting the connection. Both features should be enabled and supported, as they reduce the chance of credential theft.

Impact:

The host will support the *Restricted Admin Mode* and *Windows Defender Remote Credential Guard* features.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\CredentialsDelegation:AllowProtectedCreds
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\System\Credentials
Delegation\Remote host allows delegation of non-exportable credentials
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `CredSsp.admx/adml` that is included with the Microsoft Windows 10 version 1703 Administrative Templates (or newer).

Default Value:

Disabled. (*Restricted Admin Mode* and *Windows Defender Remote Credential Guard* are not supported. Users will always need to pass their credentials to the host.)

References:

1. https://docs.microsoft.com/en-us/windows/security/identity-protection/remote-credential-guard
2. GRID: MS-00000296

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	16.5 Encrypt Transmittal of Username and Authentication Credentials Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.		●	●

18.9.5 Device Guard

This section contains Device Guard settings.

This Group Policy section is provided by the Group Policy template `DeviceGuard.admx/adml` that is included with the Microsoft Windows 10 RTM (version 1507) Administrative Templates (or newer).

18.9.5.1 Ensure 'Turn On Virtualization Based Security' is set to 'Enabled' (Automated)

Profile Applicability:

- Next Generation Windows Security - Domain Controller
- Next Generation Windows Security - Member Server

Description:

This policy setting specifies whether Virtualization Based Security is enabled. Virtualization Based Security uses the Windows Hypervisor to provide support for security services.

The recommended state for this setting is: `Enabled`

Note: Virtualization Based Security requires a 64-bit version of Windows with Secure Boot enabled, which in turn requires that Windows was installed with a UEFI BIOS configuration, not a Legacy BIOS configuration. In addition, if running Windows on a virtual machine, the hardware-assisted CPU virtualization feature (Intel VT-x or AMD-V) must be exposed by the host to the guest VM.

More information on system requirements for this feature can be found at Windows Defender Credential Guard Requirements (Windows 10) | Microsoft Docs

Note #2: Credential Guard and Device Guard are not currently supported when using Azure IaaS VMs.

Rationale:

Kerberos, NTLM, and Credential manager isolate secrets by using virtualization-based security. Previous versions of Windows stored secrets in the Local Security Authority (LSA). Prior to Windows 10, the LSA stored secrets used by the operating system in its process memory. With Windows Defender Credential Guard enabled, the LSA process in the operating system talks to a new component called the isolated LSA process that stores and protects those secrets. Data stored by the isolated LSA process is protected using virtualization-based security and is not accessible to the rest of the operating system.

Impact:

Warning: All drivers on the system must be compatible with this feature or the system may crash. Ensure that this policy setting is only deployed to computers which are known to be compatible.

Warning #2: Enabling Windows Defender Credential Guard on Domain Controllers is not supported. The domain controller hosts authentication services which integrate with processes isolated when Windows Defender Credential Guard is enabled, causing crashes.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\DeviceGuard:EnableVirtualizationBase
dSecurity
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\System\Device
Guard\Turn On Virtualization Based Security
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `DeviceGuard.admx/adml` that is included with the Microsoft Windows 10 RTM (version 1507) Administrative Templates (or newer).

Default Value:

Disabled.

References:

1. GRID: MS-00000297

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

18.9.5.2 Ensure 'Turn On Virtualization Based Security: Select Platform Security Level' is set to 'Secure Boot' or higher (Automated)

Profile Applicability:

- Next Generation Windows Security - Domain Controller
- Next Generation Windows Security - Member Server

Description:

This policy setting specifies whether Virtualization Based Security (VBS) is enabled. VBS uses the Windows Hypervisor to provide support for security services.

The recommended state for this setting is: `Secure Boot`. Configuring this setting to `Secure Boot and DMA Protection` also conforms to the benchmark.

Note: VBS requires a 64-bit version of Windows with Secure Boot enabled, which in turn requires that Windows was installed with a UEFI BIOS configuration, not a Legacy BIOS configuration. In addition, if running Windows on a virtual machine, the hardware-assisted CPU virtualization feature (Intel VT-x or AMD-V) must be exposed by the host to the guest VM.

More information on system requirements for this feature can be found at Windows Defender Credential Guard Requirements (Windows 10) | Microsoft Docs

Note #2: Credential Guard and Device Guard are not currently supported when using Azure IaaS VMs.

Rationale:

Secure Boot can help reduce the risk of bootloader attacks and in conjunction with DMA protections to help protect data from being scraped from memory.

Impact:

Choosing the `Secure Boot` option provides the system with as much protection as is supported by the computer's hardware. A system with input/output memory management units (IOMMUs) will have Secure Boot with DMA protection. A system without IOMMUs will simply have Secure Boot enabled without DMA protection.

Choosing the `Secure Boot with DMA protection` option requires the system to have IOMMUs in order to enable VBS. Without IOMMU hardware support, VBS will be disabled.

Warning: All drivers on the system must be compatible with this feature or the system may crash. Ensure that this policy setting is only deployed to computers which are known to be compatible.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`or `3`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DeviceGuard:RequirePla
tformSecurityFeatures
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Secure Boot` or `Secure Boot and DMA Protection`:

```
Computer Configuration\Policies\Administrative Templates\System\Device
Guard\Turn On Virtualization Based Security: Select Platform Security Level
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `DeviceGuard.admx/adml` that is included with the Microsoft Windows 10 RTM (version 1507) Administrative Templates (or newer).

Default Value:

Disabled.

References:

1. GRID: MS-00000302

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

18.9.5.3 Ensure 'Turn On Virtualization Based Security: Virtualization Based Protection of Code Integrity' is set to 'Enabled with UEFI lock' (Automated)

Profile Applicability:

- Next Generation Windows Security - Domain Controller
- Next Generation Windows Security - Member Server

Description:

This setting enables virtualization based protection of Kernel Mode Code Integrity. When this is enabled, kernel mode memory protections are enforced and the Code Integrity validation path is protected by the Virtualization Based Security feature.

The recommended state for this setting is: `Enabled with UEFI lock`

Note: Virtualization Based Security requires a 64-bit version of Windows with Secure Boot enabled, which in turn requires that Windows was installed with a UEFI BIOS configuration, not a Legacy BIOS configuration. In addition, if running Windows on a virtual machine, the hardware-assisted CPU virtualization feature (Intel VT-x or AMD-V) must be exposed by the host to the guest VM.

More information on system requirements for this feature can be found at Windows Defender Credential Guard Requirements (Windows 10) | Microsoft Docs

Note #2: Credential Guard and Device Guard are not currently supported when using Azure IaaS VMs.

Rationale:

The `Enabled with UEFI lock` option ensures that Virtualization Based Protection of Code Integrity cannot be disabled remotely.

Impact:

Warning: All drivers on the system must be compatible with this feature or the system may crash. Ensure that this policy setting is only deployed to computers which are known to be compatible.

Warning #2: Once this setting is turned on and active, **Virtualization Based Security cannot be disabled solely via GPO** or any other remote method. After removing the setting from GPO, the features must also be manually disabled *locally at the machine* using the steps provided at this link:

Manage Windows Defender Credential Guard (Windows 10) | Microsoft Docs

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\DeviceGuard:HypervisorEnforcedCodeIntegrity
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled with UEFI lock`:

```
Computer Configuration\Policies\Administrative Templates\System\Device Guard\Turn On Virtualization Based Security: Virtualization Based Protection of Code Integrity
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `DeviceGuard.admx/adml` that is included with the Microsoft Windows 10 RTM (version 1507) Administrative Templates (or newer).

Default Value:

Disabled.

References:

1. GRID: MS-00000303

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

18.9.5.4 Ensure 'Turn On Virtualization Based Security: Require UEFI Memory Attributes Table' is set to 'True (checked)' (Automated)

Profile Applicability:

- Next Generation Windows Security - Domain Controller
- Next Generation Windows Security - Member Server

Description:

This option will only enable Virtualization Based Protection of Code Integrity on devices with UEFI firmware support for the Memory Attributes Table. Devices without the UEFI Memory Attributes Table may have firmware that is incompatible with Virtualization Based Protection of Code Integrity which in some cases can lead to crashes or data loss or incompatibility with certain plug-in cards. If not setting this option the targeted devices should be tested to ensure compatibility.

The recommended state for this setting is: `True (checked)`

Note: Virtualization Based Security requires a 64-bit version of Windows with Secure Boot enabled, which in turn requires that Windows was installed with a UEFI BIOS configuration, not a Legacy BIOS configuration. In addition, if running Windows on a virtual machine, the hardware-assisted CPU virtualization feature (Intel VT-x or AMD-V) must be exposed by the host to the guest VM.

More information on system requirements for this feature can be found at Windows Defender Credential Guard Requirements (Windows 10) | Microsoft Docs

Note #2: Credential Guard and Device Guard are not currently supported when using Azure IaaS VMs.

Rationale:

This setting will help protect this control from being enabled on a system that is not compatible which could lead to a crash or data loss.

Impact:

Warning: All drivers on the system must be compatible with this feature or the system may crash. Ensure that this policy setting is only deployed to computers which are known to be compatible.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\DeviceGuard:HVCIMATRequired
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `TRUE`:

```
Computer Configuration\Policies\Administrative Templates\System\Device
Guard\Turn On Virtualization Based Security: Require UEFI Memory Attributes
Table
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `DeviceGuard.admx/adml` that is included with the Microsoft Windows 10 version 1703 Administrative Templates (or newer).

Default Value:

Disabled.

References:

1. GRID: MS-00000300

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

18.9.5.5 Ensure 'Turn On Virtualization Based Security: Credential Guard Configuration' is set to 'Enabled with UEFI lock' (MS Only) (Automated)

Profile Applicability:

- Next Generation Windows Security - Member Server

Description:

This setting lets users turn on Credential Guard with virtualization-based security to help protect credentials. The "Enabled with UEFI lock" option ensures that Credential Guard cannot be disabled remotely. In order to disable the feature, you must set the Group Policy to "Disabled" as well as remove the security functionality from each computer, with a physically present user, in order to clear configuration persisted in UEFI.

The recommended state for this setting is: `Enabled with UEFI lock`, *but only on Member Servers (not Domain Controllers).*

Note: Virtualization Based Security requires a 64-bit version of Windows with Secure Boot enabled, which in turn requires that Windows was installed with a UEFI BIOS configuration, not a Legacy BIOS configuration. In addition, if running Windows on a virtual machine, the hardware-assisted CPU virtualization feature (Intel VT-x or AMD-V) must be exposed by the host to the guest VM.

More information on system requirements for this feature can be found at Windows Defender Credential Guard Requirements (Windows 10) | Microsoft Docs

Note #2: Credential Guard and Device Guard are not currently supported when using Azure IaaS VMs.

Rationale:

The `Enabled with UEFI lock` option ensures that Credential Guard cannot be disabled remotely.

Impact:

Warning: All drivers on the system must be compatible with this feature or the system may crash. Ensure that this policy setting is only deployed to computers which are known to be compatible.

Warning #2: Enabling Windows Defender Credential Guard on Domain Controllers is not supported. The domain controller hosts authentication services which integrate with processes isolated when Windows Defender Credential Guard is enabled, causing crashes.

Warning #3: Once this setting is turned on and active, **Credential Guard cannot be disabled solely via GPO** or any other remote method. After removing the setting from GPO, the features must also be manually disabled *locally at the machine* using the steps provided at this link:

Manage Windows Defender Credential Guard (Windows 10) | Microsoft Docs

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\DeviceGuard:LsaCfgFlags
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled with UEFI lock` (on Member Servers only):

```
Computer Configuration\Policies\Administrative Templates\System\Device
Guard\Turn On Virtualization Based Security: Credential Guard Configuration
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `DeviceGuard.admx/adml` that is included with the Microsoft Windows 10 version 1511 Administrative Templates (or newer).

Default Value:

Disabled.

References:

1. GRID: MS-00000298

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

18.9.5.6 Ensure 'Turn On Virtualization Based Security: Credential Guard Configuration' is set to 'Disabled' (DC Only) (Automated)

Profile Applicability:

- Next Generation Windows Security - Domain Controller

Description:

This setting lets users turn on Credential Guard with virtualization-based security to help protect credentials.

The recommended state for this setting is: `Disabled` *on Domain Controllers*.

Note: Virtualization Based Security requires a 64-bit version of Windows with Secure Boot enabled, which in turn requires that Windows was installed with a UEFI BIOS configuration, not a Legacy BIOS configuration. In addition, if running Windows on a virtual machine, the hardware-assisted CPU virtualization feature (Intel VT-x or AMD-V) must be exposed by the host to the guest VM.

More information on system requirements for this feature can be found at Windows Defender Credential Guard Requirements (Windows 10) | Microsoft Docs

Note #2: Credential Guard and Device Guard are not currently supported when using Azure IaaS VMs.

Rationale:

Credential Guard is not useful on Domain Controllers and can cause crashes on them.

Impact:

None - this is the default behavior.

Warning: Enabling Windows Defender Credential Guard on Domain Controllers is not supported. The domain controller hosts authentication services which integrate with processes isolated when Windows Defender Credential Guard is enabled, causing crashes.

Manage Windows Defender Credential Guard (Windows 10) | Microsoft Docs

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\DeviceGuard:LsaCfgFlags
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\System\Device
Guard\Turn On Virtualization Based Security: Credential Guard Configuration
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `DeviceGuard.admx/adml` that is included with the Microsoft Windows 10 version 1511 Administrative Templates (or newer).

Default Value:

Disabled. (Credential Guard is disabled.)

References:

1. GRID: MS-00000298

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

18.9.5.7 Ensure 'Turn On Virtualization Based Security: Secure Launch Configuration' is set to 'Enabled' (Automated)

Profile Applicability:

- Next Generation Windows Security - Domain Controller
- Next Generation Windows Security - Member Server

Description:

Secure Launch protects the Virtualization Based Security environment from exploited vulnerabilities in device firmware.

The recommended state for this setting is: `Enabled`.

Note: Virtualization Based Security requires a 64-bit version of Windows with Secure Boot enabled, which in turn requires that Windows was installed with a UEFI BIOS configuration, not a Legacy BIOS configuration. In addition, if running Windows on a virtual machine, the hardware-assisted CPU virtualization feature (Intel VT-x or AMD-V) must be exposed by the host to the guest VM.

More information on system requirements for this feature can be found at Windows Defender Credential Guard Requirements (Windows 10) | Microsoft Docs

Note #2: Credential Guard and Device Guard are not currently supported when using Azure IaaS VMs.

Rationale:

Secure Launch changes the way windows boots to use Intel Trusted Execution Technology (TXT) and Runtime BIOS Resilience features to prevent firmware exploits from being able to impact the security of the Windows Virtualization Based Security environment.

Impact:

Warning: All drivers on the system must be compatible with this feature or the system may crash. Ensure that this policy setting is only deployed to computers which are known to be compatible.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\DeviceGuard:ConfigureSystemGuardLaun
ch
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\System\Device
Guard\Turn On Virtualization Based Security: Secure Launch Configuration
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `DeviceGuard.admx/adml` that is included with the Microsoft Windows 10 version 1809 & Server 2019 Administrative Templates (or newer).

Default Value:

Not Configured. (Administrative users can choose whether to enable or disable Secure Launch.)

References:

1. GRID: MS-00000301

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

18.9.6 Device Health Attestation Service

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `TPM.admx/adml` that is included with the Microsoft Windows 10 version 1709 Administrative Templates (or newer).

18.9.7 Device Installation

This section contains recommendations related to device installation.

This Group Policy section is provided by the Group Policy template `DeviceInstallation.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.7.1 Device Installation Restrictions

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `DeviceInstallation.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.7.2 Ensure 'Prevent automatic download of applications associated with device metadata' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to prevent Windows from retrieving device metadata from the Internet.

The recommended state for this setting is: `Enabled`.

Note: This will not prevent the installation of basic hardware drivers, but does prevent associated third-party utility software from automatically being installed under the context of the `SYSTEM` account.

Rationale:

Installation of software should be conducted by an authorized system administrator and not a standard user. Allowing automatic third-party software installations under the context of the `SYSTEM` account has potential for allowing unauthorized access via backdoors or installation software bugs.

Impact:

Standard users without administrator privileges will not be able to install associated third-party utility software for peripheral devices. This may limit the use of advanced features of those devices unless/until an administrator installs the associated utility software for the device.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\Device
Metadata:PreventDeviceMetadataFromNetwork
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\System\Device
Installation\Prevent automatic download of applications associated with
device metadata
```

Note: This Group Policy path is provided by the Group Policy template `DeviceInstallation.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates, or with the Group Policy template `DeviceSetup.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Prevent device metadata retrieval from the Internet*. It was renamed to *Prevent automatic download of applications associated with device metadata* starting with the Windows 11 version 25H2 Administrative Templates.

Default Value:

Disabled. (The setting in the Device Installation Settings dialog box controls whether Windows retrieves device metadata from the Internet.)

References:

1. GRID: MS-00000304

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	18.3 Verify That Acquired Software is Still Supported Verify that the version of all software acquired from outside your organization is still supported by the developer or appropriately hardened based on developer security recommendations.		●	●

18.9.8 Disk NV Cache

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `DiskNVCache.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.9 Disk Quotas

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `DiskQuota.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.10 Display

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Display.admx/adml` that is included with the Microsoft Windows 10 version 1703 Administrative Templates (or newer).

18.9.11 Distributed COM

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `DCOM.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.12 Driver Installation

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `DeviceInstallation.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.13 Early Launch Antimalware

This section contains recommendations for configuring boot-start driver initialization settings.

This Group Policy section is provided by the Group Policy template `EarlyLaunchAM.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

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

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to specify which boot-start drivers are initialized based on a classification determined by an Early Launch Antimalware boot-start driver. The Early Launch Antimalware boot-start driver can return the following classifications for each boot-start driver:

- `Good`: The driver has been signed and has not been tampered with.
- `Bad`: The driver has been identified as malware. It is recommended that you do not allow known bad drivers to be initialized.
- `Bad, but required for boot`: The driver has been identified as malware, but the computer cannot successfully boot without loading this driver.
- `Unknown`: This driver has not been attested to by your malware detection application and has not been classified by the Early Launch Antimalware boot-start driver.

If you enable this policy setting you will be able to choose which boot-start drivers to initialize the next time the computer is started.

If your malware detection application does not include an Early Launch Antimalware boot-start driver or if your Early Launch Antimalware boot-start driver has been disabled, this setting has no effect and all boot-start drivers are initialized.

The recommended state for this setting is: `Enabled: Good, unknown and bad but critical`.

Rationale:

This policy setting helps reduce the impact of malware that has already infected your system.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `3`.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Policies\EarlyLaunch:DriverLoadPolicy
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Good, unknown and bad but critical:`

```
Computer Configuration\Policies\Administrative Templates\System\Early Launch Antimalware\Boot-Start Driver Initialization Policy
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `EarlyLaunchAM.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Disabled. (Boot-start drivers determined to be Good, Unknown or Bad but Boot Critical are initialized and the initialization of drivers determined to be bad is skipped.)

References:

1. GRID: MS-00000311

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

18.9.14 Enhanced Storage Access

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `EnhancedStorage.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.9.15 File Classification Infrastructure

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `srm-fci.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.9.16 File Share Shadow Copy Provider

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy templates `FileServerVSSProvider.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.9.17 Filesystem (formerly NTFS Filesystem)

This section contains recommendations related to Filesystem.

This Group Policy section is provided by the Group Policy template `FileSys.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note: This section was initially named *NTFS Filesystem* but was renamed by Microsoft to *Filesystem* starting with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates.

18.9.17.1 Ensure 'Enable / disable CLFS logfile authentication' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting configures Common Log File System (CLFS) logfile authentication. Logfile authentication provides the ability for the CLFS driver to detect malicious modifications made to logfiles.

The recommended state for this setting is: `Enabled`.

Rationale:

CLFS is a security feature which hardens logfile parsing. If modifications to logfiles are detected, CLFS will consider the logfile unsafe for parsing and return an error to the caller. It is also able to detect modifications by writing authentication codes to logfiles which combines file data with a system-unique cryptographic key.

Impact:

None - this is the default behavior.

Warning: Logfiles that were created on other systems will fail to open as these contain authentication codes created using a system-unique cryptographic key. To open a logfile that was created on another system an administrator must first use the `fsutil.exe clfs authenticate` command to correct the authentication codes.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SYSTEM\CurrentControlSet\Policies:ClfsAuthenticationChecking
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative
Templates\System\Filesystem\Enable / disable CLFS logfile authentication
```

Note: This Group Policy path is provided by the Group Policy template `FileSys.admx/adml` that is included with the Microsoft Windows 11 version 25H2 Administrative Templates (or newer).

Default Value:

Enabled. (CLFS will perform logfile authentication.)

References:

1. GRID: MS-00000635
2. https://learn.microsoft.com/en-us/windows-hardware/drivers/kernel/introduction-to-the-common-log-file-system

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

18.9.18 Folder Redirection

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `FolderRedirection.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.19 Group Policy

This section contains recommendations for configuring group policy-related settings.

This Group Policy section is provided by the Group Policy template `GroupPolicy.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.19.1 Logging and tracing

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `GroupPolicyPreferences.admx/adml` that is included with the Microsoft Windows Server 2008 (non-R2) Administrative Templates (or newer).

18.9.19.2 Ensure 'Configure security policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

The "Do not apply during periodic background processing" option prevents the system from updating affected security policies in the background while the computer is in use. When background updates are disabled, updates to security policies will not take effect until the next user logon or system restart.

This setting affects all policy settings that use the built-in security template of Group Policy (e.g. Windows Settings\Security Settings).

The recommended state for this setting is: `Enabled: FALSE` (unchecked).

Rationale:

Setting this option to false (unchecked) will ensure that domain security policy changes are applied more quickly, as compared to waiting until the next user logon or system restart.

Impact:

Built-in security template settings will be reapplied by Group Policy even when the system is in use, which may have a slight impact on performance.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\Group Policy\{827D319E-6EAC-11D2-A4EA-00C04F79F83A}:NoBackgroundPolicy
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`, then set the `Do not apply during periodic background processing` option to `FALSE` (unchecked):

```
Computer Configuration\Policies\Administrative Templates\System\Group
Policy\Configure security policy processing
```

Note: This Group Policy path is provided by the Group Policy template `GroupPolicy.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Disabled. (Group policies are not reapplied until the next logon or restart.)

References:

1. https://learn.microsoft.com/en-us/previous-versions/ms813374(v=msdn.10)?redirectedfrom=MSDN
2. GRID: MS-00000314

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	5.4 Deploy System Configuration Management Tools Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.		●	●

18.9.19.3 Ensure 'Configure security policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

The "Process even if the Group Policy objects have not changed" option updates and reapplies security policies even if the security policies have not changed.

This setting affects all policy settings within the built-in security template of Group Policy (e.g. Windows Settings\Security Settings).

The recommended state for this setting is: `Enabled: TRUE` (checked).

Rationale:

Setting this option to true (checked) will ensure unauthorized local changes are reverted to match the domain-based Group Policy settings.

Impact:

Built-in security template settings will be reapplied even if they have not been changed, which may cause Group Policy refreshes to take longer.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\Group Policy\{827D319E-6EAC-11D2-A4EA-00C04F79F83A}:NoGPOListChanges
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`, then set the `Process even if the Group Policy objects have not changed` option to `TRUE` (checked):

```
Computer Configuration\Policies\Administrative Templates\System\Group Policy\Configure security policy processing
```

Note: This Group Policy path is provided by the Group Policy template `GroupPolicy.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Disabled. (Group policies are not reapplied if they have not been changed.)

References:

1. https://learn.microsoft.com/en-us/previous-versions/ms813374(v=msdn.10)?redirectedfrom=MSDN
2. GRID: MS-00000315

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	5.4 Deploy System Configuration Management Tools Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.		●	●

18.9.19.4 Ensure 'Continue experiences on this device' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether the Windows device is allowed to participate in cross-device experiences (continue experiences).

The recommended state for this setting is: `Disabled`.

Rationale:

A cross-device experience is when a system can access app and send messages to other devices. In an enterprise managed environment only trusted systems should be communicating within the network. Access to any other system should be prohibited.

Impact:

The Windows device will not be discoverable by other devices, and cannot participate in cross-device experiences.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\System:EnableCdp
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\System\Group
Policy\Continue experiences on this device
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `GroupPolicy.admx/adml` that is included with the Microsoft Windows 10 version 1607 & Server 2016 Administrative Templates (or newer).

Default Value:

The default behavior depends on the Windows edition.

References:

1. GRID: MS-00000316

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.9.19.5 Ensure 'Turn off background refresh of Group Policy' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting prevents Group Policy from being updated while the computer is in use. This policy setting applies to Group Policy for computers, users and Domain Controllers.

The recommended state for this setting is: `Disabled`.

Rationale:

This setting ensures that group policy changes take effect more quickly, as compared to waiting until the next user logon or system restart.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location and when set properly a value `does not exist`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:
DisableBkGndGroupPolicy
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled:`

```
Computer Configuration\Policies\Administrative Templates\System\Group
Policy\Turn off background refresh of Group Policy
```

Note: This Group Policy path is provided by the Group Policy template `GroupPolicy.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Updates can be applied while users are working.)

References:

1. GRID: MS-00000317

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	5.4 Deploy System Configuration Management Tools Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.		●	●

18.9.20 Internet Communication Management

This section contains recommendations related to Internet Communication Management.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.20.1 Internet Communication settings

This section contains recommendations related to Internet Communication settings.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.20.1.1 Ensure 'Turn off downloading of print drivers over HTTP' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls whether the computer can download print driver packages over HTTP. To set up HTTP printing, printer drivers that are not available in the standard operating system installation might need to be downloaded over HTTP.

The recommended state for this setting is: `Enabled`.

Rationale:

Users might download drivers that include malicious code.

Impact:

Print drivers cannot be downloaded over HTTP.

Note: This policy setting does not prevent the client computer from printing to printers on the intranet or the Internet over HTTP. It only prohibits downloading drivers that are not already installed locally.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Printers:DisableWebPnPDownload
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\System\Internet
Communication Management\Internet Communication settings\Turn off downloading
of print drivers over HTTP
```

Note: This Group Policy path is provided by the Group Policy template `ICM.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Users can download print drivers over HTTP.)

References:

1. GRID: MS-00000319

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.5 Allowlist Authorized Software Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.		●	●
v7	2.7 Utilize Application Whitelisting Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets.			●

18.9.20.1.2 Ensure 'Turn off handwriting personalization data sharing' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This setting turns off data sharing from the handwriting recognition personalization tool.

The handwriting recognition personalization tool enables Tablet PC users to adapt handwriting recognition to their own writing style by providing writing samples. The tool can optionally share user writing samples with Microsoft to improve handwriting recognition in future versions of Windows. The tool generates reports and transmits them to Microsoft over a secure connection.

The recommended state for this setting is: `Enabled`.

Rationale:

A person's handwriting is Personally Identifiable Information (PII), especially when it comes to your signature. As such, it is unacceptable in many environments to automatically upload PII to a website without explicit approval by the user.

Impact:

Tablet PC users cannot choose to share writing samples from the handwriting recognition personalization tool with Microsoft.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\TabletPC:PreventHandwritingDataSharing
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled:`

```
Computer Configuration\Policies\Administrative Templates\System\Internet
Communication Management\Internet Communication settings\Turn off handwriting
personalization data sharing
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `ShapeCollector.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Default Value:

Tablet PC users can choose whether or not they want to share their writing samples from the handwriting recognition personalization tool with Microsoft.

References:

1. GRID: MS-00000320

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.9.20.1.3 Ensure 'Turn off handwriting recognition error reporting' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

Turns off the handwriting recognition error reporting tool.

The handwriting recognition error reporting tool enables users to report errors encountered in Tablet PC Input Panel. The tool generates error reports and transmits them to Microsoft over a secure connection. Microsoft uses these error reports to improve handwriting recognition in future versions of Windows.

The recommended state for this setting is: `Enabled`.

Rationale:

A person's handwriting is Personally Identifiable Information (PII), especially when it comes to your signature. As such, it is unacceptable in many environments to automatically upload PII to a website without explicit approval by the user.

Impact:

Users cannot start the handwriting recognition error reporting tool or send error reports to Microsoft.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\HandwritingErrorReports:PreventHandw
ritingErrorReports
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\System\Internet
Communication Management\Internet Communication settings\Turn off handwriting
recognition error reporting
```

Note: This Group Policy path is provided by the Group Policy template `InkWatson.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Tablet PC users can report handwriting recognition errors to Microsoft.)

References:

1. GRID: MS-00000321

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.9.20.1.4 Ensure 'Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting specifies whether the Internet Connection Wizard can connect to Microsoft to download a list of Internet Service Providers (ISPs).

The recommended state for this setting is: `Enabled`.

Rationale:

In an enterprise managed environment we want to lower the risk of a user unknowingly exposing sensitive data.

Impact:

The "Choose a list of Internet Service Providers" path in the Internet Connection Wizard causes the wizard to exit. This prevents users from retrieving the list of ISPs, which resides on Microsoft servers.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\Internet Connection
Wizard:ExitOnMSICW
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\System\Internet
Communication Management\Internet Communication settings\Turn off Internet
Connection Wizard if URL connection is referring to Microsoft.com
```

Note: This Group Policy path is provided by the Group Policy template `ICM.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Users can connect to Microsoft to download a list of ISPs for their area.)

References:

1. GRID: MS-00000322

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.9.20.1.5 Ensure 'Turn off Internet download for Web publishing and online ordering wizards' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls whether Windows will download a list of providers for the Web publishing and online ordering wizards.

The recommended state for this setting is: `Enabled`.

Rationale:

Although the risk is minimal, enabling this setting will reduce the possibility of a user unknowingly downloading malicious content through this feature.

Impact:

Windows is prevented from downloading providers; only the service providers cached in the local registry are displayed.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer:NoWebServices
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off Internet download for Web publishing and online ordering wizards
```

Note: This Group Policy path is provided by the Group Policy template `ICM.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (A list of providers is downloaded when the user uses the web publishing or online ordering wizards.)

References:

1. GRID: MS-00000323

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.9.20.1.6 Ensure 'Turn off printing over HTTP' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting allows you to disable the client computer's ability to print over HTTP, which allows the computer to print to printers on the intranet as well as the Internet.

The recommended state for this setting is: `Enabled`.

Note: This control affects printing over **both** HTTP and HTTPS.

Rationale:

Information that is transmitted over HTTP through this capability is not protected and can be intercepted by threat actors. For this reason, it is not often used in enterprise managed environments.

Impact:

The client computer will not be able to print to Internet printers over HTTP or HTTPS.

Note: This policy setting affects the client side of Internet printing only. Regardless of how it is configured, a computer could act as an Internet Printing server and make its shared printers available through HTTP.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Printers:DisableHTTPPrinting
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\System\Internet
Communication Management\Internet Communication settings\Turn off printing
over HTTP
```

Note: This Group Policy path is provided by the Group Policy template `ICM.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Users can choose to print to Internet printers over HTTP.)

References:

1. GRID: MS-00000324

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	13.3 Monitor and Block Unauthorized Network Traffic Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.			●

18.9.20.1.7 Ensure 'Turn off Registration if URL connection is referring to Microsoft.com' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting specifies whether the Windows Registration Wizard connects to Microsoft.com for online registration.

The recommended state for this setting is: `Enabled`.

Rationale:

Users in an enterprise managed environment should not be registering their own copies of Windows, providing their own PII in the process.

Impact:

Users are blocked from connecting to Microsoft.com for online registration and they cannot register their copy of Windows online.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\Registration Wizard
Control:NoRegistration
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\System\Internet
Communication Management\Internet Communication settings\Turn off
Registration if URL connection is referring to Microsoft.com
```

Note: This Group Policy path is provided by the Group Policy template `ICM.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Users can connect to Microsoft.com to complete the online Windows Registration.)

References:

1. GRID: MS-00000325

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.9.20.1.8 Ensure 'Turn off Search Companion content file updates' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting specifies whether Search Companion should automatically download content updates during local and Internet searches.

The recommended state for this setting is: `Enabled`.

Rationale:

There is a small risk that users will unknowingly reveal sensitive information because of the topics they are searching for. This risk is very low because even if this setting is enabled users still must submit search queries to the desired search engine in order to perform searches.

Impact:

Search Companion does not download content updates during searches.

Note: Internet searches will still send the search text and information about the search to Microsoft and the chosen search provider. If you select Classic Search, the Search Companion feature will be unavailable. You can select Classic Search by clicking Start, Search, Change Preferences, and then Change Internet Search Behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\SearchCompanion:DisableContentFileUpdates
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\System\Internet
Communication Management\Internet Communication settings\Turn off Search
Companion content file updates
```

Note: This Group Policy path is provided by the Group Policy template `ICM.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Search Companion downloads content updates unless the user is using Classic Search.)

References:

1. GRID: MS-00000326

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.9.20.1.9 Ensure 'Turn off the "Order Prints" picture task' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting specifies whether the "Order Prints Online" task is available from Picture Tasks in Windows folders.

The Order Prints Online Wizard is used to download a list of providers and allow users to order prints online.

The recommended state for this setting is: `Enabled`.

Rationale:

In an enterprise managed environment we want to lower the risk of a user unknowingly exposing sensitive data.

Impact:

The task "Order Prints Online" is removed from Picture Tasks in File Explorer folders.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer:NoOnlinePrintsWizard
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off the "Order Prints" picture task
```

Note: This Group Policy path is provided by the Group Policy template `ICM.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (The "Order Prints Online" task is displayed in Picture Tasks in File Explorer folders.)

References:

1. GRID: MS-00000327

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.9.20.1.10 Ensure 'Turn off the "Publish to Web" task for files and folders' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting specifies whether the tasks Publish this file to the Web, Publish this folder to the Web, and Publish the selected items to the Web are available from File and Folder Tasks in Windows folders.

The recommended state for this setting is: `Enabled`.

Rationale:

Users may publish confidential or sensitive information to a public service outside of the control of the organization.

Impact:

The "Publish to Web" task is removed from File and Folder tasks in Windows folders.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer:NoPublishing
Wizard
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\System\Internet
Communication Management\Internet Communication settings\Turn off the
"Publish to Web" task for files and folders
```

Note: This Group Policy path is provided by the Group Policy template `ICM.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (The "Publish to Web" task is shown in File and Folder tasks in Windows folders.)

References:

1. GRID: MS-00000328

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.9.20.1.11 Ensure 'Turn off the Windows Messenger Customer Experience Improvement Program' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting specifies whether Windows Messenger can collect anonymous information about how the Windows Messenger software and service is used. Microsoft uses information collected through the Customer Experience Improvement Program to detect software flaws so that they can be corrected more quickly, enabling this setting will reduce the amount of data Microsoft is able to gather for this purpose.

The recommended state for this setting is: `Enabled`.

Rationale:

Large enterprise managed environments may not want to have information collected by Microsoft from managed client computers.

Impact:

Windows Messenger will not collect usage information, and the user settings to enable the collection of usage information will not be shown.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `2`.

```
HKLM\SOFTWARE\Policies\Microsoft\Messenger\Client:CEIP
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\System\Internet
Communication Management\Internet Communication settings\Turn off the Windows
Messenger Customer Experience Improvement Program
```

Note: This Group Policy path is provided by the Group Policy template `ICM.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Users have the choice to opt-in and allow information to be collected.

References:

1. GRID: MS-00000329

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.9.20.1.12 Ensure 'Turn off Windows Customer Experience Improvement Program' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting specifies whether the Windows Customer Experience Improvement Program can collect anonymous information about how Windows is used.

Microsoft uses information collected through the Windows Customer Experience Improvement Program to improve features that are most used and to detect flaws so that they can be corrected more quickly. Enabling this setting will reduce the amount of data Microsoft is able to gather for this purpose. The recommended state for this setting is: `Enabled`.

Rationale:

Large enterprise managed environments may not want to have information collected by Microsoft from managed client computers.

Impact:

All users are opted out of the Windows Customer Experience Improvement Program.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\SQMClient\Windows:CEIPEnable
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\System\Internet
Communication Management\Internet Communication settings\Turn off Windows
Customer Experience Improvement Program
```

Note: This Group Policy path is provided by the Group Policy template `ICM.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

The Administrator can use the Problem Reports and Solutions component in Control Panel to enable Windows Customer Experience Improvement Program for all users.

References:

1. GRID: MS-00000330

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.9.20.1.13 Ensure 'Turn off Windows Error Reporting' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting controls whether or not errors are reported to Microsoft.

Error Reporting is used to report information about a system or application that has failed or has stopped responding and is used to improve the quality of the product.

The recommended state for this setting is: `Enabled`.

Rationale:

If a Windows Error occurs in a secure, enterprise managed environment, the error should be reported directly to IT staff for troubleshooting and remediation. There is no benefit to the corporation to report these errors directly to Microsoft, and there is some risk of unknowingly exposing sensitive data as part of the error.

Impact:

Users are not given the option to report errors to Microsoft.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0` (DoReport) and `1` (Disabled).

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Windows Error
Reporting:Disabled
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\PCHealth\ErrorReporting:DoRepo
rt
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\System\Internet
Communication Management\Internet Communication settings\Turn off Windows
Error Reporting
```

Note: This Group Policy path is provided by the Group Policy template `ICM.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Errors may be reported to Microsoft via the Internet or to a corporate file share.)

References:

1. GRID: MS-00000331

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.9.21 iSCSI

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `iSCSI.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.22 KDC

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `KDC.admx/adml` that is included with the Microsoft Windows Server 2008 (non-R2) Administrative Templates (or newer).

18.9.23 Kerberos

This section contains recommendations for Kerberos settings.

This Group Policy section is provided by the Group Policy template `Kerberos.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.23.1 Ensure 'Support device authentication using certificate' is set to 'Enabled: Automatic' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting allows you to set support for Kerberos to attempt authentication using the certificate for the device to the domain.

Support for device authentication using certificate will require connectivity to a DC in the device account domain which supports certificate authentication for computer accounts.

The recommended state for this setting is: `Enabled: Automatic`.

Rationale:

Having stronger device authentication with the use of certificates is strongly encouraged over standard username and password authentication. Having this set to Automatic will allow certificate based authentication to be used whenever possible.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0` (DevicePKInitBehavior) and `1` (DevicePKInitEnabled).

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\
kerberos\parameters:DevicePKInitBehavior
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\
kerberos\parameters:DevicePKInitEnabled
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Automatic`:

```
Computer Configuration\Policies\Administrative
Templates\System\Kerberos\Support device authentication using certificate
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `Kerberos.admx/adml` that is included with the Microsoft Windows 10 RTM (version 1507) Administrative Templates (or newer).

Default Value:

Automatic. (Devices will attempt to authenticate using their certificate. If the DC does not support computer account authentication using certificates then authentication with password will be attempted.)

References:

1. GRID: MS-00000332

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

18.9.24 Kernel DMA Protection

This section contains recommendations for Kernel DMA Protection settings.

This Group Policy section is provided by the Group Policy template `DmaGuard.admx/adml` that is included with the Microsoft Windows 10 version 1809 and Server 2019 Administrative Templates (or newer).

18.9.24.1 Ensure 'Enumeration policy for external devices incompatible with Kernel DMA Protection' is set to 'Enabled: Block All' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy is intended to provide additional security against external DMA-capable devices. It allows for more control over the enumeration of external DMA-capable devices that are not compatible with DMA Remapping/device memory isolation and sandboxing.

The recommended state for this setting is: `Enabled: Block All`.

Note: This policy does not apply to 1394, PCMCIA or ExpressCard devices. The protection also only applies to Windows 10 v1803 or higher, and also requires a UEFI BIOS to function.

Note #2: More information on this feature is available at this link: Kernel DMA Protection for Thunderbolt™ 3 (Windows 10) | Microsoft Docs.

Rationale:

Device memory sandboxing allows the OS to leverage the I/O Memory Management Unit (IOMMU) of a device to block unpermitted I/O, or memory access, by the peripheral.

Impact:

External devices that are not compatible with DMA-remapping will not be enumerated and will not function unless/until the user has logged in successfully *and* has an unlocked user session. Once enumerated, these devices will continue to function, regardless of the state of the session. Devices that **are** compatible with DMA-remapping will be enumerated immediately, with their device memory isolated.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\Kernel DMA
Protection:DeviceEnumerationPolicy
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Block All`:

```
Computer Configuration\Policies\Administrative Templates\System\Kernel DMA
Protection\Enumeration policy for external devices incompatible with Kernel
DMA Protection
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `DmaGuard.admx/adml` that is included with the Microsoft Windows 10 version 1809 & Server 2019 Administrative Templates (or newer).

Default Value:

Windows Server 2019 or newer, if UEFI BIOS is present: Enabled: Only while logged in (default)

Windows Server 2019 or newer, if using legacy BIOS: Disabled

Windows Server 2016 or older: Not supported (i.e. Disabled)

References:

1. GRID: MS-00000333

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	1.4 Maintain Detailed Asset Inventory Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all hardware assets, whether connected to the organization's network or not.	●	●	●

18.9.25 Keyboard Filter

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `KeyboardFilterPolicy.admx/adml` that is included with the Microsoft Windows 11 version 25H2 Administrative Templates (or newer).

18.9.26 LAPS

This section contains recommendations for Windows Local Administrator Password Solution (LAPS) settings.

This Group Policy section is provided by the Group Policy template `LAPS.admx/adml` that is included with the Microsoft Windows 11 version 22H2 Administrative Templates v3.0 (or newer).

18.9.26.1 Ensure 'Configure password backup directory' is set to 'Enabled: Active Directory' or 'Enabled: Azure Active Directory' (MS only) (Automated)

Profile Applicability:

- Level 1 - Member Server

Description:

This policy setting configures which directory Windows LAPS will use to back up the local admin account password.

The recommended state for this setting is: `Enabled: Active Directory` or `Enabled: Azure Active Directory`.

Note: Organizations that utilize third-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations.

Note #2: Windows LAPS does not support standalone computers - they must be joined to an Active Directory domain or Entra ID (formerly Azure Active Directory).

Note #3: Windows LAPS does not support simultaneous storage of the local admin password in both directory types.

Note #4: If the setting is configured and the managed device is not joined to the configured directory type, the local administrator password will not be managed by Windows LAPS.

Rationale:

Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or Member Servers when deploying them. This creates a serious attack surface security risk because if a threat actor manages to compromise one system and learn the password to its local Administrator account, then they can leverage that account to instantly gain access to all other computers that also use that password for their local Administrator account.

Impact:

The passwords managed by Windows LAPS will only be retrievable from the configured directory type.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1` or `2`.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\LAPS:BackupDirectory
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Active Directory` or `Enabled: Azure Active Directory`:

```
Computer Configuration\Policies\Administrative
Templates\System\LAPS\Configure password backup directory
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `LAPS.admx/adml` that is included with the Microsoft Windows 11 version 22H2 Administrative Templates v3.0 (or newer).

Default Value:

Disabled. (The local administrator password is not managed by Windows LAPS.)

References:

1. https://learn.microsoft.com/en-us/windows-server/identity/laps/laps-management-policy-settings
2. GRID: MS-00000334

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

18.9.26.2 Ensure 'Do not allow password expiration time longer than required by policy' is set to 'Enabled' (MS only) (Automated)

Profile Applicability:

- Level 1 - Member Server

Description:

This policy setting configures whether the password age dictated by the Windows LAPS "Password Settings" policy is enforced and cannot be extended manually (only shortened) by an authorized technician.

If an expiration is detected, the password is changed immediately, and password expiration is set according to policy.

The recommended state for this setting is: `Enabled`.

Note: Organizations that utilize third-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations.

Note #2: Windows LAPS does not support standalone computers - they must be joined to an Active Directory domain or Entra ID (formerly Azure Active Directory).

Rationale:

Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or Member Servers when deploying them. This creates a serious attack surface security risk because if a threat actor manages to compromise one system and learn the password to its local Administrator account, then they can leverage that account to instantly gain access to all other computers that also use that password for their local Administrator account.

Impact:

None - this is the default behavior.

Planned password expiration longer than password age dictated by "Password Settings" policy is NOT allowed.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\LAPS:PasswordExpirationProtectionEnabled
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\System\LAPS\Do not allow password expiration time longer than required by policy
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `LAPS.admx/adml` that is included with the Microsoft Windows 11 version 23H2 Administrative Templates v2.0 (or newer).

Note #2: This setting also existed in the Microsoft Windows 11 version 22H2 v3.0 and 23H2 v1.0 Administrative Templates, but it was misconfigured in those versions with the incorrect registry value. Please ensure you are using Windows 11 version 23H2 Administrative Templates v2.0 (or newer) when configuring this setting to ensure the correct registry value is set.

Default Value:

Enabled. (Planned password expiration longer than the password age policy is not allowed.)

References:

1. https://learn.microsoft.com/en-us/windows-server/identity/laps/laps-management-policy-settings
2. GRID: MS-00000335

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

18.9.26.3 Ensure 'Enable password encryption' is set to 'Enabled' (MS only) (Automated)

Profile Applicability:

- Level 1 - Member Server

Description:

This policy setting controls whether the Windows LAPS managed password is encrypted before being sent to Active Directory.

The recommended state for this setting is: `Enabled`.

Note: Organizations that utilize third-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations.

Note #2: Windows LAPS does not support standalone computers - they must be joined to an Active Directory domain or Entra ID (formerly Azure Active Directory).

Note #3: This setting has no effect unless the password has been configured to be backed up to Active Directory, and the Active Directory domain functional level is at Windows Server 2016 or above.

Note #4: This setting has no relevance (but is harmless) when storing Windows LAPS passwords to Entra ID (formerly Azure Active Directory) as it automatically encrypts all Windows LAPS passwords.

Rationale:

Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or Member Servers when deploying them. This creates a serious attack surface security risk because if a threat actor manages to compromise one system and learn the password to its local Administrator account, then they can leverage that account to instantly gain access to all other computers that also use that password for their local Administrator account.

Impact:

None - this is the default behavior.

If the domain functional level is set at or above Windows Server 2016, the Windows LAPS managed account password is encrypted automatically, if it is set at a lower domain functional level, the Windows LAPS managed account password will not be backed up to the directory.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\LAPS:ADPasswordEncryptionEnabled
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\System\LAPS\Enable password encryption
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `LAPS.admx/adml` that is included with the Microsoft Windows 11 version 22H2 Administrative Templates v3.0 (or newer).

Default Value:

Enabled. (Windows LAPS managed passwords are encrypted before being sent to Active Directory.)

References:

1. https://learn.microsoft.com/en-us/windows-server/identity/laps/laps-management-policy-settings
2. GRID: MS-00000336

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	14.4 Encrypt All Sensitive Information in Transit Encrypt all sensitive information in transit.		●	●

18.9.26.4 Ensure 'Password Settings: Password Complexity' is set to 'Enabled: Large letters + small letters + numbers + specials' (MS only) (Automated)

Profile Applicability:

- Level 1 - Member Server

Description:

This policy setting configures the Windows LAPS Password Settings policy for password complexity.

The recommended state for this setting is: `Enabled: Large letters + small letters + numbers + specials`

Note: Organizations that utilize third-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations.

Note #2: Windows LAPS does not support standalone computers - they must be joined to an Active Directory domain or Entra ID (formerly Azure Active Directory).

Rationale:

Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or Member Servers when deploying them. This creates a serious attack surface security risk because if a threat actor manages to compromise one system and learn the password to its local Administrator account, then they can leverage that account to instantly gain access to all other computers that also use that password for their local Administrator account.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `4`.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\LAPS:PasswordComplexity
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Large letters + small letters + numbers + specials`:

```
Computer Configuration\Policies\Administrative Templates\System\LAPS\Password Settings
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `LAPS.admx/adml` that is included with the Microsoft Windows 11 version 22H2 Administrative Templates v3.0 (or newer).

Default Value:

Large letters + small letters + numbers + specials.

References:

1. https://learn.microsoft.com/en-us/windows-server/identity/laps/laps-management-policy-settings
2. GRID: MS-00000337

Additional Information:

Each additional character in a password increases its complexity exponentially. For instance, a seven-character, all lower-case alphabetic password would have 26 to the power of 7 (approximately 8 x 10 to the power of 9 or 8 billion) possible combinations. At 1,000,000 attempts per second (a capability of many password-cracking utilities), it would only take 133 minutes to crack. A seven-character alphabetic password with case sensitivity has 52 to the power of 7 combinations. A seven-character case-sensitive alphanumeric password without punctuation has 627 combinations. An eight-character password has 26 to the power of 8 (or 2 x 10 to the power of 11) possible combinations. Although this might seem to be a large number, at 1,000,000 attempts per second it would take only 59 hours to try all possible passwords. Remember, these times will significantly increase for passwords that use ALT characters and other special keyboard characters such as "!" or "@". Proper use of the password settings can help make it difficult to mount a brute force attack.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

18.9.26.5 Ensure 'Password Settings: Password Length' is set to 'Enabled: 15 or more' (MS only) (Automated)

Profile Applicability:

- Level 1 - Member Server

Description:

This policy setting configures the Windows LAPS Password Settings policy for password length.

The recommended state for this setting is: `Enabled: 15 or more`.

Note: Organizations that utilize third-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations.

Note #2: Windows LAPS does not support standalone computers - they must be joined to an Active Directory domain or Entra ID (formerly Azure Active Directory).

Rationale:

Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or Member Servers when deploying them. This creates a serious attack surface security risk because if a threat actor manages to compromise one system and learn the password to its local Administrator account, then they can leverage that account to instantly gain access to all other computers that also use that password for their local Administrator account.

Impact:

Windows LAPS-generated passwords will be required to have a length of 15 characters (or more, if selected).

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `15`.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\LAPS:PasswordLength
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`, and configure the `Password Length` option to `15 or more`:

```
Computer Configuration\Policies\Administrative Templates\System\LAPS\Password Settings
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `LAPS.admx/adml` that is included with the Microsoft Windows 11 version 22H2 Administrative Templates v3.0 (or newer).

Default Value:

14 characters.

References:

1. https://learn.microsoft.com/en-us/windows-server/identity/laps/laps-management-policy-settings
2. GRID: MS-00000338

Additional Information:

Each additional character in a password increases its complexity exponentially. For instance, a seven-character, all lower-case alphabetic password would have 26 to the power of 7 (approximately 8 x 10 to the power of 9 or 8 billion) possible combinations. At 1,000,000 attempts per second (a capability of many password-cracking utilities), it would only take 133 minutes to crack. A seven-character alphabetic password with case sensitivity has 52 to the power of 7 combinations. A seven-character case-sensitive alphanumeric password without punctuation has 627 combinations. An eight-character password has 26 to the power of 8 (or 2 x 10 to the power of 11) possible combinations. Although this might seem to be a large number, at 1,000,000 attempts per second it would take only 59 hours to try all possible passwords. Remember, these times will significantly increase for passwords that use ALT characters and other special keyboard characters such as "!" or "@". Proper use of the password settings can help make it difficult to mount a brute force attack.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

18.9.26.6 Ensure 'Password Settings: Password Age (Days)' is set to 'Enabled: 30 or fewer' (MS only) (Automated)

Profile Applicability:

- Level 1 - Member Server

Description:

This policy setting configures the Windows LAPS Password Settings policy for password age.

The recommended state for this setting is: `Enabled: 30 or fewer`.

Note: Organizations that utilize third-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations.

Note #2: Windows LAPS does not support standalone computers - they must be joined to an Active Directory domain or Entra ID (formerly Azure Active Directory).

Rationale:

Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or Member Servers when deploying them. This creates a serious attack surface security risk because if a threat actor manages to compromise one system and learn the password to its local Administrator account, then they can leverage that account to instantly gain access to all other computers that also use that password for their local Administrator account.

Impact:

None - this is the default behavior, unless set to fewer than 30 days.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `30`.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\LAPS:PasswordAgeDays
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`, and configure the `Password Age (Days)` option to `30 or fewer`:

```
Computer Configuration\Policies\Administrative Templates\System\LAPS\Password Settings
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `LAPS.admx/adml` that is included with the Microsoft Windows 11 version 22H2 Administrative Templates v3.0 (or newer).

Default Value:

30 days.

References:

1. https://learn.microsoft.com/en-us/windows-server/identity/laps/laps-management-policy-settings
2. GRID: MS-00000339

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	16.10 Ensure All Accounts Have An Expiration Date Ensure that all accounts have an expiration date that is monitored and enforced.		●	●

18.9.26.7 Ensure 'Post-authentication actions: Grace period (hours)' is set to 'Enabled: 8 or fewer hours, but not 0' (MS only) (Automated)

Profile Applicability:

- Level 1 - Member Server

Description:

This policy settings configures post-authentication actions which will be executed after detecting an authentication by the Windows LAPS managed account. The `Grace period` refers to the amount of time (hours) to wait after an authentication before executing the specified post-authentication actions.

The recommended state for this setting is: `Enabled: 8 or fewer hours, but not 0`.

Note: Organizations that utilize third-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations.

Note #2: Windows LAPS does not support standalone computers - they must be joined to an Active Directory domain or Entra ID (formerly Azure Active Directory).

Note #3: If this policy is set to `0` it prevents all post-authentication actions from occurring.

Rationale:

Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or Member Servers when deploying them. This creates a serious attack surface security risk because if a threat actor manages to compromise one system and learn the password to its local Administrator account, then they can leverage that account to instantly gain access to all other computers that also use that password for their local Administrator account.

Impact:

After 8 hours, the Windows LAPS managed account password will be reset and log off the system.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `8` or less, but not `0`.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\LAPS:PostAuthenticationResetDelay
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: 8 or fewer hours, but not 0`:

```
Computer Configuration\Policies\Administrative Templates\System\LAPS\Post-authentication actions: Grace period (hours)
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `LAPS.admx/adml` that is included with the Microsoft Windows 11 version 22H2 Administrative Templates v3.0 (or newer).

Default Value:

Disabled. (Specified post-authentication actions will be executed after a default 24-hour grace period.)

References:

1. https://learn.microsoft.com/en-us/windows-server/identity/laps/laps-management-policy-settings
2. GRID: MS-00000340

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

18.9.26.8 Ensure 'Post-authentication actions: Actions' is set to 'Enabled: Reset the password and logoff the managed account' or higher (MS only) (Automated)

Profile Applicability:

- Level 1 - Member Server

Description:

This policy settings configures post-authentication actions which will be executed after detecting an authentication by the LAPS managed account. The `Action` refers to actions to take upon expiry of the grace period before executing the specified post-authentication actions.

Post-authentication actions:

- `Reset password`: upon expiry of the grace period, the managed account password will be reset.
- `Reset the password and logoff the managed account`: upon expiry of the grace period, the managed account password will be reset and any interactive logon sessions using the managed account will terminated.
- `Reset the password and reboot the device`: upon expiry of the grace period, the managed account password will be reset and the managed device will be immediately rebooted.
- `Reset the password, logoff the managed account, and terminate any remaining processes`: upon expiration of the grace period, the managed account password is reset, any interactive logon sessions using the managed account are logged off, and any remaining processes are terminated.

The recommended state for this setting is: `Enabled: Reset the password and logoff the managed account`. Configuring this setting to `Reset the password and reboot the device` or `Reset the password, logoff the managed account, and terminate any remaining processes` also conforms to the benchmark.

Warning: After an interactive logon session is terminated, other authenticated sessions using the Windows LAPS managed account may still be active. The only way to ensure that the previous password is no longer in use is to reboot the OS.

Note: Organizations that utilize third-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations.

Note #2: Windows LAPS does not support standalone computers - they must be joined to an Active Directory domain or Entra ID (formerly Azure Active Directory).

Rationale:

Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or Member Servers when deploying them. This creates a serious attack surface security risk because if a threat actor manages to compromise one system and learn the password to its local Administrator account, then they can leverage that account to instantly gain access to all other computers that also use that password for their local Administrator account.

Impact:

After the grace period expires, the Windows LAPS managed account password will be reset and logged off the system or the OS will be restarted.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `3`, `5` or `11`.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\LAPS:PostAuthenticationActions
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Reset the password and logoff the managed account`, `Reset the password and reboot the device` or `Reset the password, logoff the managed account, and terminate any remaining processes`:

```
Computer Configuration\Policies\Administrative Templates\System\LAPS\Post-authentication actions: Actions
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `LAPS.admx/adml` that is included with the Microsoft Windows 11 version 22H2 Administrative Templates v3.0 (or newer).

Default Value:

Disabled. (Reset the password and logoff the managed account after the specified grace period.)

References:

1. https://learn.microsoft.com/en-us/windows-server/identity/laps/laps-management-policy-settings
2. GRID: MS-00000341

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

18.9.27 Local Security Authority

This section contains recommendations for Local Security Authority settings.

This Group Policy section is provided by the Group Policy template `LocalSecurityAuthority.admx/adml` that is included with the Microsoft Windows 11 version 22H2 Administrative Templates v1.0 (or newer).

18.9.27.1 Ensure 'Allow Custom SSPs and APs to be loaded into LSASS' is set to 'Disabled' (DC only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This policy setting controls the configuration under which the Local Security Authority Subsystem Service (LSASS) will load custom Security Support Provider/Authentication Package (SSP/AP).

The recommended state for this setting is: `Disabled`.

Rationale:

Vulnerabilities exist where threat actors can intercept logon credentials via SSP/AP. Disabling Custom SSPs and APs to be loaded into LSASS minimizes this vulnerability.

Impact:

Custom Security Support Provider/Authentication Packages will not be permitted to load this may impact some legitimate third-party packages.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\System:AllowCustomSSPsAPs
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\System\Local
Security Authority\Allow Custom SSPs and APs to be loaded into LSASS
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `LocalSecurityAuthority.admx/adml` that is included with the Microsoft Windows 11 version 22H2 Administrative Templates v1.0 (or newer).

Default Value:

Enabled. (LSA allows custom SSPs and APs to be loaded).

References:

1. https://learn.microsoft.com/en-us/windows/win32/secauthn/ssp-aps-versus-ssps
2. GRID: MS-00000342

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●

18.9.27.2 Ensure 'Configures LSASS to run as a protected process' is set to 'Enabled: Enabled with UEFI Lock' (Automated)

Profile Applicability:

- Next Generation Windows Security - Domain Controller
- Next Generation Windows Security - Member Server

Description:

This policy setting controls whether the Local Security Authority Subservice Service (LSASS) runs in protected mode and also has the option to lock in protected mode with Unified Extensible Firmware Interface (UEFI). The Local Security Authority (LSA), which includes the LSASS process, validates users for local and remote sign-ins and enforces local security policies.

The recommended state for this setting is: `Enabled: Enabled with UEFI Lock`.

Note: This additional protection to prevent reading memory and code injection by non-protected processes is supported by Windows 8.1 (or newer).

Rationale:

Provides added security for the credentials that LSA stores and manages. Enabling this setting with `UEFI Lock` prevents the setting from being changed remotely.

Impact:

Once this setting has been applied (Enabled), removing the group policy setting (set to Not Configured) will not reverse the impact. In order to reverse the impact, you must explicitly configure this setting to Disabled and follow Microsoft's documentation on disabling the UEFI Lock.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\System:RunAsPPL
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Enabled with UEFI Lock`:

```
Computer Configuration\Policies\Administrative Templates\System\Local
Security Authority\Configures LSASS to run as a protected process
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `LocalSecurityAuthority.admx/adml` that is included with the Microsoft Windows 11 version 22H2 Administrative Templates v1.0 (or newer).

Note #2: In the Microsoft Windows 11 version 23H2 Administrative Templates, the registry location of *HKLM\SYSTEM\CurrentControlSet\Control\Lsa:RunAsPPL* was set for *Configures LSASS to run as a protected process*. This same registry location and value was also created if the setting *Ensure 'LSA Protection' is set to 'Enabled'* was also applied. This appears to have been a mistake in the ADMX/ADML Templates for that release.

Starting with the Microsoft Windows 11 version 24H2 Administrative Templates, the setting *Configures LSASS to run as a protected process* has a new registry location of *HKLM\Software\Policies\Microsoft\Windows\System*. In addition, the setting *LSA Protection* will be displayed by GPME when this setting (*Configures LSASS to run as a protected process*) is configured.

If *Configures LSASS to run as a protected process* was configured using an older version of the ADML/ADML templates, the new registry location will not auto-apply to the system, and assessment scans using the latest benchmark might fail. To fix this issue, the ADMX/ADML templates must be updated to the latest version, the setting removed from the GPO, and then added back in.

If the CIS Microsoft Windows Server 2012 R2, Server 2016, or Server 2019 Benchmark is applied, *LSA Protection* is configured via a separate recommendation for those older versions of the Windows Server Operating System using the `SecGuide.admx/adml` template. That configuration is verified separately from this recommendation.

Default Value:

Not configured. (LSA will run as protected process for clean installed, HVCI capable, client SKUs that are domain or cloud domain-joined devices. This configuration is not UEFI locked.)

References:

1. https://learn.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/configuring-additional-lsa-protection
2. https://learn.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard-manage#disabling-windows-defender-credential-guard-with-uefi-lock
3. GRID: MS-00000343

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●

18.9.28 Locale Services

This section contains recommendations for Locale Services settings.

This Group Policy section is provided by the Group Policy template `Globalization.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.28.1 Ensure 'Disallow copying of user input methods to the system account for sign-in' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy prevents automatic copying of user input methods to the system account for use on the sign-in screen. The user is restricted to the set of input methods that are enabled in the system account.

The recommended state for this setting is: `Enabled`.

Rationale:

This is a way to increase the security of the system account.

Impact:

Users will have input methods enabled for the system account on the sign-in page.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Control
Panel\International:BlockUserInputMethodsForSignIn
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\System\Locale
Services\Disallow copying of user input methods to the system account for
sign-in
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `Globalization.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Disabled. (Users will be able to use input methods enabled for their user account on the sign-in page.)

References:

1. GRID: MS-00000344

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

18.9.29 Logon

This section contains recommendations related to the logon process and lock screen.

This Group Policy section is provided by the Group Policy template `Logon.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.29.1 Ensure 'Block user from showing account details on sign-in' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy prevents the user from showing account details (email address or user name) on the sign-in screen.

The recommended state for this setting is: `Enabled`.

Rationale:

A threat actor with access to the console (for example, someone with physical access or someone who is able to connect to the server through Remote Desktop Services) could view the name of the last user who logged on to the server. The threat actor could then try to guess the password, use a dictionary, or use a brute-force attack to try and log on.

Impact:

The user cannot choose to show account details on the sign-in screen.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\System:BlockUserFromShowingAccountDetailsOnSignin
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\System\Logon\Block user from showing account details on sign-in
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `Logon.admx/adml` that is included with the Microsoft Windows 10 version 1607 & Server 2016 Administrative Templates (or newer).

Default Value:

Disabled. (The user may choose to show account details on the sign-in screen.)

References:

1. GRID: MS-00000345

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

18.9.29.2 Ensure 'Do not display network selection UI' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to control whether anyone can interact with available networks UI on the logon screen.

The recommended state for this setting is: `Enabled`.

Rationale:

An unauthorized user could disconnect the PC from the network or can connect the PC to other available networks without signing into Windows.

Impact:

The PC's network connectivity state cannot be changed without signing into Windows.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\System:DontDisplayNetworkSelectionUI
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\System\Logon\Do not
display network selection UI
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `Logon.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Default Value:

Disabled. (Any user can disconnect the PC from the network or can connect the PC to other available networks without signing into Windows.)

References:

1. GRID: MS-00000346

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

18.9.29.3 Ensure 'Do not enumerate connected users on domain-joined computers' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting prevents connected users from being enumerated on domain-joined computers.

The recommended state for this setting is: `Enabled`.

Rationale:

A threat actor could use this feature to gather account names of other users, that information could then be used in conjunction with other types of attacks such as guessing passwords or social engineering. The value of this countermeasure is small because a user with domain credentials could gather the same account information using other methods.

Impact:

The Logon UI will not enumerate any connected users on domain-joined computers.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\System:DontEnumerateConnectedUsers
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\System\Logon\Do not
enumerate connected users on domain-joined computers
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `Logon.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Disabled. (Connected users will be enumerated on domain-joined computers.)

References:

1. GRID: MS-00000347

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

18.9.29.4 Ensure 'Enumerate local users on domain-joined computers' is set to 'Disabled' (MS only) (Automated)

Profile Applicability:

- Level 1 - Member Server

Description:

This policy setting allows local users to be enumerated on domain-joined computers.

The recommended state for this setting is: `Disabled`.

Rationale:

A threat actor could use this feature to gather account names of other users, that information could then be used in conjunction with other types of attacks such as guessing passwords or social engineering. The value of this countermeasure is small because a user with domain credentials could gather the same account information using other methods.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\System:EnumerateLocalUsers
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative
Templates\System\Logon\Enumerate local users on domain-joined computers
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `Logon.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Disabled. (The Logon UI will not enumerate local users on domain-joined computers.)

References:

1. GRID: MS-00000348

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

18.9.29.5 Ensure 'Turn off app notifications on the lock screen' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to prevent app notifications from appearing on the lock screen.

The recommended state for this setting is: `Enabled`.

Rationale:

App notifications might display sensitive business or personal data.

Impact:

No app notifications are displayed on the lock screen.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\System:DisableLockScreenAppNotificat
ions
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\System\Logon\Turn
off app notifications on the lock screen
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `Logon.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Disabled. (Users can choose which apps display notifications on the lock screen.)

References:

1. GRID: MS-00000349

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●

18.9.29.6 Ensure 'Turn on convenience PIN sign-in' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to control whether a domain user can sign in using a convenience PIN. In Windows 10, convenience PIN was replaced with Passport, which has stronger security properties. To configure Passport for domain users, use the policies under Computer Configuration\Administrative Templates\Windows Components\Microsoft Passport for Work.

Note: The user's domain password will be cached in the system vault when using this feature.

The recommended state for this setting is: `Disabled`.

Rationale:

A PIN is created from a much smaller selection of characters than a password, so in most cases a PIN will be much less robust than a password.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\System:AllowDomainPINLogon
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\System\Logon\Turn on convenience PIN sign-in
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `CredentialProviders.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Turn on PIN sign-in*, but it was renamed starting with the Windows 10 version 1511 Administrative Templates.

Default Value:

Disabled. (A domain user can't set up and use a convenience PIN.)

References:

1. GRID: MS-00000351

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●

18.9.30 Mitigation Options

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `GroupPolicy.admx/adml` that is included with the Microsoft Windows 10 RTM (version 1507) Administrative Templates (or newer).

18.9.31 Net Logon

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Netlogon.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.32 NTLM

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Ntlm.admx/adml` that is included with the Microsoft Windows 11 version 25H2 Administrative Templates (or newer).

18.9.33 OS Policies

This section contains recommendations related to OS Policies.

This Group Policy section is provided by the Group Policy template `OSPolicy.admx/adml` that is included with the Microsoft Windows 10 version 1709 Administrative Templates (or newer).

18.9.33.1 Ensure 'Allow Clipboard synchronization across devices' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 - Member Server
- Level 2 - Domain Controller

Description:

This policy setting determines whether Clipboard contents can be synchronized across devices.

The recommended state for this setting is: `Disabled`.

Rationale:

Due to privacy concerns, clipboard data should stay local to the system and not synced across devices.

Impact:

If you disable this policy setting, Clipboard contents cannot be shared to other devices.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\System:AllowCrossDeviceClipboard
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\System\OS
Policies\Allow Clipboard synchronization across devices
```

Note: This Group Policy path is provided by the Group Policy template `OSPolicy.admx/adml` that is included with the Microsoft Windows 10 version 1809 & Server 2019 Administrative Templates (or newer).

Default Value:

Enabled. (Clipboard contents are allowed to be synchronized across devices logged in under the same Microsoft account or Azure AD account.)

References:

1. GRID: MS-00000352

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●

18.9.33.2 Ensure 'Allow upload of User Activities' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting determines whether published User Activities can be uploaded to the cloud.

The recommended state for this setting is: `Disabled`.

Rationale:

In high-security environments, data must never be shared with third-parties without explicit consent, as it may contain sensitive information.

Impact:

Activities of type User Activity are not allowed to be uploaded to the cloud. The Timeline feature will not function across devices.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\System:UploadUserActivities
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\System\OS
Policies\Allow upload of User Activities
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `OSPolicy.admx/adml` that is included with the Microsoft Windows 10 version 1803 Administrative Templates (or newer).

Default Value:

Enabled. (Activities of type User Activity are allowed to be uploaded to the cloud.)

References:

1. GRID: MS-00000353

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.9.34 PIN Complexity

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Passport.admx/adml` that is included with the Microsoft Windows 10 version 1703 Administrative Templates (or newer).

18.9.35 Power Management

This section contains recommendations for Power Management settings.

This Group Policy section is provided by the Group Policy template `Power.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.35.1 Button Settings

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Power.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.35.2 Energy Saver Settings

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Power.admx/adml` that is included with the Microsoft Windows 10 version 1607 & Server 2016 Administrative Templates (or newer).

18.9.35.3 Hard Disk Settings

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Power.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.35.4 Notification Settings

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Power.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.35.5 Power Throttling Settings

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Power.admx/adml` that is included with the Microsoft Windows 10 version 1709 Administrative Templates (or newer).

18.9.35.6 Sleep Settings

This section contains recommendations related to Power Management Sleep mode.

This Group Policy section is provided by the Group Policy template `Power.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.35.6.1 Ensure 'Allow network connectivity during connected-standby (on battery)' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting allows you to control the network connectivity state in standby on modern standby-capable systems.

The recommended state for this setting is: `Disabled`.

Rationale:

Disabling this setting ensures that the computer will not be accessible to threat actors over a WLAN network while left unattended, on battery and in a sleep state.

Impact:

Network connectivity in standby (while on battery) is not guaranteed. This connectivity restriction currently only applies to WLAN networks only, but is subject to change (according to Microsoft).

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Power\PowerSettings\f15576e8-98b7-4186-b944-eafa664402d9:DCSettingIndex
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\System\Power Management\Sleep Settings\Allow network connectivity during connected-standby (on battery)
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `Power.admx/adml` that is included with the Microsoft Windows 10 version 1607 & Server 2016 Administrative Templates (or newer).

Default Value:

Enabled. (Network connectivity will be maintained in standby while on battery.)

References:

1. GRID: MS-00000354

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.9.35.6.2 Ensure 'Allow network connectivity during connected-standby (plugged in)' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting allows you to control the network connectivity state in standby on modern standby-capable systems.

The recommended state for this setting is: `Disabled`.

Rationale:

Disabling this setting ensures that the computer will not be accessible to threat actors over a WLAN network while left unattended, plugged in and in a sleep state.

Impact:

Network connectivity in standby (while plugged in) is not guaranteed. This connectivity restriction currently only applies to WLAN networks only, but is subject to change (according to Microsoft).

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Power\PowerSettings\f15576e8-98b7-4186-b944-eafa664402d9:ACSettingIndex
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\System\Power Management\Sleep Settings\Allow network connectivity during connected-standby (plugged in)
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `Power.admx/adml` that is included with the Microsoft Windows 10 version 1607 & Server 2016 Administrative Templates (or newer).

Default Value:

Enabled. (Network connectivity will be maintained in standby while plugged in.)

References:

1. GRID: MS-00000355

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.9.35.6.3 Ensure 'Require a password when a computer wakes (on battery)' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Specifies whether or not the user is prompted for a password when the system resumes from sleep.

The recommended state for this setting is: `Enabled`.

Rationale:

Enabling this setting ensures that anyone who wakes an unattended computer from sleep state will have to provide logon credentials before they can access the system.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Power\PowerSettings\0e796bdb-100d-47d6-a2d5-f7d2daa51f51:DCSettingIndex
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\System\Power Management\Sleep Settings\Require a password when a computer wakes (on battery)
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `Power.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Enabled. (The user is prompted for a password when the system resumes from sleep while on battery.)

References:

1. GRID: MS-00000357

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

18.9.35.6.4 Ensure 'Require a password when a computer wakes (plugged in)' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Specifies whether or not the user is prompted for a password when the system resumes from sleep.

The recommended state for this setting is: `Enabled`.

Rationale:

Enabling this setting ensures that anyone who wakes an unattended computer from sleep state will have to provide logon credentials before they can access the system.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Power\PowerSettings\0e796bdb-100d-47d6-a2d5-f7d2daa51f51:ACSettingIndex
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\System\Power Management\Sleep Settings\Require a password when a computer wakes (plugged in)
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `Power.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Enabled. (The user is prompted for a password when the system resumes from sleep while plugged in.)

References:

1. GRID: MS-00000358

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

18.9.36 Recovery

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `ReAgent.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.9.37 Remote Assistance

This section contains recommendations related to Remote Assistance.

This Group Policy section is provided by the Group Policy template `RemoteAssistance.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.37.1 Ensure 'Configure Offer Remote Assistance' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to turn on or turn off Offer (Unsolicited) Remote Assistance on this computer.

Help desk and support personnel will not be able to proactively offer assistance, although they can still respond to user assistance requests.

The recommended state for this setting is: `Disabled`.

Rationale:

A user might be tricked and accept an unsolicited Remote Assistance offer from a threat actor.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal
Services:fAllowUnsolicited
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\System\Remote
Assistance\Configure Offer Remote Assistance
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `RemoteAssistance.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Disabled. (Users on this computer cannot get help from their corporate technical support staff using Offer (Unsolicited) Remote Assistance.)

References:

1. GRID: MS-00000359

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.9.37.2 Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to turn on or turn off Solicited (Ask for) Remote Assistance on this computer.

The recommended state for this setting is: `Disabled`.

Rationale:

There is slight risk that a rogue administrator will gain access to another user's desktop session, however, they cannot connect to a user's computer unannounced or control it without permission from the user. When an expert tries to connect, the user can still choose to deny the connection or give the expert view-only privileges. The user must explicitly click the Yes button to allow the expert to remotely control the workstation.

Impact:

Users on this computer cannot use e-mail or file transfer to ask someone for help. Also, users cannot use instant messaging programs to allow connections to this computer.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services:fAllowToGetHelp
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\System\Remote
Assistance\Configure Solicited Remote Assistance
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `RemoteAssistance.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Users can turn on or turn off Solicited (Ask for) Remote Assistance themselves in System Properties in Control Panel. Users can also configure Remote Assistance settings.

References:

1. GRID: MS-00000360

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.9.38 Remote Procedure Call

This section contains recommendations related to Remote Procedure Call.

This Group Policy section is provided by the Group Policy template `RPC.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.38.1 Ensure 'Enable RPC Endpoint Mapper Client Authentication' is set to 'Enabled' (MS only) (Automated)

Profile Applicability:

- Level 1 - Member Server

Description:

This policy setting controls whether RPC clients authenticate with the Endpoint Mapper Service when the call they are making contains authentication information. The Endpoint Mapper Service on computers running Windows NT4 (all service packs) cannot process authentication information supplied in this manner.

The recommended state for this setting is: `Enabled`.

Note: This policy will not be in effect until the system is rebooted.

Rationale:

Anonymous access to RPC services could result in accidental disclosure of information to unauthenticated users.

Impact:

RPC clients will authenticate to the Endpoint Mapper Service for calls that contain authentication information. Clients making such calls will not be able to communicate with the Windows NT4 Server Endpoint Mapper Service.

Note: This policy setting can cause a specific issue with *1-way* forest trusts if it is applied to the *trusting* domain DCs (see Microsoft KB3073942), so it is not recommend applying it to Domain Controllers.

Note #2: When this setting is combined with blocking or disabling the NTLM protocol, SID translation may not function.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Rpc:EnableAuthEpResolution
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\System\Remote
Procedure Call\Enable RPC Endpoint Mapper Client Authentication
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `RPC.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Disabled. (RPC clients will not authenticate to the Endpoint Mapper Service, but they will be able to communicate with the Windows NT4 Server Endpoint Mapper Service.)

References:

1. GRID: MS-00000361

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.9.38.2 Ensure 'Restrict Unauthenticated RPC clients' is set to 'Enabled: Authenticated' (MS only) (Automated)

Profile Applicability:

- Level 2 - Member Server

Description:

This policy setting controls how the RPC server runtime handles unauthenticated RPC clients connecting to RPC servers.

This policy setting impacts all RPC applications. In a domain environment this policy setting should be used with caution as it can impact a wide range of functionality including group policy processing itself. Reverting a change to this policy setting can require manual intervention on each affected machine. **This policy setting should never be applied to a Domain Controller.**

A client will be considered an authenticated client if it uses a named pipe to communicate with the server or if it uses RPC Security. RPC Interfaces that have specifically requested to be accessible by unauthenticated clients may be exempt from this restriction, depending on the selected value for this policy setting.

- "**None**" allows all RPC clients to connect to RPC Servers running on the machine on which the policy setting is applied.
- "**Authenticated**" allows only authenticated RPC Clients (per the definition above) to connect to RPC Servers running on the machine on which the policy setting is applied. Exemptions are granted to interfaces that have requested them.
- "**Authenticated without exceptions**" allows only authenticated RPC Clients (per the definition above) to connect to RPC Servers running on the machine on which the policy setting is applied. No exceptions are allowed. **This value has the potential to cause serious problems and is not recommended.**

Note: This policy setting will not be applied until the system is rebooted.

The recommended state for this setting is: `Enabled: Authenticated`.

Rationale:

Unauthenticated RPC communication can create a security vulnerability.

Impact:

Only authenticated RPC Clients will be allowed to connect to RPC servers running on the machine on which the policy setting is applied. Exemptions are granted to interfaces that have requested them.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Rpc:RestrictRemoteClients
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Authenticated`:

```
Computer Configuration\Policies\Administrative Templates\System\Remote
Procedure Call\Restrict Unauthenticated RPC clients
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `RPC.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Enabled: None. (All RPC clients are allowed to connect to RPC servers running on the machine.)

References:

1. GRID: MS-00000362

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.9.39 Removable Storage Access

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `RemovableStorage.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.40 Scripts

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Scripts.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.41 Security Account Manager

This section contains recommendations related to the Security Account Manager.

This Group Policy section is provided by the Group Policy template `SAM.admx/adml` that is included with the Microsoft Windows 11 version 21H2 Administrative Templates (or newer).

18.9.41.1 Ensure 'Configure validation of ROCA-vulnerable WHfB keys during authentication' is set to 'Enabled: Block' (DC only) (Automated)

Profile Applicability:

- Level 1 - Domain Controller

Description:

This policy setting allows you to configure how Domain Controllers handle Windows Hello for Business (WHfB) keys that are vulnerable to the "Return of Coppersmith´s attack" (ROCA) vulnerability.

If this policy setting is enabled the following options are supported:

- `Ignore`: During authentication the Domain Controller will not probe any WHfB keys for the ROCA vulnerability.
- `Audit`: During authentication the Domain Controller will emit audit events for WHfB keys that are subject to the ROCA vulnerability (authentications will still succeed).
- `Block`: During authentication the Domain Controller will block the use of WHfB keys that are subject to the ROCA vulnerability (vulnerable authentications will fail).

The recommended state for this setting is: `Enabled: Block`.

Note: This setting only takes effect on Domain Controllers running on Server 2022 (or newer).

Note #2: A reboot is not required for changes to this setting to take effect.

Rationale:

The "Return of Coppersmith´s attack" or ROCA vulnerability is a cryptographic weakness in a widely used cryptographic library. A threat actor can reveal secret keys (offline with no physical access to the affected device) on certified devices using this library.

For more information on this vulnerability, visit ADV170012 - Security Update Guide - Microsoft - Vulnerability in TPM could allow Security Feature Bypass.

Impact:

This setting may affect vulnerable Trusted Platform Module (TPMs). To avoid issues, this setting should not be set to `Block` until appropriate mitigations have been performed, for example patching of vulnerable TPMs.

Warning: It is recommended that this setting is first set to `Audit` to ensure there are no audit events for WHfB keys that are subject to the ROCA vulnerability. If these exist, remediate before configuring this to `Block`.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `2`.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\SAM:SamNGCKeyROCAValidation
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Block`:

```
Computer Configuration\Policies\Administrative Templates\System\Security Account Manager\Configure validation of ROCA-vulnerable WHfB keys during authentication
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `Sam.admx/adml` that is included with the Microsoft Windows 11 version 21H2 Administrative Templates (or newer).

Default Value:

Enabled: Audit. (Domain Controllers will default to using their local configuration. The default local configuration is Audit.)

References:

1. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-15361
2. https://nvd.nist.gov/vuln/detail/CVE-2017-15361
3. GRID: MS-00000363

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

18.9.42 Server Manager

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `ServerManager.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.43 Service Control Manager Settings

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `ServiceControlManager.admx/adml` that is included with the Microsoft Windows 10 version 1903 Administrative Templates (or newer).

18.9.44 Shutdown

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WinInit.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.9.45 Shutdown Options

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Winsrv.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.46 Storage Health

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `StorageHealth.admx/adml` that is included with the Microsoft Windows 10 version 1709 Administrative Templates (or newer).

18.9.47 Storage Sense

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `StorageSense.admx/adml` that is included with the Microsoft Windows 10 version 1903 Administrative Templates (or newer).

18.9.48 System Restore

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `SystemRestore.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.49 Troubleshooting and Diagnostics

This section contains recommendations related to Troubleshooting and Diagnostics.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.49.1 Application Compatibility Diagnostics

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `pca.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.49.2 Corrupted File Recovery

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `FileRecovery.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.49.3 Disk Diagnostic

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `DiskDiagnostic.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.49.4 Fault Tolerant Heap

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `fthsvc.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.9.49.5 Microsoft Support Diagnostic Tool

This section contains recommendations related to the Microsoft Support Diagnostic Tool.

This Group Policy section is provided by the Group Policy template `MSDT.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.49.5.1 Ensure 'Microsoft Support Diagnostic Tool: Turn on MSDT interactive communication with support provider' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting configures Microsoft Support Diagnostic Tool (MSDT) interactive communication with the support provider. MSDT gathers diagnostic data for analysis by support professionals.

The recommended state for this setting is: `Disabled`.

Rationale:

In high-security environments, data must never be shared with third-parties without explicit consent, as it may contain sensitive information.

Impact:

MSDT cannot run in support mode, and no data can be collected or sent to the support provider.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\ScriptedDiagnosticsProvider\Policy:D
isableQueryRemoteServer
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative
Templates\System\Troubleshooting and Diagnostics\Microsoft Support Diagnostic
Tool\Microsoft Support Diagnostic Tool: Turn on MSDT interactive
communication with support provider
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSDT.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Enabled. (Users can use MSDT to collect and send diagnostic data to a support professional to resolve a problem. By default, the support provider is set to Microsoft Corporation.)

References:

1. GRID: MS-00000364

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.9.49.6 MSI Corrupted File Recovery

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Msi-FileRecovery.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.9.49.7 Scheduled Maintenance

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `sdiagschd.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.9.49.8 Scripted Diagnostics

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `sdiageng.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.9.49.9 Windows Boot Performance Diagnostics

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `PerformanceDiagnostics.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.49.10 Windows Memory Leak Diagnosis

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `LeakDiagnostic.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.49.11 Windows Performance PerfTrack

This section contains recommendations related to Windows Performance PerfTrack.

This Group Policy section is provided by the Group Policy template `PerformancePerftrack.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.9.49.11.1 Ensure 'Enable/Disable PerfTrack' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting specifies whether to enable or disable tracking of responsiveness events.

The recommended state for this setting is: `Disabled`.

Rationale:

When enabled the aggregated data of a given event will be transmitted to Microsoft. The option exists to restrict this feature for a specific user, set the consent level, and designate specific programs for which error reports could be sent. However, centrally restricting the ability to execute PerfTrack to limit the potential for unauthorized or undesired usage, data leakage, or unintentional communications is highly recommended.

Impact:

Responsiveness events are not processed.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\WDI\{9c5a40da-b965-4fc3-8781-
88dd50a6299d}:ScenarioExecutionEnabled
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled:`

```
Computer Configuration\Policies\Administrative
Templates\System\Troubleshooting and Diagnostics\Windows Performance
PerfTrack\Enable/Disable PerfTrack
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `PerformancePerftrack.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Default Value:

Enabled. (Responsiveness events are processed and aggregated. The aggregated data will be transmitted to Microsoft through SQM.)

References:

1. GRID: MS-00000365

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.9.50 Trusted Platform Module Services

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `TPM.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.51 User Profiles

This section contains recommendations related to User Profiles.

This Group Policy section is provided by the Group Policy template `UserProfiles.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.51.1 Ensure 'Turn off the advertising ID' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting turns off the advertising ID, preventing apps from using the ID for experiences across apps.

The recommended state for this setting is: `Enabled`.

Rationale:

In high-security environments, data must never be shared with third-parties without explicit consent, as it may contain sensitive information. In addition, tracking user activity for advertising purposes, even anonymously, could be a privacy concern.

Impact:

The advertising ID is turned off. Apps can't use the ID for experiences across apps.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\AdvertisingInfo:DisabledByGroupPolic
y
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\System\User
Profiles\Turn off the advertising ID
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `UserProfiles.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Default Value:

Disabled. (Users can control whether apps can use the advertising ID for experiences across apps.)

References:

1. GRID: MS-00000366

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.9.52 Windows File Protection

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsFileProtection.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.53 Windows Time Service

This section contains recommendations related to the Windows Time Service.

This Group Policy section is provided by the Group Policy template `W32Time.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.53.1 Time Providers

This section contains recommendations related to Time Providers.

This Group Policy section is provided by the Group Policy template `W32Time.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.53.1.1 Ensure 'Enable Windows NTP Client' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting specifies whether the Windows NTP Client is enabled. Enabling the Windows NTP Client allows synchronization from a systems computer clock to NTP server(s).

The recommended state for this setting is: `Enabled`.

Note: If a third-party time provider is used in the environment, an exception to this recommendation will be needed.

Rationale:

A reliable and accurate account of time is important for a number of services and security requirements, including but not limited to distributed applications, authentication services, multi-user databases and logging services. The use of an NTP client (with secure operation) establishes functional accuracy and is a focal point when reviewing security relevant events

Impact:

System time will be synced to the configured NTP server(s).

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\W32Time\TimeProviders\NtpClient:Enabled
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled:`

```
Computer Configuration\Policies\Administrative Templates\System\Windows Time
Service\Time Providers\Enable Windows NTP Client
```

Note: This Group Policy path is provided by the Group Policy template `W32Time.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (The local computer clock does not synchronize time with NTP servers.)

References:

1. GRID: MS-00000367

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.4 Standardize Time Synchronization Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.		●	●
v7	6.1 Utilize Three Synchronized Time Sources Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.		●	●

18.9.53.1.2 Ensure 'Enable Windows NTP Server' is set to 'Disabled' (MS only) (Automated)

Profile Applicability:

- Level 1 - Member Server

Description:

This policy setting specifies whether the Windows NTP Server is enabled. Disabling this setting prevents the system from acting as a NTP Server (time source) to service NTP requests from other systems (NTP Clients).

The recommended state for this setting is: `Disabled`.

Note: In most enterprise managed environments, you should *not* disable the Windows NTP Server on Domain Controllers, as it is very important for the operation of NT5DS (domain hierarchy-based) time synchronization.

Rationale:

The configuration of proper time synchronization is critically important in an enterprise managed environment both due to the sensitivity of Kerberos authentication timestamps and also to ensure accurate security logging. This should be done through a known NTP server. Member servers and workstations should not typically be time sources for other clients.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\W32Time\TimeProviders\NtpServer:Enabled
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\System\Windows Time Service\Time Providers\Enable Windows NTP Server
```

Note: This Group Policy path is provided by the Group Policy template `W32Time.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (The computer cannot service NTP requests from other computers.)

References:

1. GRID: MS-00000368

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.4 Standardize Time Synchronization Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.		●	●
v7	6.1 Utilize Three Synchronized Time Sources Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.		●	●

18.10 Windows Components

This section contains recommendations for Windows Component settings.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.1 ActiveX Installer Service

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `ActiveXInstallService.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.2 Add features to Windows 10 (formerly Windows Anytime Upgrade)

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsAnytimeUpgrade.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Note: This section was initially named *Windows Anytime Upgrade* but was renamed by Microsoft to *Add features to Windows x* starting with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

18.10.3 App and Device Inventory

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `AppDeviceInventory.admx/adml` that is included with the Microsoft Windows 11 version 24H2 Administrative Templates (or newer).

18.10.4 App Package Deployment

This section contains recommendations for App Package Deployment settings.

This Group Policy section is provided by the Group Policy template `AppxPackageManager.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.10.4.1 Ensure 'Allow a Windows app to share application data between users' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

Manages a Windows app's ability to share data between users who have installed the app. Data is shared through the `SharedLocal` folder. This folder is available through the `Windows.Storage` API.

The recommended state for this setting is: `Disabled`.

Rationale:

Users of a system could accidentally share sensitive data with other users on the same system.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\AppModel\StateManager
:AllowSharedLocalAppData
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\App Package Deployment\Allow a Windows app to share application
data between users
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `AppxPackageManager.admx/adml` that is included with the Microsoft Windows 10 RTM (version 1507) Administrative Templates (or newer).

Default Value:

Disabled. (Windows apps won't be able to share app data with other instances of that app.)

References:

1. GRID: MS-00000369

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

18.10.5 App Privacy

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `AppPrivacy.admx/adml` that is included with the Microsoft Windows 10 version 1511 Administrative Templates (or newer).

18.10.6 App runtime

This section contains recommendations for App runtime settings.

This Group Policy section is provided by the Group Policy template `AppXRuntime.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.10.6.1 Ensure 'Allow Microsoft accounts to be optional' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting lets you control whether Microsoft accounts are optional for Windows Store apps that require an account to sign in. This policy only affects Windows Store apps that support it.

The recommended state for this setting is: `Enabled`.

Rationale:

Enabling this setting allows an organization to use their enterprise user accounts instead of using their Microsoft accounts when accessing Windows store apps. This provides the organization with greater control over relevant credentials. Microsoft accounts cannot be centrally managed and as such enterprise credential security policies cannot be applied to them, which could put any information accessed by using Microsoft accounts at risk.

Impact:

Windows Store apps that typically require a Microsoft account to sign in will allow users to sign in with an enterprise account instead.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:MSAOptional
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\App runtime\Allow Microsoft accounts to be optional
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `AppXRuntime.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Default Value:

Disabled. (Users will need to sign in with a Microsoft account.)

References:

1. GRID: MS-00000372

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.6 Centralize Account Management Centralize account management through a directory or identity service.		●	●
v7	16.2 Configure Centralized Point of Authentication Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.		●	●

18.10.7 Application Compatibility

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `AppCompat.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.8 AutoPlay Policies

This section contains recommendations for AutoPlay policies.

This Group Policy section is provided by the Group Policy template `AutoPlay.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.8.1 Ensure 'Disallow Autoplay for non-volume devices' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting disallows AutoPlay for MTP devices like cameras or phones.

The recommended state for this setting is: `Enabled`.

Rationale:

A threat actor could use this feature to launch a program to damage a client computer or data on the computer.

Impact:

AutoPlay will not be allowed for MTP devices like cameras or phones.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\Explorer:NoAutoplayfornonVolume
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\AutoPlay Policies\Disallow Autoplay for non-volume devices
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `AutoPlay.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Disabled. (AutoPlay is enabled for non-volume devices.)

References:

1. GRID: MS-00000374

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.3 Disable Autorun and Autoplay for Removable Media Disable autorun and autoplay auto-execute functionality for removable media.	●	●	●
v7	8.5 Configure Devices Not To Auto-run Content Configure devices to not auto-run content from removable media.	●	●	●

18.10.8.2 Ensure 'Set the default behavior for AutoRun' is set to 'Enabled: Do not execute any autorun commands' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting sets the default behavior for Autorun commands. Autorun commands are generally stored in `autorun.inf` files. They often launch the installation program or other routines.

The recommended state for this setting is: `Enabled: Do not execute any autorun commands`.

Rationale:

Prior to Windows Vista, when media containing an autorun command is inserted, the system will automatically execute the program without user intervention. This creates a major security concern as code may be executed without user's knowledge. The default behavior starting with Windows Vista is to prompt the user whether autorun command is to be run. The autorun command is represented as a handler in the Autoplay dialog.

Impact:

AutoRun commands will be completely disabled.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer:NoAutorun
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Do not execute any autorun commands`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\AutoPlay Policies\Set the default behavior for AutoRun
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `AutoPlay.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Disabled. (Windows will prompt the user whether autorun command is to be run.)

References:

1. GRID: MS-00000375

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.3 Disable Autorun and Autoplay for Removable Media Disable autorun and autoplay auto-execute functionality for removable media.	●	●	●
v7	8.5 Configure Devices Not To Auto-run Content Configure devices to not auto-run content from removable media.	●	●	●

18.10.8.3 Ensure 'Turn off Autoplay' is set to 'Enabled: All drives' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls Autoplay. Autoplay starts to read from a drive as soon as the media is inserted in the drive, which causes the setup file for programs or audio media to start immediately.

The recommended state for this setting is: `Enabled: All drives`.

Note: This policy setting cannot be used to enable Autoplay on computer drives in which it is disabled by default, such as floppy disk and network drives.

Rationale:

A threat actor could use this feature to launch a program to damage a client computer or data on the computer.

Impact:

Autoplay will be disabled - users will have to manually launch setup or installation programs that are provided on removable media.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `255`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explore
r:NoDriveTypeAutoRun
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: All drives`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\AutoPlay Policies\Turn off Autoplay
```

Note: This Group Policy path is provided by the Group Policy template `AutoPlay.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Autoplay is enabled.) Autoplay is disabled by default on some removable drive types, such as floppy disk and network drives, but not on CD-ROM drives.

References:

1. GRID: MS-00000376

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.3 Disable Autorun and Autoplay for Removable Media Disable autorun and autoplay auto-execute functionality for removable media.	●	●	●
v7	8.5 Configure Devices Not To Auto-run Content Configure devices to not auto-run content from removable media.	●	●	●

18.10.9 Biometrics

This section contains recommendations related to Biometrics.

This Group Policy section is provided by the Group Policy template `Biometrics.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.10.9.1 Facial Features

This section contains recommendations related to Facial Feature Biometrics.

This Group Policy section is provided by the Group Policy template `Biometrics.admx/adml` that is included with the Microsoft Windows 10 version 1511 Administrative Templates (or newer).

18.10.9.1.1 Ensure 'Configure enhanced anti-spoofing' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether enhanced anti-spoofing is configured for devices which support it.

The recommended state for this setting is: `Enabled`.

Rationale:

Enterprise managed environments are now supporting a wider range of mobile devices, increasing the security on these devices will help protect against unauthorized access on your network.

Impact:

Windows will require all users on the device to use anti-spoofing for facial features, on devices which support it.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Biometrics\FacialFeatures:EnhancedAntiSpoofi
ng
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Biometrics\Facial Features\Configure enhanced anti-spoofing
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `Biometrics.admx/adml` that is included with the Microsoft Windows 10 version 1511 Administrative Templates (or newer).

Note #2: In the Windows 10 version 1511 and Windows 10 version 1607 & Server 2016 Administrative Templates, this setting was initially named *Use enhanced anti-spoofing when available*. It was renamed to *Configure enhanced anti-spoofing* starting with the Windows 10 version 1703 Administrative Templates.

Default Value:

Disabled. (Windows doesn't require enhanced anti-spoofing for Windows Hello face authentication.)

References:

1. GRID: MS-00000377

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

18.10.10 BitLocker Drive Encryption

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `VolumeEncryption.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.11 Camera

This section contains recommendations related to Camera.

This Group Policy section is provided by the Group Policy template `Camera.admx/adml` that is included with the Microsoft Windows 10 version 1607 & Server 2016 Administrative Templates (or newer).

18.10.11.1 Ensure 'Allow Use of Camera' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting controls whether the use of Camera devices on the machine are permitted.

The recommended state for this setting is: `Disabled`.

Rationale:

Cameras in a high security environment can pose serious privacy and data exfiltration risks - they should be disabled to help mitigate that risk.

Impact:

Users will not be able to utilize the camera on a system.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Camera:AllowCamera
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Camera\Allow Use of Camera
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `Camera.admx/adml` that is included with the Microsoft Windows 10 version 1607 & Server 2016 Administrative Templates (or newer).

Default Value:

Enabled. (Camera devices are enabled.)

References:

1. GRID: MS-00000424

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●

18.10.12 Chat

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Taskbar.admx/adml` that is included with the Microsoft Windows 11 version 21H2 Administrative Templates (or newer).

18.10.13 Cloud Content

This section contains recommendations related to Cloud Content.

This Group Policy section is provided by the Group Policy template `CloudContent.admx/adml` that is included with the Microsoft Windows 10 version 1511 Administrative Templates (or newer).

18.10.13.1 Ensure 'Turn off cloud consumer account state content' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether cloud consumer account state content is allowed in all Windows experiences.

The recommended state for this setting is: `Enabled`.

Rationale:

The use of consumer accounts in an enterprise managed environment is not good security practice as it could lead to possible data leakage.

Impact:

Users will not be able to use Microsoft consumer accounts on the system, and associated Windows experiences will instead present default fallback content.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\CloudContent:DisableConsumerAccountS
tateContent
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Cloud Content\Turn off cloud consumer account state content
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `CloudContent.admx/adml` that is included with the Microsoft Windows 11 version 21H2 Administrative Templates (or newer).

Default Value:

Disabled. (Windows experiences are able to use cloud consumer accounts.)

References:

1. GRID: MS-00000425

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.6 Centralize Account Management Centralize account management through a directory or identity service.		●	●

18.10.13.2 Ensure 'Turn off cloud optimized content' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting turns off cloud optimized content in all Windows experiences.

The recommended state for this setting is: `Enabled`.

Rationale:

In high-security environments, data must never be shared with third-parties without explicit consent, as it may contain sensitive information.

Impact:

Windows experiences that use the cloud optimized content client component, will present the default fallback content instead of customized content.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\CloudContent:DisableCloudOptimizedCo
ntent
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Cloud Content\Turn off cloud optimized content
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `CloudContent.admx/adml` that is included with the Microsoft Windows 10 version 20H2 Administrative Templates (or newer).

Default Value:

Disabled. (Windows experiences will be able to use cloud optimized content.)

References:

1. GRID: MS-00000426

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.10.14 Connect

This section contains recommendations related to Connect.

This Group Policy section is provided by the Group Policy template `WirelessDisplay.admx/adml` that is included with the Microsoft Windows 10 version 1607 & Server 2016 Administrative Templates (or newer).

18.10.14.1 Ensure 'Require pin for pairing' is set to 'Enabled: First Time' OR 'Enabled: Always' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls whether or not a PIN is required for pairing to a wireless display device.

The recommended state for this setting is: `Enabled: First Time` OR `Enabled: Always`.

Rationale:

If this setting is not configured or disabled then a PIN would not be required when pairing wireless display devices to the system, increasing the risk of unauthorized use.

Impact:

The pairing ceremony for connecting to new wireless display devices will always require a PIN.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`or `2`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\Connect:RequirePinForPairing
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: First Time` OR `Enabled: Always`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Connect\Require pin for pairing
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WirelessDisplay.admx/adml` that is included with the Microsoft Windows 10 version 1607 & Server 2016 Administrative Templates (or newer). The new `Choose one of the following actions` sub-option was later added as of the Windows 10 version 1809 Administrative Templates. Choosing `Enabled` in the older templates is the equivalent of choosing `Enabled: First Time` in the newer templates.

Default Value:

Disabled. (A PIN is not required for pairing to a wireless display device.)

References:

1. GRID: MS-00000428

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

18.10.15 Credential User Interface

This section contains recommendations related to the Credential User Interface.

This Group Policy section is provided by the Group Policy template `CredUI.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.15.1 Ensure 'Do not display the password reveal button' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to configure the display of the password reveal button in password entry user experiences.

The recommended state for this setting is: `Enabled`.

Rationale:

This is a useful feature when entering a long and complex password, especially when using a touchscreen. The potential risk is that someone else may see your password while surreptitiously observing your screen.

Impact:

The password reveal button will not be displayed after a user types a password in the password entry text box.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\CredUI:DisablePasswordReveal
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Credential User Interface\Do not display the password reveal
button
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `CredUI.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Disabled. (The password reveal button is displayed after a user types a password in the password entry text box. If the user clicks on the button, the typed password is displayed on-screen in plain text.)

References:

1. GRID: MS-00000429

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

18.10.15.2 Ensure 'Enumerate administrator accounts on elevation' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls whether administrator accounts are displayed when a user attempts to elevate a running application.

The recommended state for this setting is: `Disabled`.

Rationale:

Users could see the list of administrator accounts, making it slightly easier for a threat actor who has logged onto a console session to try to crack the passwords of those accounts.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\CredUI:EnumerateAdmin
istrators
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Credential User Interface\Enumerate administrator accounts on
elevation
```

Note: This Group Policy path is provided by the Group Policy template `CredUI.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Users will be required to always type in a username and password to elevate.)

References:

1. GRID: MS-00000430

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

18.10.16 Data Collection and Preview Builds

This section contains settings for Data Collection and Preview Builds.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with the Microsoft Windows 10 RTM (version 1507) Administrative Templates (or newer).

18.10.16.1 Ensure 'Allow Diagnostic Data' is set to 'Enabled: Diagnostic data off (not recommended)' or 'Enabled: Send required diagnostic data' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines the amount of diagnostic and usage data reported to Microsoft:

- A value of (0) `Diagnostic data off (not recommended)`. Using this value, no diagnostic data is sent from the device. This value is only supported on Enterprise, Education, and Server editions. If you choose this setting, devices in your organization will still be secure.
- A value of (1) `Send required diagnostic data`. This is the minimum diagnostic data necessary to keep Windows secure, up to date, and performing as expected. Using this value disables the *Optional diagnostic data* control in the Settings app.
- A value of (3) `Send optional diagnostic data`. Additional diagnostic data is collected that helps us to detect, diagnose and fix issues, as well as make product improvements. Required diagnostic data will always be included when you choose to send optional diagnostic data. Optional diagnostic data can also include diagnostic log files and crash dumps. Use the *Limit Dump Collection* and the *Limit Diagnostic Log Collection* policies for more granular control of what optional diagnostic data is sent.

Windows telemetry settings apply to the Windows operating system and some first party apps. This setting does not apply to third party apps running on Windows 10/11.

The recommended state for this setting is: `Enabled: Diagnostic data off (not recommended)` or `Enabled: Send required diagnostic data`.

Note: If your organization relies on Windows Update, the minimum recommended setting is `Required diagnostic data`. Because no Windows Update information is collected when diagnostic data is off, important information about update failures is not sent. Microsoft uses this information to fix the causes of those failures and improve the quality of updates.

Note #2: The *Configure diagnostic data opt-in settings user interface* group policy can be used to prevent end users from changing their data collection settings.

Note #3: Enhanced diagnostic data setting is not available on Windows 11 and Windows Server 2022 and has been replaced with policies that can control the amount of optional diagnostic data that is sent. For more information on these settings visit Manage diagnostic data using Group Policy and MDM

Rationale:

Certain aspects of Microsoft Anti-Virus must have the setting *Allow Diagnostic Data* on and sending data to function properly.

Impact:

Note that setting values of 0 or 1 will degrade certain experiences on the device.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0` or `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\DataCollection:AllowTelemetry
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Diagnostic data off (not recommended)` or `Enabled: Send required diagnostic data`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Data Collection and Preview Builds\Allow Diagnostic Data
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `DataCollection.admx/adml` that is included with the Microsoft Windows 10 RTM (version 1507) Administrative Templates (or newer).

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Allow Telemetry*. It was renamed to *Allow Diagnostic Data* starting with the Windows 11 version 21H2 Administrative Templates.

Default Value:

Disabled. (The device will send required diagnostic data and the end user can choose whether to send optional diagnostic data from the Settings app.)

References:

1. https://docs.microsoft.com/en-us/windows/privacy/configure-windows-diagnostic-data-in-your-organization
2. GRID: MS-00000432

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.10.16.2 Ensure 'Configure Authenticated Proxy usage for the Connected User Experience and Telemetry service' is set to 'Enabled: Disable Authenticated Proxy usage' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting controls whether the Connected User Experience and Telemetry service can automatically use an authenticated proxy to send data back to Microsoft.

The recommended state for this setting is: `Enabled: Disable Authenticated Proxy usage`.

Rationale:

In high-security environments, data must never be shared with third-parties without explicit consent, as it may contain sensitive information.

Impact:

The Connected User Experience and Telemetry service will be blocked from automatically using an authenticated proxy.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\DataCollection:DisableEnterpriseAuth
Proxy
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Disable Authenticated Proxy usage`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Data Collection and Preview Builds\Configure Authenticated Proxy
usage for the Connected User Experience and Telemetry service
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `DataCollection.admx/adml` that is included with the Microsoft Windows 10 version 1703 Administrative Templates (or newer).

Default Value:

Disabled. (The Connected User Experience and Telemetry service will automatically use an authenticated proxy to send data back to Microsoft.)

References:

1. GRID: MS-00000433

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.10.16.3 Ensure 'Do not show feedback notifications' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows an organization to prevent its devices from showing feedback questions from Microsoft.

The recommended state for this setting is: `Enabled`.

Rationale:

Data must never be shared with third-parties without explicit consent, as it may contain sensitive information.

Impact:

Users will no longer see feedback notifications through the Windows Feedback app.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\DataCollection:DoNotShowFeedbackNoti
fications
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Data Collection and Preview Builds\Do not show feedback
notifications
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `FeedbackNotifications.admx/adml` that is included with the Microsoft Windows 10 version 1511 Administrative Templates (or newer).

Default Value:

Disabled. (Users may see notifications through the Windows Feedback app asking users for feedback. Users can control how often they receive feedback questions.)

References:

1. GRID: MS-00000435

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.10.16.4 Ensure 'Enable OneSettings Auditing' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting controls whether Windows records attempts to connect with the OneSettings service to the Event Log.

The recommended state for this setting is: `Enabled`.

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of threat actors.

Impact:

Windows will record attempts to connect with the OneSettings service to the `Applications and Services Logs\Microsoft\Windows\Privacy-Auditing\Operational` Event Log channel.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\DataCollection:EnableOneSettingsAuditing
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Data Collection and Preview Builds\Enable OneSettings Auditing
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `DataCollection.admx/adml` that is included with the Microsoft Windows 11 version 21H2 Administrative Templates (or newer).

Default Value:

Disabled. (Windows will not record attempts to connect with the OneSettings service to the Event Log.)

References:

1. GRID: MS-00000436

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	8.5 Configure Devices Not To Auto-run Content Configure devices to not auto-run content from removable media.	●	●	●

18.10.16.5 Ensure 'Limit Diagnostic Log Collection' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting controls whether additional diagnostic logs are collected when more information is needed to troubleshoot a problem on the device.

The recommended state for this setting is: `Enabled`.

Note: Diagnostic logs are only sent when the device has been configured to send optional diagnostic data. Diagnostic data is limited when recommendation `Allow Diagnostic Data` is set to `Enabled: Diagnostic data off (not recommended)` or `Enabled: Send required diagnostic data` to send only basic information.

Rationale:

In high-security environments, data must never be shared with third-parties without explicit consent, as it may contain sensitive information.

Impact:

Diagnostic logs and information such as crash dumps will not be collected for transmission to Microsoft.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\DataCollection:LimitDiagnosticLogCol
lection
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Data Collection and Preview Builds\Limit Diagnostic Log Collection
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `DataCollection.admx/adml` that is included with the Microsoft Windows 11 version 21H2 Administrative Templates (or newer).

Default Value:

Disabled. (Microsoft may occasionally collect diagnostic logs if the device has been configured to send optional diagnostic data.)

References:

1. GRID: MS-00000437

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●

18.10.16.6 Ensure 'Limit Dump Collection' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting limits the type of memory dumps that can be collected when more information is needed to troubleshoot a problem.

The recommended state for this setting is: `Enabled`.

Note: Memory dumps are only sent when the device has been configured to send optional diagnostic data. Diagnostic data is limited when recommendation `Allow Diagnostic Data` is set to `Enabled: Diagnostic data off (not recommended)` or `Enabled: Send required diagnostic data` to send only basic information.

Rationale:

Data must never be shared with third-parties without explicit consent, as it may contain sensitive information.

Impact:

Windows Error Reporting will not send full and/or heap memory dumps to Microsoft - they will be limited to kernel mini and/or user mode triage memory dumps (if sending optional diagnostic data is permitted).

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\DataCollection:LimitDumpCollection
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`.

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Data Collection and Preview Builds\Limit Dump Collection
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `DataCollection.admx/adml` that is included with the Microsoft Windows 11 version 21H2 Administrative Templates (or newer).

Default Value:

Disabled. (Microsoft may occasionally collect full or heap memory dumps, if sending optional diagnostic data is permitted.)

References:

1. GRID: MS-00000438

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

18.10.17 Delivery Optimization

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `DeliveryOptimization.admx/adml` that is included with the Microsoft Windows 10 RTM (version 1507) Administrative Templates (or newer).

18.10.18 Desktop App Installer

This section contains settings for Desktop App Installer.

This Group Policy section is provided by the Group Policy template `DesktopAppInstaller.admx/adml` that is included with the Microsoft Windows 11 version 22H2 Administrative Templates v1.0 (or newer).

18.10.18.1 Ensure 'Enable App Installer' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting controls whether user have access to the Windows Package Manager. Windows Package Manager is a package manager solution that consists of a command line tool and set of services for installing applications on Microsoft Windows Server 2019 (or newer).

The recommended state for this setting is: `Disabled`.

Rationale:

Windows Package Manager is a command line tool can be used to discover, install, upgrade, remove and configure applications, and it can be used as a distribution channel for software packages containing tools and applications. Users should not have access to these types of development tools.

Impact:

Users will not have access to the command line tool, `winget` to discover, install, upgrade, remove, configure, or distribute applications.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\AppInstaller:EnableAppInstaller
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Desktop App Installer\Enable App Installer
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `DesktopAppInstaller.admx/adml` that is included with the Microsoft Windows 11 version 22H2 Administrative Templates v1.0 (or newer).

Default Value:

Enabled. (Users will be able to use the Windows Package Manager.)

References:

1. https://learn.microsoft.com/en-us/windows/package-manager/
2. https://www.malwarebytes.com/blog/news/2024/01/microsoft-disables-ms-appinstaller-after-malicious-use
3. GRID: MS-00000441

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.10.18.2 Ensure 'Enable App Installer Experimental Features' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls whether users can enable experimental features in the Windows Package Manager.

The recommended state for this setting is `Disabled`.

Rationale:

Windows Package Manager is a command line tool can be used to discover, install, upgrade, remove and configure applications, and it can be used as a distribution channel for software packages containing tools and applications. Users should not have access to experimental features.

Impact:

Users will not have access to experimental features in the command line tool, winget to discover, install, upgrade, remove, configure, or distribute applications.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\AppInstaller:EnableExperimentalFeatu
res
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Desktop App Installer\Enable App Installer Experimental Features
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `DesktopAppInstaller.admx/adml` that is included with the Microsoft Windows 11 version 22H2 Administrative Templates v1.0 (or newer).

Default Value:

Enabled. (Users have access to experimental features for the Windows Package Manager.)

References:

1. https://learn.microsoft.com/en-us/windows/package-manager/
2. GRID: MS-00000442

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.10.18.3 Ensure 'Enable App Installer Hash Override' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls whether or not users can override the SHA256 security validation in the Windows Package Manager settings.

The recommended state for this setting is: `Disabled`.

Rationale:

Users should not have the ability to override SHA256 security validation.

Impact:

Users will not have the ability to override the SHA256 security validation.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\AppInstaller:EnableHashOverride
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Desktop App Installer\Enable App Installer Hash Override
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `DesktopAppInstaller.admx/adml` that is included with the Microsoft Windows 11 version 22H2 Administrative Templates v1.0 (or newer).

Default Value:

Enabled. (Users can override the SHA256 security validation in the Windows Package Manager settings.)

References:

1. https://learn.microsoft.com/en-us/windows/package-manager/
2. GRID: MS-00000443

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.10.18.4 Ensure 'Enable App Installer Local Archive Malware Scan Override' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls the ability to override malware scans when the following conditions are true:

1. installing an archive file
2. using a local manifest
3. via command line arguments

The recommended state for this setting is: `Disabled`.

Rationale:

Users should not have the ability to override malware scans.

Impact:

Users will not have the ability to override malware scans when installing an archived file.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\AppInstaller:EnableLocalArchiveMalwa
reScanOverride
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Desktop App Installer\Enable App Installer Local Archive Malware
Scan Override
```

Note: This Group Policy path is provided by the Group Policy template `DesktopAppInstaller.admx/adml` that is included with the Microsoft Windows 11 version 24H2 Administrative Templates (or newer).

Default Value:

Not configured. (Windows Package Manager administrator settings will be adhered to.)

References:

1. https://learn.microsoft.com/en-us/windows/package-manager/
2. GRID: MS-00000592

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.10.18.5 Ensure 'Enable App Installer Microsoft Store Source Certificate Validation Bypass' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls whether Windows Package Manager validates the Microsoft Store certificate hash to match a known Microsoft Store certificate when it initiates a connection to the Microsoft Store source.

The recommended state for this setting is: `Disabled`.

Rationale:

It is important to validate that the Microsoft Store source is not spoofed.

Impact:

Source certificate validation by Windows Package Manager cannot be bypassed when a connection is initiated to the Microsoft Store.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\AppInstaller:EnableBypassCertificate
PinningForMicrosoftStore
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Desktop App Installer\Enable App Installer Microsoft Store Source
Certificate Validation Bypass
```

Note: This Group Policy path is provided by the Group Policy template `DesktopAppInstaller.admx/adml` that is included with the Microsoft Windows 11 version 24H2 Administrative Templates (or newer).

Default Value:

Not configured. (The Windows Package Manager administrator settings will be adhered to.)

References:

1. https://learn.microsoft.com/en-us/windows/package-manager/
2. GRID: MS-00000595

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.10.18.6 Ensure 'Enable App Installer ms-appinstaller protocol' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls whether users can install packages from a website that is using the `ms-appinstaller` protocol. The `ms-appinstaller` protocol allows users to install an application by clicking a link on a website.

The recommended state for this setting is: `Disabled`.

Rationale:

Users should not have the ability to install an application by clicking a link on a website. If an unknown or malicious link is clicked, malicious software could be installed on the system.

Impact:

Users will not have the ability to use the `ms-appinstaller` protocol to install applications by clicking a link on a website.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\AppInstaller:EnableMSAppInstallerPro
tocol
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Desktop App Installer\Enable App Installer ms-appinstaller
protocol
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `DesktopAppInstaller.admx/adml` that is included with the Microsoft Windows 11 version 22H2 Administrative Templates v1.0 (or newer).

Default Value:

Enabled. (Users can install packages from websites that use the `ms-appinstaller` protocol.)

References:

1. https://learn.microsoft.com/en-us/windows/package-manager/
2. GRID: MS-00000444

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.10.18.7 Ensure 'Enable Windows Package Manager command line interfaces' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting controls whether a user can perform actions using the Windows Package Manager through a command line interface (Windows CLI or PowerShell).

The recommended state for this setting is: `Disabled`.

Note: This policy does not override the *Enable App Installer* policy, which is set to `Disabled` in the L2 profile of the CIS Windows Operating System Benchmarks.

Rationale:

Windows Package Manager is a command line tool can be used to discover, install, upgrade, remove and configure applications. It can also be used as a distribution channel for software packages containing tools and applications. Users should not have access to these types of development tools.

Impact:

Users will not have the ability to use Windows Package Manager with Windows CLI or PowerShell.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\AppInstaller:EnableWindowsPackageManagerCommandLineInterfaces
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Desktop App Installer\Enable Windows Package Manager command line interfaces
```

Note: This Group Policy path is provided by the Group Policy template `DesktopAppInstaller.admx/adml` that is included with the Microsoft Windows 11 version 24H2 Administrative Templates (or newer).

Default Value:

Enabled. (Users will be able to execute the Windows Package Manager CLI commands and PowerShell cmdlets if the Enable App Installer policy is not disabled.)

References:

1. https://learn.microsoft.com/en-us/windows/package-manager/
2. GRID: MS-00000594

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.10.19 Desktop Gadgets

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Sidebar.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.10.20 Desktop Window Manager

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `DWM.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.21 Device and Driver Compatibility

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `DeviceCompat.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.10.22 Device Registration (formerly Workplace Join)

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WorkplaceJoin.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Note: This section was initially named *Workplace Join* but was renamed by Microsoft to *Device Registration* starting with the Microsoft Windows 10 RTM (version 1507) Administrative Templates.

18.10.23 Digital Locker

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `DigitalLocker.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.24 Edge UI

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `EdgeUI.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.10.25 Event Forwarding

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `EventForwarding.admx/adml` that is included with the Microsoft Windows Server 2008 (non-R2) Administrative Templates (or newer).

18.10.26 Event Log Service

This section contains recommendations for configuring the Event Log Service.

This Group Policy section is provided by the Group Policy template `EventLog.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.26.1 Application

This section contains recommendations for configuring the Application Event Log.

This Group Policy section is provided by the Group Policy template `EventLog.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.26.1.1 Ensure 'Application: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls Event Log behavior when the log file reaches its maximum size.

The recommended state for this setting is: `Disabled`.

Note: Old events may or may not be retained according to the *Backup log automatically when full* policy setting.

Rationale:

If new events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of threat actors.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_SZ` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\EventLog\Application:Retention
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Event Log Service\Application\Control Event Log behavior when the
log file reaches its maximum size
```

Note: This Group Policy path is provided by the Group Policy template `EventLog.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Retain old events*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

Default Value:

Disabled. (When a log file reaches its maximum size, new events overwrite old events.)

References:

1. GRID: MS-00000445

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 Ensure Adequate Audit Log Storage Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	●	●	●
v7	6.4 Ensure adequate storage for logs Ensure that all systems that store logs have adequate storage space for the logs generated.		●	●

18.10.26.1.2 Ensure 'Application: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting specifies the maximum size of the log file in kilobytes. The maximum log file size can be configured between 1 megabyte (1,024 kilobytes) and 2 terabytes (2,147,483,647 kilobytes) in kilobyte increments.

The recommended state for this setting is: `Enabled: 32,768 or greater`.

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of threat actors.

The consequence of this configuration is that older events will be removed from the logs. Threat actors can take advantage of such a configuration, because they can generate a large number of extraneous events to overwrite any evidence of their attack. These risks can be somewhat reduced if you automate the archival and backup of event log data.

Ideally, all specifically monitored events should be sent to a server that uses Microsoft System Center Operations Manager (SCOM) or some other automated monitoring tool. Such a configuration is particularly important because a threat actor who successfully compromises a server could clear the Security log. If all events are sent to a monitoring server, then you will be able to gather forensic information about the threat actor's activities.

Impact:

When event logs fill to capacity, they will stop recording information unless the retention method for each is set so that the computer will overwrite the oldest entries with the most recent ones. To mitigate the risk of loss of recent data, you can configure the retention method so that older events are overwritten as needed.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `32768`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\EventLog\Application:MaxSize
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: 32,768 or greater`:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Application\Specify the maximum log file size (KB)
```

Note: This Group Policy path is provided by the Group Policy template `EventLog.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Maximum Log Size (KB)*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

Default Value:

Disabled. (The default log size is 20,480 KB - this value can be changed by the local administrator using the Log Properties dialog.)

References:

1. GRID: MS-00000446

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 Ensure Adequate Audit Log Storage Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	●	●	●
v7	6.4 Ensure adequate storage for logs Ensure that all systems that store logs have adequate storage space for the logs generated.		●	●

18.10.26.2 Security

This section contains recommendations for configuring the Security Event Log.

This Group Policy section is provided by the Group Policy template `EventLog.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.26.2.1 Ensure 'Security: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls Event Log behavior when the log file reaches its maximum size.

The recommended state for this setting is: `Disabled`.

Note: Old events may or may not be retained according to the *Backup log automatically when full* policy setting.

Rationale:

If new events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of threat actors.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_SZ` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\EventLog\Security:Retention
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Event Log Service\Security\Control Event Log behavior when the log
file reaches its maximum size
```

Note: This Group Policy path is provided by the Group Policy template `EventLog.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Retain old events*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

Default Value:

Disabled. (When a log file reaches its maximum size, new events overwrite old events.)

References:

1. GRID: MS-00000447

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 Ensure Adequate Audit Log Storage Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	●	●	●
v7	6.4 Ensure adequate storage for logs Ensure that all systems that store logs have adequate storage space for the logs generated.		●	●

18.10.26.2.2 Ensure 'Security: Specify the maximum log file size (KB)' is set to 'Enabled: 196,608 or greater' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting specifies the maximum size of the log file in kilobytes. The maximum log file size can be configured between 1 megabyte (1,024 kilobytes) and 2 terabytes (2,147,483,647 kilobytes) in kilobyte increments.

The recommended state for this setting is: `Enabled: 196,608 or greater`.

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of threat actors.

The consequence of this configuration is that older events will be removed from the logs. Threat actors can take advantage of such a configuration, because they can generate a large number of extraneous events to overwrite any evidence of their attack. These risks can be somewhat reduced if you automate the archival and backup of event log data.

Ideally, all specifically monitored events should be sent to a server that uses Microsoft System Center Operations Manager (SCOM) or some other automated monitoring tool. Such a configuration is particularly important because a threat actor who successfully compromises a server could clear the Security log. If all events are sent to a monitoring server, then you will be able to gather forensic information about the threat actor's activities.

Impact:

When event logs fill to capacity, they will stop recording information unless the retention method for each is set so that the computer will overwrite the oldest entries with the most recent ones. To mitigate the risk of loss of recent data, you can configure the retention method so that older events are overwritten as needed.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `196608`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\EventLog\Security:MaxSize
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: 196,608 or greater`:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Security\Specify the maximum log file size (KB)
```

Note: This Group Policy path is provided by the Group Policy template `EventLog.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Maximum Log Size (KB)*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

Default Value:

Disabled. (The default log size is 20,480 KB - this value can be changed by the local administrator using the Log Properties dialog.)

References:

1. GRID: MS-00000448

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 Ensure Adequate Audit Log Storage Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	●	●	●
v7	6.4 Ensure adequate storage for logs Ensure that all systems that store logs have adequate storage space for the logs generated.		●	●

18.10.26.3 Setup

This section contains recommendations for configuring the Setup Event Log.

This Group Policy section is provided by the Group Policy template `EventLog.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.26.3.1 Ensure 'Setup: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls Event Log behavior when the log file reaches its maximum size.

The recommended state for this setting is: `Disabled`.

Note: Old events may or may not be retained according to the *Backup log automatically when full* policy setting.

Rationale:

If new events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of threat actors.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_SZ` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\EventLog\Setup:Retention
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Event Log Service\Setup\Control Event Log behavior when the log
file reaches its maximum size
```

Note: This Group Policy path is provided by the Group Policy template `EventLog.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Retain old events*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

Default Value:

Disabled. (When a log file reaches its maximum size, new events overwrite old events.)

References:

1. GRID: MS-00000449

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 Ensure Adequate Audit Log Storage Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	●	●	●
v7	6.4 Ensure adequate storage for logs Ensure that all systems that store logs have adequate storage space for the logs generated.		●	●

18.10.26.3.2 Ensure 'Setup: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting specifies the maximum size of the log file in kilobytes. The maximum log file size can be configured between 1 megabyte (1,024 kilobytes) and 2 terabytes (2,147,483,647 kilobytes) in kilobyte increments.

The recommended state for this setting is: `Enabled: 32,768 or greater`.

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of threat actors.

The consequence of this configuration is that older events will be removed from the logs. Threat actors can take advantage of such a configuration, because they can generate a large number of extraneous events to overwrite any evidence of their attack. These risks can be somewhat reduced if you automate the archival and backup of event log data.

Ideally, all specifically monitored events should be sent to a server that uses Microsoft System Center Operations Manager (SCOM) or some other automated monitoring tool. Such a configuration is particularly important because a threat actor who successfully compromises a server could clear the Security log. If all events are sent to a monitoring server, then you will be able to gather forensic information about the threat actor's activities.

Impact:

When event logs fill to capacity, they will stop recording information unless the retention method for each is set so that the computer will overwrite the oldest entries with the most recent ones. To mitigate the risk of loss of recent data, you can configure the retention method so that older events are overwritten as needed.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `32768`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\EventLog\Setup:MaxSize
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: 32,768 or greater`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Event Log Service\Setup\Specify the maximum log file size (KB)
```

Note: This Group Policy path is provided by the Group Policy template `EventLog.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Maximum Log Size (KB)*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

Default Value:

Disabled. (The default log size is 20,480 KB - this value can be changed by the local administrator using the Log Properties dialog.)

References:

1. GRID: MS-00000451

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 Ensure Adequate Audit Log Storage Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	●	●	●
v7	6.4 Ensure adequate storage for logs Ensure that all systems that store logs have adequate storage space for the logs generated.		●	●

18.10.26.4 System

This section contains recommendations for configuring the System Event Log.

This Group Policy section is provided by the Group Policy template `EventLog.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.26.4.1 Ensure 'System: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls Event Log behavior when the log file reaches its maximum size.

The recommended state for this setting is: `Disabled`.

Note: Old events may or may not be retained according to the *Backup log automatically when full* policy setting.

Rationale:

If new events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of threat actors.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_SZ` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\EventLog\System:Retention
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Event Log Service\System\Control Event Log behavior when the log
file reaches its maximum size
```

Note: This Group Policy path is provided by the Group Policy template `EventLog.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Retain old events*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

Default Value:

Disabled. (When a log file reaches its maximum size, new events overwrite old events.)

References:

1. GRID: MS-00000452

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 Ensure Adequate Audit Log Storage Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	●	●	●
v7	6.4 Ensure adequate storage for logs Ensure that all systems that store logs have adequate storage space for the logs generated.		●	●

18.10.26.4.2 Ensure 'System: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting specifies the maximum size of the log file in kilobytes. The maximum log file size can be configured between 1 megabyte (1,024 kilobytes) and 2 terabytes (2,147,483,647 kilobytes) in kilobyte increments.

The recommended state for this setting is: `Enabled: 32,768 or greater`.

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of threat actors.

The consequence of this configuration is that older events will be removed from the logs. Threat actors can take advantage of such a configuration, because they can generate a large number of extraneous events to overwrite any evidence of their attack. These risks can be somewhat reduced if you automate the archival and backup of event log data.

Ideally, all specifically monitored events should be sent to a server that uses Microsoft System Center Operations Manager (SCOM) or some other automated monitoring tool. Such a configuration is particularly important because a threat actor who successfully compromises a server could clear the Security log. If all events are sent to a monitoring server, then you will be able to gather forensic information about the threat actor's activities.

Impact:

When event logs fill to capacity, they will stop recording information unless the retention method for each is set so that the computer will overwrite the oldest entries with the most recent ones. To mitigate the risk of loss of recent data, you can configure the retention method so that older events are overwritten as needed.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `32768`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\EventLog\System:MaxSize
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: 32,768 or greater`:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\System\Specify the maximum log file size (KB)
```

Note: This Group Policy path is provided by the Group Policy template `EventLog.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Maximum Log Size (KB)*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

Default Value:

Disabled. (The default log size is 20,480 KB - this value can be changed by the local administrator using the Log Properties dialog.)

References:

1. GRID: MS-00000453

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 Ensure Adequate Audit Log Storage Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	●	●	●
v7	6.4 Ensure adequate storage for logs Ensure that all systems that store logs have adequate storage space for the logs generated.		●	●

18.10.27 Event Logging

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `EventLogging.admx/adml` that is included with the Microsoft Windows 10 RTM (version 1507) Administrative Templates (or newer).

18.10.28 Event Viewer

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `EventViewer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.29 File Explorer (formerly Windows Explorer)

This section contains recommendations to control the availability of options such as menu items and tabs in dialog boxes.

This Group Policy section is provided by the Group Policy template `WindowsExplorer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note: This section was initially named *Windows Explorer* but was renamed by Microsoft to *File Explorer* starting with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

18.10.29.1 Previous Versions

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `PreviousVersions.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.29.2 Ensure 'Do not apply the Mark of the Web tag to files copied from insecure sources' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether files that are sourced from insecure locations are tagged with Mark of the Web (MOTW).

The recommended state for this setting is: `Disabled`.

Rationale:

MOTW is an important security feature that ensures files from insecure locations are treated with extra caution and are tagged with MOTW. If files are left untagged, users and computers could be exposed to security risks.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\Explorer:DisableMotWOnInsecurePathCopy
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\File Explorer\Do not apply the Mark of the Web tag to files copied from insecure sources
```

Note: This Group Policy path is provided by the Group Policy template `WindowsExplorer.admx/adml` that is included with the Microsoft Windows 11 version 24H2 Administrative Templates (or newer).

Default Value:

Disabled. (Files copied from unsecure sources will be tagged with the appropriate Mark of the Web.)

References:

1. GRID: MS-00000596

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

18.10.29.3 Ensure 'Turn off Data Execution Prevention for Explorer' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Disabling Data Execution Prevention can allow certain legacy plug-in applications to function without terminating Explorer.

The recommended state for this setting is: `Disabled`.

Note: Some legacy plug-in applications and other software may not function with Data Execution Prevention and will require an exception to be defined for that specific plug-in/software.

Rationale:

Data Execution Prevention is an important security feature supported by Explorer that helps to limit the impact of certain types of malware.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\Explorer:NoDataExecutionPrevention
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\File Explorer\Turn off Data Execution Prevention for Explorer
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `Explorer.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Default Value:

Disabled. (Data Execution Prevention will block certain types of malware from exploiting Explorer.)

References:

1. GRID: MS-00000455

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

18.10.29.4 Ensure 'Turn off heap termination on corruption' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Without heap termination on corruption, legacy plug-in applications may continue to function when a File Explorer session has become corrupt. Ensuring that heap termination on corruption is active will prevent this.

The recommended state for this setting is: `Disabled`.

Rationale:

Allowing an application to function after its session has become corrupt increases the risk posture to the system.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\Explorer:NoHeapTerminationOnCorrupti
on
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\File Explorer\Turn off heap termination on corruption
```

Note: This Group Policy path is provided by the Group Policy template `Explorer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Heap termination on corruption is enabled.)

References:

1. GRID: MS-00000456

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

18.10.29.5 Ensure 'Turn off shell protocol protected mode' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to configure the amount of functionality that the shell protocol can have. When using the full functionality of this protocol, applications can open folders and launch files. The protected mode reduces the functionality of this protocol allowing applications to only open a limited set of folders. Applications are not able to open files with this protocol when it is in the protected mode. It is recommended to leave this protocol in the protected mode to increase the security of Windows.

The recommended state for this setting is: `Disabled`.

Rationale:

Limiting the opening of files and folders to a limited set reduces the attack surface of the system.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer:PreXPSP2Shel
lProtocolBehavior
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\File Explorer\Turn off shell protocol protected mode
```

Note: This Group Policy path is provided by the Group Policy template `WindowsExplorer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (The protocol is in the protected mode, allowing applications to only open a limited set of folders.)

References:

1. GRID: MS-00000457

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

18.10.30 File History

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `FileHistory.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.10.31 Find My Device

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `FindMy.admx/adml` that is included with the Microsoft Windows 10 version 1703 Administrative Templates (or newer).

18.10.32 Handwriting

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Handwriting.admx/adml` that is included with the Microsoft Windows 10 version 1709 Administrative Templates (or newer).

18.10.33 HomeGroup

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Sharing.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.10.34 Human Presence

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Sensors.admx/adml` that is included with the Microsoft Windows 11 version 21H2 Administrative Templates (or newer).

18.10.35 Internet Explorer

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `InetRes.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

CIS publishes security guidance for Microsoft Internet Explorer in a separate benchmark from Windows. Additional details can be found in the CIS Microsoft Web Browser Benchmarks Community.

18.10.36 Location and Sensors

This section contains settings for Locations and Sensors.

This Group Policy section is provided by the Group Policy template `Sensors.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.10.36.1 Ensure 'Turn off location' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting turns off the location feature for the computer.

The recommended state for this setting is: `Enabled`.

Rationale:

This setting affects the location feature (e.g. GPS or other location tracking). From a security perspective, it's not a good idea to reveal your location to software in most cases, but there are legitimate uses, such as mapping software. However, they should not be used in high security environments.

Impact:

The location feature is turned off, and all programs on the computer are prevented from using location information from the location feature.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\LocationAndSensors:DisableLocation
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Location and Sensors\Turn off location
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `Sensors.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Default Value:

Disabled. (Programs on the computer are permitted to use location information from the location feature.)

References:

1. GRID: MS-00000459

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.10.37 Maintenance Scheduler

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `msched.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.10.38 Maps

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WinMaps.admx/adml` that is included with the Microsoft Windows 10 version 1511 Administrative Templates (or newer).

18.10.39 MDM

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `MDM.admx/adml` that is included with the Microsoft Windows 10 version 1607 & Server 2016 Administrative Templates (or newer).

18.10.40 Messaging

This section contains messaging settings.

This Group Policy section is provided by the Group Policy template `Messaging.admx/adml` that is included with the Microsoft Windows 10 version 1709 Administrative Templates (or newer).

18.10.40.1 Ensure 'Allow Message Service Cloud Sync' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting allows backup and restore of cellular text messages to Microsoft's cloud services.

The recommended state for this setting is: `Disabled`.

Rationale:

In high-security environments, data must never be shared with third-parties without explicit consent, as it may contain sensitive information.

Impact:

Cellular text messages will not be backed up to (or restored from) Microsoft's cloud services.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\Messaging:AllowMessageSync
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled:`

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Messaging\Allow Message Service Cloud Sync
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `Messaging.admx/adml` that is included with the Microsoft Windows 10 version 1709 Administrative Templates (or newer).

Default Value:

Enabled. (Cellular text messages can be backed up and restored to Microsoft's cloud services.)

References:

1. GRID: MS-00000460

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.10.41 Microsoft account

This section contains recommendations related to Microsoft Accounts.

This Group Policy section is provided by the Group Policy template `MSAPolicy.admx/adml` that is included with the Microsoft Windows 10 version 1703 Administrative Templates (or newer).

18.10.41.1 Ensure 'Block all consumer Microsoft account user authentication' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This setting determines whether applications and services on the device can utilize new consumer Microsoft account authentication via the Windows `OnlineID` and `WebAccountManager` APIs.

The recommended state for this setting is: `Enabled`.

Rationale:

Organizations that want to effectively implement identity management policies and maintain firm control of what accounts are used on their computers will probably want to block Microsoft accounts. Organizations may also need to block Microsoft accounts in order to meet the requirements of compliance standards that apply to their information systems.

Impact:

All applications and services on the device will be prevented from *new* authentications using consumer Microsoft accounts via the Windows `OnlineID` and `WebAccountManager` APIs. Authentications performed directly by the user in web browsers or in apps that use `OAuth` will remain unaffected.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\MicrosoftAccount:DisableUserAuth
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled:`

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Microsoft accounts\Block all consumer Microsoft account user
authentication
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSAPolicy.admx/adml` that is included with the Microsoft Windows 10 version 1703 Administrative Templates (or newer).

Default Value:

Disabled. (Applications and services on the device will be permitted to authenticate using consumer Microsoft accounts via the Windows `OnlineID` and `WebAccountManager` APIs.)

References:

1. GRID: MS-00000461

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.6 Centralize Account Management Centralize account management through a directory or identity service.		●	●
v7	16.8 Disable Any Unassociated Accounts Disable any account that cannot be associated with a business process or business owner.	●	●	●

18.10.42 Microsoft Defender Antivirus (formerly Windows Defender and Windows Defender Antivirus)

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note: Microsoft Defender Antivirus settings have been removed from the Operating System Benchmarks. They are now published separately in the dedicated **Microsoft Defender Antivirus Benchmark**, available within the CIS Microsoft Windows Benchmarks Community.

Note #2: This section was originally named *Windows Defender* but was renamed by Microsoft to *Windows Defender Antivirus* starting with the Microsoft Windows 10 version 1703 Administrative Templates. It was renamed (again) to *Microsoft Defender Antivirus* starting with the Microsoft Windows 10 version 2004 Administrative Templates.

18.10.43 Microsoft Defender Application Guard (formerly Windows Defender Application Guard)

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `AppHVSI.admx/adml` that is included with the Microsoft Windows 10 version 1703 Administrative Templates (or newer).

Note: This section was originally named *Windows Defender Application Guard* but was renamed by Microsoft to *Microsoft Defender Application Guard* starting with the Microsoft Windows 10 version 2004 Administrative Templates.

18.10.44 Microsoft Defender Exploit Guard (formerly Windows Defender Exploit Guard)

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `ExploitGuard.admx/adml` that is included with the Microsoft Windows 10 version 1709 Administrative Templates (or newer).

Note: This section was originally named *Windows Defender Exploit Guard* but was renamed by Microsoft to *Microsoft Defender Exploit Guard* starting with the Microsoft Windows 10 version 2004 Administrative Templates.

18.10.45 Microsoft Edge

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `MicrosoftEdge.admx/adml` that is included with the Microsoft Windows 10 RTM (version 1507) Administrative Templates (or newer).

CIS publishes security guidance for Microsoft Edge in a separate benchmark from Windows. Additional details can be found in the CIS Microsoft Web Browser Benchmarks Community.

18.10.46 Microsoft Secondary Authentication Factor

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `DeviceCredential.admx/adml` that is included with the Microsoft Windows 10 version 1607 & Server 2016 Administrative Templates (or newer).

18.10.47 Microsoft User Experience Virtualization

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `UserExperienceVirtualization.admx/adml` that is included with the Microsoft Windows 10 version 1607 & Server 2016 Administrative Templates (or newer).

18.10.48 NetMeeting

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Conf.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.49 News and interests

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Feeds.admx/adml` that is included with the Microsoft Windows 10 version 21H1 Administrative Templates (or newer).

18.10.50 OneDrive (formerly SkyDrive)

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

Note: This section was initially named *SkyDrive* but was renamed by Microsoft to *OneDrive* starting with the Microsoft Windows 10 RTM (version 1507) Administrative Templates.

18.10.51 Online Assistance

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `HelpAndSupport.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.52 OOBE

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `OOBE.admx/adml` that is included with the Microsoft Windows 10 version 1809 and Server 2019 Administrative Templates (or newer).

18.10.53 Paint

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsCopilot.admx/adml` that is included with the Microsoft Windows 11 version 25H2 Administrative Templates (or newer).

18.10.54 Portable Operating System

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `ExternalBoot.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.10.55 Presentation Settings

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `MobilePCPresentationSettings.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.56 Push To Install

This section contains recommendations related to the Push To Install service.

This Group Policy section is provided by the Group Policy template `PushToInstall.admx/adml` that is included with the Microsoft Windows 10 version 1709 Administrative Templates (or newer).

18.10.56.1 Ensure 'Turn off Push To Install service' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting controls whether users can push Apps to the device from the Microsoft Store App running on other devices or the web.

The recommended state for this setting is: `Enabled`.

Rationale:

In a high security managed environment, application installations should be managed centrally by IT staff, not by end users.

Impact:

Users will not be able to push Apps to this device from the Microsoft Store running on other devices or the web.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\PushToInstall:DisablePushToInstall
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Push to Install\Turn off Push To Install service
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `PushToInstall.admx/adml` that is included with the Microsoft Windows 10 version 1709 Administrative Templates (or newer).

Default Value:

Disabled. (Users are able to push Apps to this device from the Microsoft Store running on other devices or the web.)

References:

1. GRID: MS-00000486

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.5 Allowlist Authorized Software Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.10.57 Remote Desktop Services (formerly Terminal Services)

This section contains recommendations related to Remote Desktop Services.

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note: This section was initially named *Terminal Services* but was renamed by Microsoft to *Remote Desktop Services* starting with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates.

18.10.57.1 RD Licensing (formerly TS Licensing)

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note: This section was initially named *TS Licensing* but was renamed by Microsoft to *RD Licensing* starting with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates.

18.10.57.2 Remote Desktop Connection Client

This section contains recommendations for the Remote Desktop Connection Client.

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.57.2.1 RemoteFX USB Device Redirection

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.10.57.2.2 Ensure 'Do not allow passwords to be saved' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting helps prevent Remote Desktop clients from saving passwords on a computer.

The recommended state for this setting is: `Enabled`.

Note: If this policy setting was previously configured as Disabled or Not configured, any previously saved passwords will be deleted the first time a Remote Desktop client disconnects from any server.

Rationale:

A threat actor with physical access to the computer may be able to break the protection guarding saved passwords. A threat actor who compromises a user's account and connects to their computer could use saved passwords to gain access to additional hosts.

Impact:

The password saving checkbox will be disabled for Remote Desktop clients and users will not be able to save passwords.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal
Services:DisablePasswordSaving
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Remote Desktop Services\Remote Desktop Connection Client\Do not
allow passwords to be saved
```

Note: This Group Policy path is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Users will be able to save passwords using Remote Desktop Connection.)

References:

1. GRID: MS-00000488

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

18.10.57.3 Remote Desktop Session Host (formerly Terminal Server)

This section contains recommendations for the Remote Desktop Session Host.

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note: This section was initially named *Terminal Server* but was renamed by Microsoft to *Remote Desktop Session Host* starting with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates.

18.10.57.3.1 Application Compatibility

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `TerminalServer-Server.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.10.57.3.2 Connections

This section contains recommendations for Connections to the Remote Desktop Session Host.

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.57.3.2.1 Ensure 'Restrict Remote Desktop Services users to a single Remote Desktop Services session' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting allows you to restrict users to a single Remote Desktop Services session.

The recommended state for this setting is: `Enabled`.

Rationale:

This setting ensures that users & administrators who Remote Desktop to a server will continue to use the same session - if they disconnect and reconnect, they will go back to the same session they were using before, preventing the creation of a second simultaneous session. This both prevents unnecessary resource usage by having the server host unnecessary additional sessions (which would put extra load on the server) and also ensures a consistency of experience for the user.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal
Services:fSingleSessionPerUser
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Remote Desktop Services\Remote Desktop Session
Host\Connections\Restrict Remote Desktop Services users to a single Remote
Desktop Services session
```

Note: This Group Policy path is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In older Microsoft Windows Administrative Templates, this setting was named *Restrict Terminal Services users to a single remote session*, but it was renamed starting with the Windows 7 & Server 2008 R2 Administrative Templates.

Default Value:

Enabled. (Users who log on remotely by using Remote Desktop Services will be restricted to a single session (either active or disconnected) on that server. If the user leaves the session in a disconnected state, the user automatically reconnects to that session at the next logon.)

References:

1. GRID: MS-00000490

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.10.57.3.3 Device and Resource Redirection

This section contains recommendations related to Remote Desktop Session Host Device and Resource Redirection.

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.57.3.3.1 Ensure 'Allow UI Automation redirection' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting determines whether User Interface (UI) Automation client applications running on the local computer can access UI elements on the server.

UI Automation gives programs access to most UI elements, which allows use of assistive technology products like Magnifier and Narrator that need to interact with the UI in order to work properly. UI information also allows automated test scripts to interact with the UI. For example, the local computer´s Narrator and Magnifier clients can be used to interact with UI on a web page opened in a remote session.

The recommended state for this setting is: `Disabled`.

Note: Remote Desktop sessions don´t currently support UI Automation redirection.

Rationale:

In a more security-sensitive environment, it is desirable to reduce the possible attack surface. The need for UI Automation redirection within a Remote Desktop session is rare, and not supported at this time, but it makes sense to reduce the number of unexpected avenues for malicious activity to occur.

Impact:

UI Automation clients on the local computer will not be able to interact with remote apps.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal
Services:EnableUiaRedirection
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Device and Resource Redirection\Allow UI Automation redirection
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `TerminalServer.admx/adml` that is included with the Microsoft Windows 10 version 21H2 Administrative Templates (or newer).

Default Value:

Enabled. (Any UI Automation clients on the local computer can interact with remote apps.)

References:

1. https://docs.microsoft.com/en-us/dotnet/framework/ui-automation/ui-automation-overview
2. GRID: MS-00000491

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●

18.10.57.3.3.2 Ensure 'Do not allow COM port redirection' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting specifies whether to prevent the redirection of data to client COM ports from the remote computer in a Remote Desktop Services session.

The recommended state for this setting is: `Enabled`.

Rationale:

In a more security-sensitive environment, it is desirable to reduce the possible attack surface. The need for COM port redirection within a Remote Desktop session is very rare, so makes sense to reduce the number of unexpected avenues for data exfiltration and/or malicious code transfer.

Impact:

Users in a Remote Desktop Services session will not be able to redirect server data to local (client) COM ports.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services:fDisableCcm
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Remote Desktop Services\Remote Desktop Session Host\Device and
Resource Redirection\Do not allow COM port redirection
```

Note: This Group Policy path is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Remote Desktop Services allows COM port redirection.)

References:

1. GRID: MS-00000492

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.10.57.3.3.3 Ensure 'Do not allow drive redirection' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting prevents users from sharing the local drives on their client computers to Remote Desktop Servers that they access. Mapped drives appear in the session folder tree in Windows Explorer in the following format:

`\\TSClient\<driveletter>$`

If local drives are shared they are left vulnerable to intruders who want to exploit the data that is stored on them.

The recommended state for this setting is: `Enabled`.

Rationale:

Data could be forwarded from the user's Remote Desktop Services session to the user's local computer without any direct user interaction. Malicious software already present on a compromised server would have direct and stealthy disk access to the user's local computer during the Remote Desktop session.

Impact:

Drive redirection will not be possible. In most situations, traditional network drive mapping to file shares (including administrative shares) performed manually by the connected user will serve as a capable substitute to still allow file transfers when needed.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services:fDisableCdm
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Remote Desktop Services\Remote Desktop Session Host\Device and
Resource Redirection\Do not allow drive redirection
```

Note: This Group Policy path is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (An RD Session Host maps client drives automatically upon connection.)

References:

1. GRID: MS-00000493

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.10.57.3.3.4 Ensure 'Do not allow location redirection' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting controls the redirection of location data to the remote computer in a Remote Desktop Services session.

The recommended state for this setting is: `Enabled`.

Rationale:

In a more security-sensitive environment, it is desirable to reduce the possible attack surface. The need for location data redirection within a Remote Desktop session is rare, so it makes sense to reduce the number of unexpected avenues for malicious activity to occur.

Impact:

Users will not be able to redirect their location data to the remote computer.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal
Services:fDisableLocationRedir
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Administrative Templates\Windows Components\Remote
Desktop Services\Remote Desktop Session Host\Device and Resource
Redirection\Do not allow location redirection
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `TerminalServer.admx/adml` that is included with the Microsoft Windows 10 version 21H2 Administrative Templates (or newer).

Default Value:

Disabled. (Users can redirect their location data to the remote computer.)

References:

1. GRID: MS-00000494

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●

18.10.57.3.3.5 Ensure 'Do not allow LPT port redirection' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting specifies whether to prevent the redirection of data to client LPT ports during a Remote Desktop Services session.

The recommended state for this setting is: `Enabled`.

Rationale:

In a more security-sensitive environment, it is desirable to reduce the possible attack surface. The need for LPT port redirection within a Remote Desktop session is very rare, so makes sense to reduce the number of unexpected avenues for data exfiltration and/or malicious code transfer.

Impact:

Users in a Remote Desktop Services session will not be able to redirect server data to local (client) LPT ports.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services:fDisableLPT
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Remote Desktop Services\Remote Desktop Session Host\Device and
Resource Redirection\Do not allow LPT port redirection
```

Note: This Group Policy path is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Remote Desktop Services allows LPT port redirection.)

References:

1. GRID: MS-00000495

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.10.57.3.3.6 Ensure 'Do not allow supported Plug and Play device redirection' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting allows you to control the redirection of supported Plug and Play devices, such as Windows Portable Devices, to the remote computer in a Remote Desktop Services session.

The recommended state for this setting is: `Enabled`.

Rationale:

In a more security-sensitive environment, it is desirable to reduce the possible attack surface. The need for Plug and Play device redirection within a Remote Desktop session is very rare, so makes sense to reduce the number of unexpected avenues for data exfiltration and/or malicious code transfer.

Impact:

Users in a Remote Desktop Services session will not be able to redirect their supported (local client) Plug and Play devices to the remote computer.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal
Services:fDisablePNPRedir
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Remote Desktop Services\Remote Desktop Session Host\Device and
Resource Redirection\Do not allow supported Plug and Play device redirection
```

Note: This Group Policy path is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Remote Desktop Services allows redirection of supported Plug and Play devices.)

References:

1. GRID: MS-00000496

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

18.10.57.3.3.7 Ensure 'Do not allow WebAuthn redirection' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting controls the redirection of web authentication (WebAuthn) requests from a Remote Desktop session to the local device. This redirection enables users to authenticate to resources inside the Remote Desktop session using their local authenticator (e.g. Windows Hello for Business, security key, or other).

The recommended state for this setting is: `Enabled`.

Rationale:

In a more security-sensitive environment, it is desirable to reduce the possible attack surface. To reduce this, resources inside the Remote Desktop session should not be allowed to use the local authenticator.

Impact:

Users in a Remote Desktop Services session will not be able to authenticate to resources inside the Remote Desktop session using their local authenticator.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal
Services:fDisableWebAuthn
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Remote Desktop Services\Remote Desktop Session Host\Device and
Resource Redirection\Do not allow WebAuthn redirection
```

Note: This Group Policy path is provided by the Group Policy template `TerminalServer.admx/adml` that is included with the Microsoft Windows 11 version 22H2 Administrative Templates v1.0 (or newer).

Default Value:

Disabled. (Users can use local authenticators inside the Remote Desktop session.)

References:

1. GRID: MS-00000497

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.10.57.3.4 Licensing

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.57.3.5 Printer Redirection

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.57.3.6 Profiles

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.57.3.7 RD Connection Broker (formerly TS Connection Broker)

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note: This section was initially named *TS Connection Broker* but was renamed by Microsoft to *RD Connection Broker* starting with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates.

18.10.57.3.8 Remote Session Environment

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.57.3.9 Security

This section contains recommendations related to Remote Desktop Session Host Security.

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.57.3.9.1 Ensure 'Always prompt for password upon connection' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting specifies whether Remote Desktop Services always prompts the client computer for a password upon connection. You can use this policy setting to enforce a password prompt for users who log on to Remote Desktop Services, even if they already provided the password in the Remote Desktop Connection client.

The recommended state for this setting is: `Enabled`.

Rationale:

Users have the option to store both their username and password when they create a new Remote Desktop Connection shortcut. If the server that runs Remote Desktop Services allows users who have used this feature to log on to the server but not enter their password, then it is possible that a threat actor who has gained physical access to the user's computer could connect to a Remote Desktop Server through the Remote Desktop Connection shortcut, even though they may not know the user's password.

Impact:

Users cannot automatically log on to Remote Desktop Services by supplying their passwords in the Remote Desktop Connection client. They will be prompted for a password to log on.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal
Services:fPromptForPassword
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Remote Desktop Services\Remote Desktop Session
Host\Security\Always prompt for password upon connection
```

Note: This Group Policy path is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In the Microsoft Windows Vista Administrative Templates, this setting was named *Always prompt client for password upon connection*, but it was renamed starting with the Windows Server 2008 (non-R2) Administrative Templates.

Default Value:

Disabled. (Remote Desktop Services allows users to automatically log on if they enter a password in the Remote Desktop Connection client.)

References:

1. GRID: MS-00000498

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

18.10.57.3.9.2 Ensure 'Require secure RPC communication' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to specify whether Remote Desktop Services requires secure Remote Procedure Call (RPC) communication with all clients or allows unsecured communication.

You can use this policy setting to strengthen the security of RPC communication with clients by allowing only authenticated and encrypted requests.

The recommended state for this setting is: `Enabled`.

Rationale:

Allowing unsecure RPC communication can exposes the server to man in the middle attacks and data disclosure attacks.

Impact:

Remote Desktop Services accepts requests from RPC clients that support secure requests, and does not allow unsecured communication with untrusted clients.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal
Services:fEncryptRPCTraffic
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Remote Desktop Services\Remote Desktop Session
Host\Security\Require secure RPC communication
```

Note: This Group Policy path is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Remote Desktop Services always requests security for all RPC traffic. However, unsecured communication is allowed for RPC clients that do not respond to the request.)

References:

1. GRID: MS-00000499

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●

18.10.57.3.9.3 Ensure 'Require use of specific security layer for remote (RDP) connections' is set to 'Enabled: SSL' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting specifies whether to require the use of a specific security layer to secure communications between clients and RD Session Host servers during Remote Desktop Protocol (RDP) connections.

The recommended state for this setting is: `Enabled: SSL`.

Note: In spite of this setting being labeled *SSL*, it is actually enforcing Transport Layer Security (TLS), not the older and less secure, Secure Socket Layer (SSL) protocol.

Rationale:

The native RDP encryption is now considered a weak protocol, so enforcing the use of stronger TLS encryption for all RDP communications between clients and RD Session Host servers is preferred.

Impact:

TLS will be required to authenticate to the RD Session Host server. If TLS is not supported, the connection fails.

Note: By default, this setting will use a self-signed certificate for RDP connections. If your organization has established the use of a Public Key Infrastructure (PKI) for SSL/TLS encryption, then we recommend that you also configure the *Server authentication certificate template* setting to instruct RDP to use a certificate from your PKI instead of a self-signed one. Note that the certificate template used for this purpose must have “Client Authentication” configured as an Intended Purpose. Note also that a valid, non-expired certificate using the specified template must already be installed on the server for it to work.

Note #2: Some third party two-factor authentication solutions (e.g. RSA Authentication Agent) can be negatively affected by this setting, as the SSL/TLS security layer will expect the user's Windows password upon initial connection attempt (before the RDP logon screen), and once successfully authenticated, pass the credential along to that Windows session on the RDP host (to complete the login). If a two-factor agent is present and expecting a different credential at the RDP logon screen, this initial connection may result in a failed logon attempt, and also effectively cause a “double logon” requirement for each and every new RDP session.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `2`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services:SecurityLayer
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: SSL`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Remote Desktop Services\Remote Desktop Session
Host\Security\Require use of specific security layer for remote (RDP)
connections
```

Note: This Group Policy path is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (The security method to be used for remote connections to RD Session Host servers is not specified at the Group Policy level.)

References:

1. GRID: MS-00000500

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●

18.10.57.3.9.4 Ensure 'Require user authentication for remote connections by using Network Level Authentication' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to specify whether to require user authentication for remote connections to the RD Session Host server by using Network Level Authentication.

The recommended state for this setting is: `Enabled`.

Rationale:

Requiring that user authentication occur earlier in the remote connection process enhances security.

Impact:

Only client computers that support Network Level Authentication can connect to the RD Session Host server.

Note: Some third party two-factor authentication solutions (e.g. RSA Authentication Agent) can be negatively affected by this setting, as Network Level Authentication will expect the user's Windows password upon initial connection attempt (before the RDP logon screen), and once successfully authenticated, pass the credential along to that Windows session on the RDP host (to complete the login). If a two-factor agent is present and expecting a different credential at the RDP logon screen, this initial connection may result in a failed logon attempt, and also effectively cause a “double logon” requirement for each and every new RDP session.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal
Services:UserAuthentication
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Remote Desktop Services\Remote Desktop Session
Host\Security\Require user authentication for remote connections by using
Network Level Authentication
```

Note: This Group Policy path is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In the Microsoft Windows Vista Administrative Templates, this setting was initially named *Require user authentication using RDP 6.0 for remote connections*, but it was renamed starting with the Windows Server 2008 (non-R2) Administrative Templates.

Default Value:

On Windows Server 2008 R2 or older: Disabled.

On Windows Server 2012 (non-R2) or newer: Enabled.

References:

1. GRID: MS-00000501

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●

18.10.57.3.9.5 Ensure 'Set client connection encryption level' is set to 'Enabled: High Level' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting specifies whether to require the use of a specific encryption level to secure communications between client computers and RD Session Host servers during Remote Desktop Protocol (RDP) connections. This policy only applies when you are using native RDP encryption. However, native RDP encryption (as opposed to SSL encryption) is not recommended. This policy does not apply to SSL encryption.

The recommended state for this setting is: `Enabled: High Level`.

Rationale:

If Remote Desktop client connections that use low level encryption are allowed, it is more likely that a threat actor will be able to decrypt any captured Remote Desktop Services network traffic.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `3`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services:MinEncryptionLevel
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: High Level`:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security\Set client connection encryption level
```

Note: This Group Policy path is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Enabled: High Level. (All communications between clients and RD Session Host servers during remote connections using native RDP encryption must be 128-bit strength. Clients that do not support 128-bit encryption will be unable to establish Remote Desktop Server sessions.)

References:

1. GRID: MS-00000502

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●

18.10.57.3.10 Session Time Limits

This section contains recommendations related to Remote Desktop Session Host Session Time Limits.

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.57.3.10.1 Ensure 'Set time limit for active but idle Remote Desktop Services sessions' is set to 'Enabled: 15 minutes or less, but not Never (0)' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to specify the maximum amount of time that an active Remote Desktop Services session can be idle (without user input) before it is automatically disconnected.

The recommended state for this setting is: `Enabled: 15 minutes or less, but not Never (0)`.

Rationale:

This setting helps to prevent active Remote Desktop sessions from tying up the computer for long periods of time while not in use, preventing computing resources from being consumed by large numbers of inactive sessions. In addition, old, forgotten Remote Desktop sessions that are still active can cause password lockouts if the user's password has changed but the old session is still running. For systems that limit the number of connected users (e.g. servers in the default Administrative mode - 2 sessions only), other users' old but still active sessions can prevent another user from connecting, resulting in an effective denial-of-service.

In addition, session timeouts that are misconfigured or set for a long period of time can leave the system open to a threat actor hijacking the session.

Impact:

Remote Desktop Services will automatically disconnect active but idle sessions after 15 minutes (or the specified amount of time). The user receives a warning two minutes before the session disconnects, which allows the user to press a key or move the mouse to keep the session active. Note that idle session time limits do not apply to console sessions.

Note: This setting disconnects the session but does not terminate it. Any jobs running before the disconnection will continue to run. If an organization requires sessions to be fully terminated and deleted, the *End session when time limits are reached* setting must be enabled.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a REG_DWORD value of `900000` or less, but not `0`

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal
Services:MaxIdleTime
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: 15 minutes or less, but not Never (0)`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Remote Desktop Services\Remote Desktop Session Host\Session Time
Limits\Set time limit for active but idle Remote Desktop Services sessions
```

Note: This Group Policy path is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In older Microsoft Windows Administrative Templates, this setting was named *Set time limit for active but idle Terminal Services sessions*, but it was renamed starting with the Windows 7 & Server 2008 R2 Administrative Templates.

Default Value:

Disabled. (Remote Desktop Services allows sessions to remain active but idle for an unlimited amount of time.)

References:

1. GRID: MS-00000503

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

18.10.57.3.11 Temporary folders

This section contains recommendations related to Remote Desktop Session Host Session Temporary folders.

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.57.3.11.1 Ensure 'Do not delete temp folders upon exit' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting specifies whether Remote Desktop Services retains a user's per-session temporary folders at logoff.

The recommended state for this setting is: `Disabled`.

Rationale:

Sensitive information could be contained inside the temporary folders and visible to other administrators that log into the system.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal
Services:DeleteTempDirsOnExit
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Remote Desktop Services\Remote Desktop Session Host\Temporary
Folders\Do not delete temp folders upon exit
```

Note: This Group Policy path is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In older Microsoft Windows Administrative Templates, this setting was named *Do not delete temp folder upon exit*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

Default Value:

Disabled. (Temporary folders are deleted when a user logs off.)

References:

1. GRID: MS-00000505

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

18.10.57.3.11.2 Ensure 'Do not use temporary folders per session' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

By default, Remote Desktop Services creates a separate temporary folder on the RD Session Host server for each active session that a user maintains on the RD Session Host server. The temporary folder is created on the RD Session Host server in a Temp folder under the user's profile folder and is named with the `sessionid`. This temporary folder is used to store individual temporary files.

To reclaim disk space, the temporary folder is deleted when the user logs off from a session.

The recommended state for this setting is: `Disabled`.

Rationale:

Disabling this setting keeps the cached data independent for each session, both reducing the chance of problems from shared cached data between sessions, and keeping possibly sensitive data separate to each user session.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal
Services:PerSessionTempDir
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Remote Desktop Services\Remote Desktop Session Host\Temporary
Folders\Do not use temporary folders per session
```

Note: This Group Policy path is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Per-session temporary folders are created.)

References:

1. GRID: MS-00000506

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.4 Enforce Data Retention Retain data according to the enterprise's data management process. Data retention must include both minimum and maximum timelines.	●	●	●

18.10.58 RSS Feeds

This section contains recommendations related to RSS feeds.

This Group Policy section is provided by the Group Policy template `InetRes.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.58.1 Ensure 'Prevent downloading of enclosures' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting prevents the user from having enclosures (file attachments) downloaded from an RSS feed to the user's computer.

The recommended state for this setting is: `Enabled`.

Rationale:

Allowing attachments to be downloaded through the RSS feed can introduce files that could have malicious intent.

Impact:

Users cannot set the Feed Sync Engine to download an enclosure through the Feed property page. Developers cannot change the download setting through feed APIs.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Internet
Explorer\Feeds:DisableEnclosureDownload
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\RSS Feeds\Prevent downloading of enclosures
```

Note: This Group Policy path is provided by the Group Policy template `InetRes.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In older Microsoft Windows Administrative Templates, this setting was named *Turn off downloading of enclosures*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

Default Value:

Disabled. (Users can set the Feed Sync Engine to download an enclosure through the Feed property page. Developers can change the download setting through the Feed APIs.)

References:

1. GRID: MS-00000507

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	7.2 Disable Unnecessary or Unauthorized Browser or Email Client Plugins Uninstall or disable any unauthorized browser or email client plugins or add-on applications.		●	●

18.10.58.2 Ensure 'Turn on Basic feed authentication over HTTP' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls whether RSS feeds can be authenticated using the Basic authentication scheme over an unencrypted HTTP connection.

A developer cannot change this setting through the Feed APIs.

The recommended state for this setting is: `Disabled`.

Rationale:

Allowing RSS feeds to use Basic authentication over HTTP will transmit user credentials in plain text, where they could be intercepted enroute by a threat actor.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet
Explorer\Feeds:AllowBasicAuthInClear
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Administrative Templates\Windows Components\RSS
Feeds\Turn on Basic feed authentication over HTTP
```

Note: This Group Policy path is provided by the Group Policy template `InetRes.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Default Value:

Disabled. (The Windows RSS Platform will not authenticate to RSS feed servers using the Basic authentication scheme over a less secure HTTP connection.)

References:

1. GRID: MS-00000593

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	7.2 Disable Unnecessary or Unauthorized Browser or Email Client Plugins Uninstall or disable any unauthorized browser or email client plugins or add-on applications.		●	●

18.10.59 Search

This section contains recommendations for Search settings.

This Group Policy section is provided by the Group Policy template `Search.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.59.1 OCR

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `SearchOCR.admx/adml` that is only included with the Microsoft Windows 7 & Server 2008 R2 through the Windows 10 version 1511 Administrative Templates.

18.10.59.2 Ensure 'Allow Cloud Search' is set to 'Enabled: Disable Cloud Search' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting allows search and Cortana to search cloud sources like OneDrive and SharePoint.

The recommended state for this setting is: `Enabled: Disable Cloud Search`.

Rationale:

In high-security environments, data must never be shared with third-parties without explicit consent, as it may contain sensitive information.

Impact:

Search and Cortana will not be permitted to search cloud sources like OneDrive and SharePoint.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\Windows Search:AllowCloudSearch
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Disable Cloud Search`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Search\Allow Cloud Search
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `Search.admx/adml` that is included with the Microsoft Windows 10 version 1709 Administrative Templates (or newer).

Default Value:

Enabled: Enable Cloud Search. (Allow search and Cortana to search cloud sources like OneDrive and SharePoint.)

References:

1. GRID: MS-00000508

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.10.59.3 Ensure 'Allow indexing of encrypted files' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls whether encrypted items are allowed to be indexed. When this setting is changed, the index is rebuilt completely. Full volume encryption (such as BitLocker Drive Encryption or a non-Microsoft solution) must be used for the location of the index to maintain security for encrypted files.

The recommended state for this setting is: `Disabled`.

Rationale:

Indexing and allowing users to search encrypted files could potentially reveal confidential data stored within the encrypted files.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\Windows
Search:AllowIndexingEncryptedStoresOrItems
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Search\Allow indexing of encrypted files
```

Note: This Group Policy path is provided by the Group Policy template `Search.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Search service components (including non-Microsoft components) are expected not to index encrypted items or encrypted stores.)

References:

1. GRID: MS-00000511

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	14.8 Encrypt Sensitive Information at Rest Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			●

18.10.59.4 Ensure 'Allow search highlights' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting controls search highlights in the start menu search box and in search home.

The recommended state for this setting is: `Disabled`.

Rationale:

In high-security environments, data must never be shared with third-parties without explicit consent, as it may contain sensitive information.

Impact:

“Interesting”, “informative”, and “noteworthy” information about the current date will not be displayed (by Microsoft) to the user.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\Windows
Search:EnableDynamicContentInWSB
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Search\Allow search highlights
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `Search.admx/adml` that is included with the Microsoft Windows 10 version 21H2 Administrative Templates (or newer).

Default Value:

Enabled. (Search highlights in the start menu search box and in search home will be available.)

References:

1. GRID: MS-00000513

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●

18.10.60 Security Center

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `SecurityCenter.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.61 Shutdown Options

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WinInit.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.62 Smart Card

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `SmartCard.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.63 Software Protection Platform

This section contains recommendations related to the Software Protection Platform.

This Group Policy section is provided by the Group Policy template `AVSValidationGP.admx/adml` that is included with the Microsoft Windows 10 RTM (version 1507) Administrative Templates (or newer).

18.10.63.1 Ensure 'Turn off KMS Client Online AVS Validation' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

The Key Management Service (KMS) is a Microsoft license activation method that entails setting up a local server to store the software licenses. The KMS server itself needs to connect to Microsoft to activate the KMS service, but subsequent on-network clients can activate Microsoft Windows OS and/or their Microsoft Office via the KMS server instead of connecting directly to Microsoft. This policy setting lets you opt-out of sending KMS client activation data to Microsoft automatically.

The recommended state for this setting is: `Enabled`.

Rationale:

Even though the KMS licensing method does not *require* KMS clients to connect to Microsoft, they still send KMS client activation state data to Microsoft automatically. In high-security environments, data must never be shared with third-parties without explicit consent, as it may contain sensitive information.

Impact:

The computer is prevented from sending data to Microsoft regarding its KMS client activation state.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\CurrentVersion\Software
Protection Platform:NoGenTicket
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Software Protection Platform\Turn off KMS Client Online AVS
Validation
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `AVSValidationGP.admx/adml` that is included with the Microsoft Windows 10 RTM (version 1507) Administrative Templates (or newer).

Default Value:

Disabled. (KMS client activation data will automatically be sent to Microsoft when the device activates.)

References:

1. GRID: MS-00000514

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.10.64 Sound Recorder

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `SoundRec.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.65 Speech

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Speech.admx/adml` that is included with the Microsoft Windows 10 version 1703 Administrative Templates (or newer).

18.10.66 Store

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WinStoreUI.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates, or by the Group Policy template `WindowsStore.admx/adml` that is included with the Microsoft Windows 10 version 1511 Administrative Templates (or newer).

18.10.67 Sync your settings

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `SettingSync.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.10.68 Tablet PC

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.69 Task Scheduler

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `TaskScheduler.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.70 Tenant Restrictions

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `TenantRestrictions.admx/adml` that is included with the Microsoft Windows 11 version 21H2 Administrative Templates (or newer).

18.10.71 Text Input

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `TextInput.admx/adml` that is only included with the Microsoft Windows 10 RTM (version 1507) Administrative Templates and Microsoft Windows 10 version 1511 Administrative Templates.

18.10.72 Widgets

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `NewsAndInterests.admx/adml` that is included with the Microsoft Windows 11 version 21H2 Administrative Templates (or newer).

18.10.73 Windows AI

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsCopilot.admx/adml` that is included with the Microsoft Windows 11 version 25H2 Administrative Templates (or newer).

18.10.74 Windows Calendar

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WinCal.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.75 Windows Color System

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsColorSystem.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.76 Windows Customer Experience Improvement Program

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `CEIPEnable.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.77 Windows Defender SmartScreen

This section contains Windows Defender SmartScreen settings.

This Group Policy section is provided by the Group Policy template `SmartScreen.admx/adml` that is included with the Microsoft Windows 10 version 1703 Administrative Templates (or newer).

18.10.77.1 Enhanced Phishing Protection

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WebThreatDefense.admx/adml` that is included with the Microsoft Windows 11 version 22H2 Administrative Templates v1.0 (or newer).

18.10.77.2 Explorer

This section contains recommendations for Explorer-related Windows Defender SmartScreen settings.

The Group Policy settings contained within this section are provided by the Group Policy template `WindowsExplorer.admx/adml` that is included with the Microsoft Windows 10 version 1703 Administrative Templates (or newer).

18.10.77.2.1 Ensure 'Configure Windows Defender SmartScreen' is set to 'Enabled: Warn and prevent bypass' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to manage the behavior of Windows SmartScreen. Windows SmartScreen helps keep PCs safer by warning users before running unrecognized programs downloaded from the Internet. Some information is sent to Microsoft about files and programs run on PCs with this feature enabled.

The recommended state for this setting is: `Enabled: Warn and prevent bypass`.

Rationale:

Windows SmartScreen helps keep PCs safer by warning users before running unrecognized programs downloaded from the Internet. However, due to the fact that some information is sent to Microsoft about files and programs run on PCs some organizations may prefer to disable it.

Impact:

Users will be warned and prevented from running unrecognized programs downloaded from the Internet.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1` (EnableSmartScreen) and `REG_SZ` value of `Block` (ShellSmartScreenLevel).

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System:EnableSmartScre
en
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System:ShellSmartScree
nLevel
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Warn and prevent bypass`:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender SmartScreen\Explorer\Configure Windows Defender SmartScreen
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WindowsExplorer.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Configure Windows SmartScreen*, but it was renamed starting with the Windows 10 version 1703 Administrative Templates.

Default Value:

Enabled. (Users can change settings.)

References:

1. GRID: MS-00000526

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

18.10.78 Windows Error Reporting

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `ErrorReporting.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.79 Windows Game Recording and Broadcasting

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `GameDVR.admx/adml` that is included with the Microsoft Windows 10 RTM (version 1507) Administrative Templates (or newer).

18.10.80 Windows Hello for Business (formerly Microsoft Passport for Work)

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Passport.admx/adml` that is included with the Microsoft Windows 10 RTM (version 1507) Administrative Templates (or newer).

Note: This section was initially named *Microsoft Passport for Work* but was renamed by Microsoft to *Windows Hello for Business* starting with the Microsoft Windows 10 version 1607 & Server 2016 Administrative Templates.

18.10.81 Windows Ink Workspace

This section contains recommendations related to the Windows Ink Workspace.

This Group Policy section is provided by the Group Policy template `WindowsInkWorkspace.admx/adml` that is included with the Microsoft Windows 10 version 1607 & Server 2016 Administrative Templates (or newer).

18.10.81.1 Ensure 'Allow suggested apps in Windows Ink Workspace' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting determines whether suggested apps in Windows Ink Workspace are allowed.

The recommended state for this setting is: `Disabled`.

Rationale:

This Microsoft feature is designed to collect data and suggest apps based on that data collected. Disabling this setting will help ensure your data is not shared with any third party.

Impact:

The suggested apps in Windows Ink Workspace will not be allowed.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\WindowsInkWorkspace:AllowSuggestedAppsInWind
owsInkWorkspace
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows Ink Workspace\Allow suggested apps in Windows Ink
Workspace
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WindowsInkWorkspace.admx/adml` that is included with the Microsoft Windows 10 version 1607 & Server 2016 Administrative Templates (or newer).

Default Value:

Enabled. (The suggested apps in Windows Ink Workspace will be allowed.)

References:

1. GRID: MS-00000529

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.10.81.2 Ensure 'Allow Windows Ink Workspace' is set to 'Enabled: On, but disallow access above lock' OR 'Enabled: Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether Windows Ink items are allowed above the lock screen.

The recommended state for this setting is: `Enabled: On, but disallow access above lock` OR `Enabled: Disabled`.

Rationale:

Allowing any apps to be accessed while system is locked is not recommended. If this feature is permitted, it should only be accessible once a user authenticates with the proper credentials.

Impact:

Windows Ink Workspace will not be permitted above the lock screen.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0` or `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\WindowsInkWorkspace:AllowWindowsInkWorkspace
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: On, but disallow access above lock` OR `Enabled: Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows Ink Workspace\Allow Windows Ink Workspace
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WindowsInkWorkspace.admx/adml` that is included with the Microsoft Windows 10 version 1607 & Server 2016 Administrative Templates (or newer).

Default Value:

Enabled. (Windows Ink Workspace is permitted above the lock screen.)

References:

1. GRID: MS-00000530

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.10.82 Windows Installer

This section contains recommendations related to Windows Installer.

This Group Policy section is provided by the Group Policy template `MSI.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.82.1 Ensure 'Allow user control over installs' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This setting controls whether users are permitted to change installation options that typically are available only to system administrators. The security features of Windows Installer normally prevent users from changing installation options that are typically reserved for system administrators, such as specifying the directory to which files are installed. If Windows Installer detects that an installation package has permitted the user to change a protected option, it stops the installation and displays a message. These security features operate only when the installation program is running in a privileged security context in which it has access to directories denied to the user.

The recommended state for this setting is: `Disabled`.

Rationale:

In an enterprise managed environment, only IT staff with administrative rights should be installing or changing software on a system. Allowing users the ability to have any control over installs can risk unapproved software from being installed or removed from a system, which could cause the system to become vulnerable to compromise.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer:EnableUserControl
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows Installer\Allow user control over installs
```

Note: This Group Policy path is provided by the Group Policy template `MSI.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In older Microsoft Windows Administrative Templates, this setting was named *Enable user control over installs*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

Default Value:

Disabled. (The security features of Windows Installer will prevent users from changing installation options typically reserved for system administrators, such as specifying the directory to which files are installed.)

References:

1. GRID: MS-00000531

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

18.10.82.2 Ensure 'Always install with elevated privileges' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This setting controls whether or not Windows Installer should use system permissions when it installs any program on the system.

Note: This setting appears both in the Computer Configuration and User Configuration folders. To make this setting effective, you must enable the setting in both folders.

Caution: If enabled, skilled users can take advantage of the permissions this setting grants to change their privileges and gain permanent access to restricted files and folders. Note that the User Configuration version of this setting is not guaranteed to be secure.

The recommended state for this setting is: `Disabled`.

Rationale:

Users with limited privileges can exploit this feature by creating a Windows Installer installation package that creates a new local account that belongs to the local built-in Administrators group, adds their current account to the local built-in Administrators group, installs malicious software, or performs other unauthorized activities.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer:AlwaysInstallElevated
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows Installer\Always install with elevated privileges
```

Note: This Group Policy path is provided by the Group Policy template `MSI.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Windows Installer will apply the current user's permissions when it installs programs that a system administrator does not distribute or offer. This will prevent standard users from installing applications that affect system-wide configuration items.)

References:

1. GRID: MS-00000532

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	4.3 Ensure the Use of Dedicated Administrative Accounts Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	●	●	●

18.10.82.3 Ensure 'Prevent Internet Explorer security prompt for Windows Installer scripts' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting controls whether Web-based programs are allowed to install software on the computer without notifying the user.

The recommended state for this setting is: `Disabled`.

Rationale:

Suppressing the system warning can pose a security risk and increase the attack surface on the system.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer:SafeForScripting
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows Installer\Prevent Internet Explorer security prompt for
Windows Installer scripts
```

Note: This Group Policy path is provided by the Group Policy template `MSI.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Disable IE security prompt for Windows Installer scripts*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

Default Value:

Disabled. (When a script hosted by an Internet browser tries to install a program on the system, the system warns users and allows them to select or refuse the installation.)

References:

1. GRID: MS-00000533

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.5 Allowlist Authorized Software Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.		●	●

18.10.83 Windows Logon Options

This section contains recommendations related to Windows Logon Options.

This Group Policy section is provided by the Group Policy template `WinLogon.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.83.1 Ensure 'Configure the transmission of the user's password in the content of MPR notifications sent by winlogon.' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls whether `winlogon` includes a user's password in the content of Multiple Provider Router (MPR) notifications. MPR handles communication between the Windows operating system and the installed network providers. MPR checks the registry to determine which providers are installed on the system and the order they are cycled through.

The recommended state for this setting is: `Disabled`.

Rationale:

MPR is a legacy utility that provides notifications to registered credential managers or network providers when there is a logon event, or a password change event. Although MPR can be used by legitimate applications, the user's password field of these notifications should be empty to prevent abuse by threat actors.

Impact:

None - this is the default behavior.

Note: If Citrix Workspace App is used in the environment, an exception to this recommendation is needed. For further information, please visit: Cumulative Update 2 (CU2) | Citrix Workspace™ app 2402 LTSR for Windows.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:EnableMPR
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows Logon Options\Configure the transmission of the user's
password in the content of MPR notifications sent by winlogon.
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WinLogon.admx/adml` that is included with the Microsoft Windows 11 version 22H2 Administrative Templates v1.0 (or newer).

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Enable MPR notifications for the system*, but it was renamed starting with the Windows 11 version 22H2 Administrative Templates.

Default Value:

Disabled. (Winlogon sends MPR notifications with empty password fields of the user's authentication info.)

References:

1. https://techcommunity.microsoft.com/t5/microsoft-security-baselines/windows-11-version-22h2-security-baseline/ba-p/3632520
2. https://learn.microsoft.com/en-us/windows/win32/secauthn/multiple-provider-router
3. GRID: MS-00000534

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.10.83.2 Ensure 'Sign-in and lock last interactive user automatically after a restart' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting controls whether a device will automatically sign-in the last interactive user after Windows Update restarts the system.

The recommended state for this setting is: `Disabled`.

Rationale:

Disabling this feature will prevent the caching of user's credentials and unauthorized use of the device, and also ensure the user is aware of the restart.

Impact:

The device does not store the user's credentials for automatic sign-in after a Windows Update restart. The users' lock screen apps are not restarted after the system restarts. The user is required to present the logon credentials in order to proceed after restart.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:DisableAutomat
icRestartSignOn
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows Logon Options\Sign-in and lock last interactive user
automatically after a restart
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WinLogon.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Sign-in last interactive user automatically after a system-initiated restart*, but it was renamed starting with the Windows 10 version 1903 Administrative Templates.

Default Value:

Enabled. (The device securely saves the user's credentials (including the user name, domain and encrypted password) to configure automatic sign-in after a Windows Update restart. After the Windows Update restart, the user is automatically signed-in and the session is automatically locked with all the lock screen apps configured for that user.)

References:

1. GRID: MS-00000535

Additional Information:

Disable this policy setting so that the device does not store the user's credentials for automatic sign-in after a Windows Update restart and the users' lock screen apps are not restarted after the system restarts.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

18.10.84 Windows Media Digital Rights Management

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsMediaDRM.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.85 Windows Media Player

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsMediaPlayer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.86 Windows Messenger

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsMessenger.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.87 Windows Mobility Center

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `MobilePCMobilityCenter.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.88 Windows PowerShell

This section contains recommendations related to Windows PowerShell.

This Group Policy section is provided by the Group Policy template `PowerShellExecutionPolicy.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.10.88.1 Ensure 'Turn on PowerShell Script Block Logging' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting enables logging of all PowerShell script input to the `Applications and Services Logs\Microsoft\Windows\PowerShell\Operational` Event Log channel.

The recommended state for this setting is: `Enabled`.

Note: If logging of *Script Block Invocation Start/Stop Events* is enabled (option box checked), PowerShell will log additional events when invocation of a command, script block, function, or script starts or stops. Enabling this option generates a high volume of event logs. CIS has intentionally chosen not to make a recommendation for this option, since it generates a large volume of events. **If an organization chooses to enable the optional setting (checked), this also conforms to the benchmark.**

Rationale:

Logs of PowerShell script input can be very valuable when performing forensic investigations of PowerShell attack incidents to determine what occurred.

Impact:

PowerShell script input will be logged to the `Applications and Services Logs\Microsoft\Windows\PowerShell\Operational` Event Log channel, which can contain credentials and sensitive information.

Note: Configuring this setting to `Enabled` generates a high volume of event logs which will be overwritten if the log size is not expanded or offloaded to a log collection system.

Warning: There are potential risks of capturing credentials and sensitive information in the PowerShell logs, which could be exposed to users who have read-access to those logs. Microsoft provides a feature called "Protected Event Logging" to better secure event log data. For assistance with protecting event logging, visit: About Logging Windows - PowerShell | Microsoft Docs.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging:Enable
ScriptBlockLogging
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows PowerShell\Turn on PowerShell Script Block Logging
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `PowerShellExecutionPolicy.admx/adml` that is included with the Microsoft Windows 10 RTM (version 1507) Administrative Templates (or newer).

Default Value:

Enabled. (PowerShell will log script blocks the first time they are used.)

References:

1. https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_logging_windows?view=powershell-7.2#protected-event-logging
2. GRID: MS-00000536

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.8 Collect Command-Line Audit Logs Collect command-line audit logs. Example implementations include collecting audit logs from PowerShell®, BASH™, and remote administrative terminals.		●	●
v7	8.8 Enable Command-line Audit Logging Enable command-line audit logging for command shells, such as Microsoft Powershell and Bash.		●	●

18.10.88.2 Ensure 'Turn on PowerShell Transcription' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This Policy setting lets you capture the input and output of Windows PowerShell commands into text-based transcripts.

The recommended state for this setting is: `Enabled`.

Rationale:

PowerShell transcript input can be very valuable when performing forensic investigations of PowerShell attack incidents to determine what occurred.

Impact:

PowerShell transcript input will be logged to `PowerShell_transcript` output files, which are saved to the My Documents folder (within a separate subfolder for each day) of each users´ profile by default. Optionally, a specific output directory name can be specified, which will contain all PowerShell transcript logs in a subfolder of My Documents. If specifying a full path outside the users My Documents folder, other users on the system could have access to view these logs, which may contain sensitive information such as passwords.

Warning: There are potential risks of capturing credentials and sensitive information in `PowerShell_transcript` output files, which could be exposed to users who have read access to the files.

Warning #2: PowerShell Transcription is not compatible with the natively installed PowerShell v4 on Microsoft Windows 10 version 1511 and Server 2012 R2 and below. If this recommendation is set as prescribed, PowerShell will need to be updated to at least v5.1 or newer. For more information on updating PowerShell, please see Windows PowerShell System Requirements - PowerShell | Microsoft Learn.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\PowerShell\Transcription:EnableTrans
cripting
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows PowerShell\Turn on PowerShell Transcription
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `PowerShellExecutionPolicy.admx/adml` that is included with the Microsoft Windows 10 RTM (version 1507) Administrative Templates (or newer).

Default Value:

Disabled. (Transcription of PowerShell-based applications is disabled by default, although transcription can still be enabled through the `Start-Transcript` cmdlet.)

References:

1. https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_group_policy_settings?view=powershell-7.2#turn-on-powershell-transcription
2. GRID: MS-00000537

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.8 Collect Command-Line Audit Logs Collect command-line audit logs. Example implementations include collecting audit logs from PowerShell®, BASH™, and remote administrative terminals.		●	●

18.10.89 Windows Reliability Analysis

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `RacWmiProv.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.10.90 Windows Remote Management (WinRM)

This section contains recommendations related to Windows Remote Management (WinRM).

This Group Policy section is provided by the Group Policy template `WindowsRemoteManagement.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.90.1 WinRM Client

This section contains recommendations related to the Windows Remote Management (WinRM) client.

This Group Policy section is provided by the Group Policy template `WindowsRemoteManagement.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.90.1.1 Ensure 'Allow Basic authentication' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to manage whether the Windows Remote Management (WinRM) client uses Basic authentication.

The recommended state for this setting is: `Disabled`.

Rationale:

Basic authentication is less robust than other authentication methods available in WinRM because credentials including passwords are transmitted in plain text. A threat actor who is able to capture packets on the network where WinRM is running may be able to determine the credentials used for accessing remote hosts via WinRM.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\WinRM\Client:AllowBasic
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows Remote Management (WinRM)\WinRM Client\Allow Basic
authentication
```

Note: This Group Policy path is provided by the Group Policy template `WindowsRemoteManagement.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (The WinRM client does not use Basic authentication.)

References:

1. GRID: MS-00000538

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	16.5 Encrypt Transmittal of Username and Authentication Credentials Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.		●	●

18.10.90.1.2 Ensure 'Allow unencrypted traffic' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to manage whether the Windows Remote Management (WinRM) client sends and receives unencrypted messages over the network.

The recommended state for this setting is: `Disabled`.

Rationale:

Encrypting WinRM network traffic reduces the risk of a threat actor viewing or modifying WinRM messages as they transit the network.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\WinRM\Client:AllowUnencryptedTraffic
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows Remote Management (WinRM)\WinRM Client\Allow unencrypted
traffic
```

Note: This Group Policy path is provided by the Group Policy template `WindowsRemoteManagement.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (The WinRM client sends or receives only encrypted messages over the network.)

References:

1. GRID: MS-00000539

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	14.4 Encrypt All Sensitive Information in Transit Encrypt all sensitive information in transit.		●	●

18.10.90.1.3 Ensure 'Disallow Digest authentication' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to manage whether the Windows Remote Management (WinRM) client will not use Digest authentication.

The recommended state for this setting is: `Enabled`.

Rationale:

Digest authentication is less robust than other authentication methods available in WinRM. A threat actor who is able to capture packets on the network where WinRM is running may be able to determine the credentials used for accessing remote hosts via WinRM.

Impact:

The WinRM client will not use Digest authentication.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\WinRM\Client:AllowDigest
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows Remote Management (WinRM)\WinRM Client\Disallow Digest
authentication
```

Note: This Group Policy path is provided by the Group Policy template `WindowsRemoteManagement.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (The WinRM client will use Digest authentication.)

References:

1. GRID: MS-00000540

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	16.5 Encrypt Transmittal of Username and Authentication Credentials Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.		●	●

18.10.90.2 WinRM Service

This section contains recommendations related to the Windows Remote Management (WinRM) service.

This Group Policy section is provided by the Group Policy template `WindowsRemoteManagement.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.90.2.1 Ensure 'Allow Basic authentication' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to manage whether the Windows Remote Management (WinRM) service accepts Basic authentication from a remote client.

The recommended state for this setting is: `Disabled`.

Rationale:

Basic authentication is less robust than other authentication methods available in WinRM because credentials including passwords are transmitted in plain text. A threat actor who is able to capture packets on the network where WinRM is running may be able to determine the credentials used for accessing remote hosts via WinRM.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\WinRM\Service:AllowBasic
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows Remote Management (WinRM)\WinRM Service\Allow Basic
authentication
```

Note: This Group Policy path is provided by the Group Policy template `WindowsRemoteManagement.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (The WinRM service will not accept Basic authentication from a remote client.)

References:

1. GRID: MS-00000541

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	16.5 Encrypt Transmittal of Username and Authentication Credentials Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.		●	●

18.10.90.2.2 Ensure 'Allow remote server management through WinRM' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting allows you to manage whether the Windows Remote Management (WinRM) service automatically listens on the network for requests on the HTTP transport over the default HTTP port.

The recommended state for this setting is: `Disabled`.

Rationale:

Any feature is a potential avenue of attack, those that enable inbound network connections are particularly risky. Only enable the use of the Windows Remote Management (WinRM) service on trusted networks and when feasible employ additional controls such as IPsec.

Impact:

Remote Management via the WinRM service will not be available.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\WinRM\Service:AllowAutoConfig
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled:`

```
Computer Configuration\Administrative Templates\Windows Components\Windows
Remote Management (WinRM)\WinRM Service\Allow remote server management
through WinRM
```

Note: This Group Policy path is provided by the Group Policy template `WindowsRemoteManagement.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Allow automatic configuration of listeners*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

Default Value:

Server 2012 (non-R2) and newer: Enabled. (The WinRM service automatically listens on the network for requests on the HTTP transport over the default HTTP port.)

Server 2008 R2 and older: Disabled. (The WinRM service is not configured with a listener and will not respond to requests from a remote computer.)

References:

1. GRID: MS-00000542

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.10.90.2.3 Ensure 'Allow unencrypted traffic' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to manage whether the Windows Remote Management (WinRM) service sends and receives unencrypted messages over the network.

The recommended state for this setting is: `Disabled`.

Rationale:

Encrypting WinRM network traffic reduces the risk of a threat actor viewing or modifying WinRM messages as they transit the network.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\WinRM\Service:AllowUnencryptedTraffi
c
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows Remote Management (WinRM)\WinRM Service\Allow unencrypted
traffic
```

Note: This Group Policy path is provided by the Group Policy template `WindowsRemoteManagement.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (The WinRM service sends or receives only encrypted messages over the network.)

References:

1. GRID: MS-00000543

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	14.4 Encrypt All Sensitive Information in Transit Encrypt all sensitive information in transit.		●	●

18.10.90.2.4 Ensure 'Disallow WinRM from storing RunAs credentials' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to manage whether the Windows Remote Management (WinRM) service will allow RunAs credentials to be stored for any plug-ins.

The recommended state for this setting is: `Enabled`.

Note: If you enable and then disable this policy setting, any values that were previously configured for `RunAsPassword` will need to be reset.

Rationale:

Although the ability to store RunAs credentials is a convenient feature it increases the risk of account compromise slightly. For example, if you forget to lock your desktop before leaving it unattended for a few minutes another person could access not only the desktop of your computer but also any hosts you manage via WinRM with cached RunAs credentials.

Impact:

The WinRM service will not allow the `RunAsUser` or `RunAsPassword` configuration values to be set for any plug-ins. If a plug-in has already set the `RunAsUser` and `RunAsPassword` configuration values, the `RunAsPassword` configuration value will be erased from the credential store on the computer.

If this setting is later Disabled again, any values that were previously configured for `RunAsPassword` will need to be reset.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\WinRM\Service:DisableRunAs
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows Remote Management (WinRM)\WinRM Service\Disallow WinRM
from storing RunAs credentials
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WindowsRemoteManagement.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Disabled. (The WinRM service will allow the `RunAsUser` and `RunAsPassword` configuration values to be set for plug-ins and the `RunAsPassword` value will be stored securely.)

References:

1. GRID: MS-00000544

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	14.3 Disable Workstation to Workstation Communication Disable all workstation to workstation communication to limit an attacker's ability to move laterally and compromise neighboring systems, through technologies such as Private VLANs or microsegmentation.		●	●

18.10.91 Windows Remote Shell

This section contains settings related to Windows Remote Shell (WinRS).

This Group Policy section is provided by the Group Policy template `WindowsRemoteShell.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.91.1 Ensure 'Allow Remote Shell Access' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting allows you to manage configuration of remote access to all supported shells to execute scripts and commands.

The recommended state for this setting is: `Disabled`.

Note: The GPME help text for this setting is incorrectly worded, implying that configuring it to `Enabled` will reject new Remote Shell connections, and setting it to `Disabled` will allow Remote Shell connections. The opposite is true (and is consistent with the title of the setting). This is a wording mistake by Microsoft in the Administrative Template.

Rationale:

Any feature is a potential avenue of attack, those that enable inbound network connections are particularly risky. Only enable the use of the Windows Remote Shell on trusted networks and when feasible employ additional controls such as IPsec.

Impact:

New Remote Shell connections are not allowed and are rejected by the server.

Note: On Server 2012 (non-R2) or newer, due to design changes in the OS after Server 2008 R2, configuring this setting as prescribed will prevent the ability to add or remove Roles and Features (even locally) via the GUI. We therefore recommend that the necessary Roles and Features be installed prior to configuring this setting on a Level 2 server. Alternatively, Roles and Features can still be added or removed using the PowerShell commands `Add-WindowsFeature` or `Remove-WindowsFeature` in the Server Manager module, even with this setting configured.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\WinRM\Service\WinRS:AllowRemoteShell
Access
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows Remote Shell\Allow Remote Shell Access
```

Note: This Group Policy path is provided by the Group Policy template `WindowsRemoteShell.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Enabled. (New Remote Shell connections are allowed.)

References:

1. GRID: MS-00000545

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.10.92 Windows Sandbox

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsSandbox.admx/adml` that is included with the Microsoft Windows 11 version 21H2 Administrative Templates (or newer).

18.10.93 Windows Security (formerly Windows Defender Security Center)

This section contains recommendations related to the Windows Security Center console settings.

This Group Policy section is provided by the Group Policy template `WindowsDefenderSecurityCenter.admx/adml` that is included with the Microsoft Windows 10 version 1709 Administrative Templates (or newer).

Note: This section was originally named *Windows Defender Security Center* but was renamed by Microsoft to *Windows Security* starting with the Microsoft Windows 10 version 1809 & Server 2019 Administrative Templates.

18.10.93.1 Account protection

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsDefenderSecurityCenter.admx/adml` that is included with the Microsoft Windows 10 version 1803 Administrative Templates (or newer).

18.10.93.2 App and browser protection

This section contains App and browser protection settings.

This Group Policy section is provided by the Group Policy template `WindowsDefenderSecurityCenter.admx/adml` that is included with the Microsoft Windows 10 version 1709 Administrative Templates (or newer).

18.10.93.2.1 Ensure 'Prevent users from modifying settings' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting prevent users from making changes to the Exploit protection settings area in the Windows Security settings.

The recommended state for this setting is: `Enabled`.

Rationale:

Only authorized IT staff should be able to make changes to the exploit protection settings in order to ensure the organizations specific configuration is not modified.

Impact:

Local users cannot make changes in the Exploit protection settings area.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender Security Center\App and
Browser protection:DisallowExploitProtectionOverride
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows Security\App and browser protection\Prevent users from
modifying settings
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WindowsDefenderSecurityCenter.admx/adml` that is included with the Microsoft Windows 10 version 1709 Administrative Templates (or newer).

Default Value:

Disabled. (Local users are allowed to make changes in the Exploit protection settings area.)

References:

1. GRID: MS-00000548

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

18.10.94 Windows Update

This section contains recommendations related to Windows Update.

This Group Policy section is provided by the Group Policy template `WindowsUpdate.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.94.1 Legacy Policies

This section contains recommendations related to legacy Windows Update policies.

This Group Policy section is provided by the Group Policy template `WindowsUpdate.admx/adml` that is included with the Microsoft Windows 11 version 21H2 Administrative Templates (or newer).

18.10.94.1.1 Ensure 'No auto-restart with logged on users for scheduled automatic updates installations' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting specifies that Automatic Updates will wait for computers to be restarted by the users who are logged on to them to complete a scheduled installation.

The recommended state for this setting is: `Disabled`.

Note: This setting applies only when you configure Automatic Updates to perform scheduled update installations. If you configure the Configure Automatic Updates setting to Disabled, this setting has no effect.

Rationale:

Some security updates require that the computer be restarted to complete an installation. If the computer cannot restart automatically, then the most recent update will not completely install and no new updates will download to the computer until it is restarted. Without the auto-restart functionality, users who are not security-conscious may choose to indefinitely delay the restart, therefore keeping the computer in a less secure state.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU:NoAutoRebootWithLoggedOnUsers
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows Update\Legacy Policies\No auto-restart with logged on
users for scheduled automatic updates installations
```

Note: This Group Policy path is provided by the Group Policy template `WindowsUpdate.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *No auto-restart for scheduled Automatic Updates installations*, but it was renamed starting with the Windows 7 & Server 2008 R2 Administrative Templates.

Default Value:

Disabled. (Automatic Updates will notify the user that the computer will automatically restart in 5 minutes to complete the installation of security updates.)

References:

1. GRID: MS-00000549

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.3 Perform Automated Operating System Patch Management Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v7	3.4 Deploy Automated Operating System Patch Management Tools Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.	●	●	●

18.10.94.2 Manage end user experience

This section contains recommendations related to managing Windows Update end user experience.

This Group Policy section is provided by the Group Policy template `WindowsUpdate.admx/adml` that is included with the Microsoft Windows 11 version 21H2 Administrative Templates (or newer).

18.10.94.2.1 Ensure 'Configure Automatic Updates' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting specifies whether computers in your environment will receive security updates from Windows Update or WSUS. If you configure this policy setting to Enabled, the operating system will recognize when a network connection is available and then use the network connection to search Windows Update or your designated intranet site for updates that apply to them.

After you configure this policy setting to Enabled, select one of the following four options in the Configure Automatic Updates Properties dialog box to specify how the service will work:

- 2 - Notify for download and auto install *(Notify before downloading any updates)*
- 3 - Auto download and notify for install *(Download the updates automatically and notify when they are ready to be installed.) (Default setting)*
- 4 - Auto download and schedule the install *(Automatically download updates and install them on the schedule specified below.))*
- 5 - Allow local admin to choose setting *(Leave decision on above choices up to the local Administrators (Not Recommended))*

The recommended state for this setting is: `Enabled`.

Note: The sub-setting "*Configure automatic updating:*" has 4 possible values – all of them are valid depending on specific organizational needs, however if feasible we suggest using a value of `4 - Auto download and schedule the install`. This suggestion is not a scored requirement.

Note #2: Organizations that utilize a third-party solution for patching may choose to exempt themselves from this recommendation, and instead configure it to `Disabled` so that the native Windows Update mechanism does not interfere with the third-party patching process.

Rationale:

Although each version of Windows is thoroughly tested before release, it is possible that problems will be discovered after the products are shipped. The Configure Automatic Updates setting can help you ensure that the computers in your environment will always have the most recent critical operating system updates and service packs installed.

Impact:

Critical operating system updates and service packs will be installed as necessary.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU:NoAutoUpdate
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows Update\Manage end user experience\Configure Automatic
Updates
```

Note: This Group Policy path is provided by the Group Policy template `WindowsUpdate.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Enabled: 3 - Auto download and notify for install. (Windows finds updates that apply to the computer and downloads them in the background (the user is not notified or interrupted during this process). When the downloads are complete, users will be notified that they are ready to install. After going to Windows Update, users can install them.)

References:

1. GRID: MS-00000550

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.3 Perform Automated Operating System Patch Management Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v7	3.4 Deploy Automated Operating System Patch Management Tools Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.	●	●	●

18.10.94.2.2 Ensure 'Configure Automatic Updates: Scheduled install day' is set to '0 - Every day' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting specifies when computers in your environment will receive security updates from Windows Update or WSUS.

The recommended state for this setting is: `0 - Every day`.

Note: This setting is only applicable if `4 - Auto download and schedule the install` is selected in recommendation 'Configure Automatic Updates'. It will have no impact if any other option is selected.

Rationale:

Although each version of Windows is thoroughly tested before release, it is possible that problems will be discovered after the products are shipped. The Configure Automatic Updates setting can help you ensure that the computers in your environment will always have the most recent critical operating system updates and service packs installed.

Impact:

If `4 - Auto download and schedule the install` is selected in recommendation 'Configure Automatic Updates', critical operating system updates and service packs will automatically download every day (at 3:00 A.M., by default).

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU:ScheduledInstallDay
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `0 - Every day`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows Update\Manage end user experience\Configure Automatic
Updates: Scheduled install day
```

Note: This Group Policy path is provided by the Group Policy template `WindowsUpdate.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Not Defined. (Since the default value of Configure Automatic Updates is `3 - Auto download and notify for install`, this setting is not applicable by default.)

References:

1. GRID: MS-00000551

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.3 Perform Automated Operating System Patch Management Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v7	3.4 Deploy Automated Operating System Patch Management Tools Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.	●	●	●

18.10.94.3 Manage updates offered from Windows Server Update Service

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsUpdate.admx/adml` that is included with the Microsoft Windows 11 version 21H2 Administrative Templates (or newer).

18.10.94.4 Manage updates offered from Windows Update (formerly Defer Windows Updates and Windows Update for Business)

This section contains recommendations related to managing which updates are offered from Windows Update, and when.

This Group Policy section is provided by the Group Policy template `WindowsUpdate.admx/adml` that is included with the Microsoft Windows 10 version 1607 & Server 2016 Administrative Templates (or newer).

Note: This section was initially named *Defer Windows Updates* but was renamed by Microsoft to *Windows Update for Business* starting with the Microsoft Windows 10 version 1709 Administrative Templates. It was renamed (again) to *Manage updates offered from Windows Update* starting with the Microsoft Windows 11 version 21H2 Administrative Templates.

18.10.94.4.1 Ensure 'Manage preview builds' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting manages which updates that are received prior to the update being released.

Dev Channel: Ideal for highly technical users. Insiders in the Dev Channel will receive builds from our active development branch that is earliest in a development cycle. These builds are not matched to a specific Windows 10 release.

Beta Channel: Ideal for feature explorers who want to see upcoming Windows 10 features. Your feedback will be especially important here as it will help our engineers ensure key issues are fixed before a major release.

Release Preview Channel (default): Insiders in the Release Preview Channel will have access to the upcoming release of Windows 10 prior to it being released to the world. These builds are supported by Microsoft. The Release Preview Channel is where we recommend companies preview and validate upcoming Windows 10 releases before broad deployment within their organization.

The recommended state for this setting is: `Disabled`.

Note: Preview Build enrollment requires a telemetry level setting of 2 or higher and your domain registered on insider.windows.com. For additional information on Preview Builds, see: Managing preview builds across your organization - Windows Insider Program | Microsoft Learn.

Rationale:

It can be risky for experimental features to be allowed in an enterprise managed environment because this can introduce bugs and security holes into systems, making it easier for a threat actor to gain access. It is generally preferred to only use production-ready builds.

Impact:

Preview builds are prevented from installing on the device.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate:ManagePreviewBuildsPol
icyValue
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows Update\Manage updates offered from Windows Update\Manage
preview builds
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WindowsUpdate.admx/adml` that is included with the Microsoft Windows 10 version 1709 Administrative Templates (or newer).

Default Value:

Disabled. (Windows Update will not offer you any pre-release updates and you will receive such content once released to the world. Disabling this policy will cause any devices currently on a pre-release build to opt out and stay on the latest Feature Update once released.)

References:

1. https://docs.microsoft.com/en-us/windows-insider/business/manage-builds
2. GRID: MS-00000553

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.5 Allowlist Authorized Software Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.		●	●
v7	2.6 Address unapproved software Ensure that unauthorized software is either removed or the inventory is updated in a timely manner	●	●	●

18.10.94.4.2 Ensure 'Select when Quality Updates are received' is set to 'Enabled: 0 days' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This settings controls when Quality Updates are received.

The recommended state for this setting is: `Enabled: 0 days`.

Note: If the "Allow Diagnostic Data" (formerly "Allow Telemetry") policy is set to 0, this policy will have no effect.

Note #2: Starting with Windows Server 2016 RTM (version 1607), Microsoft introduced a new Windows Update (WU) client behavior called **Dual Scan**, with an eye to cloud-based update management. In some cases, this Dual Scan feature can interfere with Windows Updates from Windows Server Update Services (WSUS) and/or manual WU updates. If you are using WSUS in your environment, you may need to set the above setting to `Not Configured` *or* configure the setting *Do not allow update deferral policies to cause scans against Windows Update* (added in the Windows 10 version 1709 Administrative Templates) in order to prevent the Dual Scan feature from interfering. More information on Dual Scan is available at these links:

- Demystifying “Dual Scan” – WSUS Product Team Blog
- Improving Dual Scan on 1607 – WSUS Product Team Blog

Rationale:

Quality Updates can contain important bug fixes and/or security patches, and should be installed as soon as possible.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1` (DeferQualityUpdates) and `0` (DeferQualityUpdatesPeriodInDays).

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate:DeferQua
lityUpdates
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate:DeferQua
lityUpdatesPeriodInDays
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled:0 days`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Windows Update\Manage updates offered from Windows Update\Select
when Quality Updates are received
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WindowsUpdate.admx/adml` that is included with the Microsoft Windows 10 version 1607 & Server 2016 Administrative Templates (or newer).

Default Value:

Enabled: 0 days. (Install new Quality Updates as soon as they are available.)

References:

1. GRID: MS-00000555

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.3 Perform Automated Operating System Patch Management Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v7	3.4 Deploy Automated Operating System Patch Management Tools Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.	●	●	●
v7	3.5 Deploy Automated Software Patch Management Tools Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.	●	●	●

18.11 Custom Settings

This section contains recommendations for CIS Custom Settings. The recommendations in this section can be set through Group Policy using the `CIS.admx/adml` custom template. These templates are found with the CIS Build Kits published after January 2026.

18.11.1 Ensure 'Disable HTTP proxy features: Disable WPAD' is set to 'Enabled: Checked' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether Web Proxy Auto-Discovery protocol (WPAD) is disabled on the system. WPAD is used to discover Proxy Auto-Config (PAC) files from the local network.

The recommended state for this setting is: `Enabled: Checked`.

Note: When this recommendation is set as prescribed, applications can still resolve the name `WPAD` by calling Domain Name System (DNS) directly.

Rationale:

WPAD could expose the system to Man-In-The-Middle (MITM) attacks. If an organization depends on HTTP proxy configuration, it is recommended that other client configuration mechanisms be used instead, such as Group Policy.

Impact:

After WPAD is disabled, all proxies must be manually configured. The registry key created by this recommendation stops WPAD detection for all proxy detection calls made through the Windows HTTP Services (WinHTTP) application programming interface (API).

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet
Settings\WinHttp:DisableWpad
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Checked`:

```
Computer Configuration\Policies\Administrative Templates\Center for Internet Security (CIS)\Additional Benchmark Settings\Disable HTTP proxy features: Disable WPAD
```

Note: This Group Policy path is **NOT** provided by Microsoft. The Group Policy template `CIS.admx/adml` is included with the CIS Microsoft Windows Build Kits published after January 2026.

Default Value:

Enabled.

References:

1. https://learn.microsoft.com/en-us/troubleshoot/windows-server/networking/disable-http-proxy-auth-features
2. GRID: MS-00000637

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.11.2 Ensure 'Disable HTTP proxy features: Disable proxy authentication' is set to 'Enabled: Disable authentication over loopback interfaces' or higher (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether Windows can authenticate over a loopback interface.

The recommended state for this setting is: `Enabled: Disable authentication over loopback interfaces`. Configuring this setting to `Disable all authentication protocols and loopback authentication` also conforms to the benchmark.

Rationale:

It is best to limit the sign-in interface to only known and trusted services, so malicious actors can't impersonate them.

Impact:

Windows will not be able to authenticate over a loopback interface

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `256` or `287`.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet
Settings:DisableProxyAuthenticationSchemes
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Disable authentication over loopback interfaces` or `Disable all authentication protocols and loopback authentication`:

```
Computer Configuration\Policies\Administrative Templates\Center for Internet
Security (CIS)\Additional Benchmark Settings\Disable HTTP proxy features:
Disable proxy authentication
```

Note: This Group Policy path is **NOT** provided by Microsoft. The Group Policy template `CIS.admx/adml` is included with the CIS Microsoft Windows Build Kits published after January 2026.

Default Value:

Enabled.

References:

1. https://learn.microsoft.com/en-us/troubleshoot/windows-server/networking/disable-http-proxy-auth-features
2. GRID: MS-00000638

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

19 Administrative Templates (User)

This section contains recommendations for user-based settings that are present within the Administrative Templates (ADMX) for domain-joined user configurations. The settings included in this section are intended to harden the system and are applied on a per-user basis, reflected to each domain-joined interactive user's **HKEY_CURRENT_USER (HKCU)** registry hive. Each interactively logged-on user has its own **HKCU** hive, which is a context-sensitive, per-user, symbolic link to a subkey under **HKEY_USERS (HKU)**, where the user's Security Identifier (SID) is the subkey name (Ex: `HKU\S-1-5-21-123123123-123123123-1231231231-12312`). User SIDs for this scenario always begin with `S-1-5-21-*` for active directory domain-joined accounts.

The group policy engine applies user configuration settings to the **HKU***SID* subkeys for interactive logons, including local console logons, remote desktop logons, and RunAs logons. User configuration settings are not applied to the built-in **NT AUTHORITY** service accounts (System, Network Service, and Local Service), nor to any other service logons. User configuration settings configured through active directory domain group policy objects (GPO) are not applied to local user accounts.

When validating user configuration settings for compliance, each recommendation should be checked against all currently-logged-on interactive users' hives:

- Audit all **HKEY_USERS** subkeys with key names beginning with `S-1-5-21-*` and do not end with **_Classes**.
- Do not audit subkeys named `.DEFAULT`, `S-1-5-18`, `S-1-5-19`, or `S-1-5-20`.
- Do not audit any **NT SERVICE** SIDs (`S-1-5-80-`).
- Do not load the hives of users that are not currently logged on (**NTUSER.DAT** files) as part of compliance verification.

A user configuration setting is considered in compliance if the correct configuration is found in all applicable user hives as described above. If there are multiple users logged on and the setting is correctly configured in some but not all the applicable user hives, the recommendation is not in full compliance.

If a system has no actively logged-on users, the recommendations in this section are not considered out of compliance. User accounts (`S-1-5-21-*`) that only log on as a service (service accounts), will not receive user configuration settings to its **HKU** registry hive since the group policy engine will not write to this type of account. Compliance findings for these accounts should be ignored.

Why CIS recommends not auditing all the **HKU** subkeys:

- Group policy applies user configuration settings only to **HKU** subkey hives associated with interactive logons. It never applies the settings to the **NT AUTHORITY** service account subkeys (`S-1-5-18`, `S-1-5-19`, `S-1-5-20`, or `.DEFAULT`) or the **NT SERVICE** subkeys (`S-1-5-80-*`).
    - The `HKU\S-1-5-18` is a symbolic link to **HKU\.DEFAULT**, so the key content is identical.
- The **HKU***SID***_Classes** subkey represents the subkey of the corresponding **HKU***SID***\SOFTWARE\Classes**, to which they are symbolically linked.

Why CIS recommends not loading the **NTUSER.DAT** file(s) to audit the hives of users that are not currently logged on:

- Unnecessary false positives of old user profiles that were last loaded before the new or updated GPO containing the user configuration settings were applied.
    - These accounts would be found out of compliance, with no supportable way to bring them into compliance other than the user logging on or deleting the old profiles.
    - These account settings being out of compliance should not cause issues if the user never logs on; and if they do, a group policy update should bring them into compliance.
- Risk of system issues if the user logs on while the scanning tool has the hive loaded, and then also when the scanning tool unloads the hive.
- Significant performance hit.

User configuration settings configured through active directory domain GPOs are not applied to local user accounts. Since these accounts begin with the SID `S-1-5-21-*`, a failure may occur with CIS-CAT and other third-party assessment tools. To mitigate this, user recommendations (Section 19 of this benchmark) should be applied to local accounts separately. If this is not a concern for the organization, local accounts should be ignored. The above is also true when an account with a `S-1-5-21-*` SID logs on as a service.

19.1 Control Panel

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.2 Desktop

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.3 Network

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.4 Shared Folders

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `SharedFolders.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.5 Start Menu and Taskbar

This section contains recommendations for Start Menu and Taskbar settings.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.5.1 Notifications

This section contains recommendations for Notification settings.

This Group Policy section is provided by the Group Policy template `WPN.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

19.5.1.1 Ensure 'Turn off toast notifications on the lock screen' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting turns off toast notifications on the lock screen.

The recommended state for this setting is `Enabled`.

Rationale:

While this feature can be handy for users, applications that provide toast notifications might display sensitive personal or business data while the device is left unattended.

Impact:

Applications will not be able to raise toast notifications on the lock screen.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKU\[USER
SID]\Software\Policies\Microsoft\Windows\CurrentVersion\PushNotifications:NoT
oastApplicationNotificationOnLockScreen
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
User Configuration\Policies\Administrative Templates\Start Menu and
Taskbar\Notifications\Turn off toast notifications on the lock screen
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WPN.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Disabled. (Toast notifications on the lock screen are enabled and can be turned off by the administrator or user.)

References:

1. GRID: MS-00000557

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

19.6 System

This section contains recommendations for System settings.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.6.1 Ctrl+Alt+Del Options

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `CtrlAltDel.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.6.2 Display

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Display.admx/adml` that is included with the Microsoft Windows 10 version 1803 Administrative Templates (or newer).

19.6.3 Driver Installation

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `DeviceInstallation.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.6.4 Folder Redirection

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `FolderRedirection.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.6.5 Group Policy

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `GroupPolicy.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.6.6 Internet Communication Management

This section contains recommendations related to Internet Communication Management.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.6.6.1 Internet Communication settings

This section contains recommendations related to Internet Communication settings.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.6.6.1.1 Ensure 'Turn off Help Experience Improvement Program' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting specifies whether users can participate in the Help Experience Improvement program. The Help Experience Improvement program collects information about how customers use Windows Help so that Microsoft can improve it.

The recommended state for this setting is: `Enabled`.

Rationale:

Large enterprise managed environments may not want to have information collected by Microsoft from managed client computers.

Impact:

Users cannot participate in the Help Experience Improvement program.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKU\[USER SID]\Software\Policies\Microsoft\Assistance\Client\1.0:NoImplicitFeedback
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled:`

```
User Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication Settings\Turn off Help Experience Improvement Program
```

Note: This Group Policy path is provided by the Group Policy template `HelpAndSupport.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Users can turn on the Help Experience Improvement program feature from the Help and Support settings page.)

References:

1. GRID: MS-00000558

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

19.6.7 Keyboard Filter

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `KeyboardFilterPolicy.admx/adml` that is included with the Microsoft Windows 11 version 25H2 Administrative Templates (or newer).

19.7 Windows Components

This section contains recommendations for Windows Component settings.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.1 Account Notifications

This section contains recommendations for Account Notifications settings.

This Group Policy section is provided by the Group Policy template `AccountNotifications.admx/adml` that is included with the Microsoft Windows 11 version 22H2 Administrative Templates v3.0 (or newer).

19.7.2 Add features to Windows 8 / 8.1 / 10 (formerly Windows Anytime Upgrade)

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsAnytimeUpgrade.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Note: This section was initially named *Windows Anytime Upgrade* but was renamed by Microsoft to *Add features to Windows x* starting with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

19.7.3 App runtime

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `AppXRuntime.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

19.7.4 Application Compatibility

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `AppCompat.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.5 Attachment Manager

This section contains recommendations related to Attachment Manager.

This Group Policy section is provided by the Group Policy template `AttachmentManager.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.5.1 Ensure 'Do not preserve zone information in file attachments' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to manage whether Windows marks file attachments with information about their zone of origin (such as restricted, Internet, intranet, local). This requires NTFS in order to function correctly, and will fail without notice on FAT32. By not preserving the zone information, Windows cannot make proper risk assessments.

The recommended state for this setting is: `Disabled`.

Note: The Attachment Manager feature warns users when opening or executing files which are marked as being from an untrusted source, unless/until the file's zone information has been removed via the "Unblock" button on the file's properties or via a separate tool such as Microsoft Sysinternals Streams.

Rationale:

A file that is downloaded from a computer in the Internet or Restricted Sites zone may be moved to a location that makes it appear safe, like an intranet file share, and executed by an unsuspecting user. The Attachment Manager feature will warn users when opening or executing files which are marked as being from an untrusted source, unless/until the file's zone information has been removed.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `2`.

```
HKU\[USER SID]\Software\Microsoft\Windows\CurrentVersion\Policies\Attachments:SaveZoneInformation
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
User Configuration\Policies\Administrative Templates\Windows
Components\Attachment Manager\Do not preserve zone information in file
attachments
```

Note: This Group Policy path is provided by the Group Policy template `AttachmentManager.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Windows marks file attachments with their zone information.)

References:

1. GRID: MS-00000559

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

19.7.5.2 Ensure 'Notify antivirus programs when opening attachments' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting manages the behavior for notifying registered antivirus programs. If multiple programs are registered, they will all be notified.

The recommended state for this setting is: `Enabled`.

Note: An updated antivirus program must be installed for this policy setting to function properly.

Rationale:

Antivirus programs that do not perform on-access checks may not be able to scan downloaded files.

Impact:

Windows tells the registered antivirus program(s) to scan the file when a user opens a file attachment. If the antivirus program fails, the attachment is blocked from being opened.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `3`.

```
HKU\[USER
SID]\Software\Microsoft\Windows\CurrentVersion\Policies\Attachments:ScanWithA
ntiVirus
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
User Configuration\Policies\Administrative Templates\Windows
Components\Attachment Manager\Notify antivirus programs when opening
attachments
```

Note: This Group Policy path is provided by the Group Policy template `AttachmentManager.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Windows does not call the registered antivirus program(s) when file attachments are opened.)

References:

1. GRID: MS-00000560

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v7	8.1 Utilize Centrally Managed Anti-malware Software Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.		●	●

19.7.6 AutoPlay Policies

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `AutoPlay.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.7 Calculator

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Programs.admx/adml` that is included with the Microsoft Windows 10 version 2004 Administrative Templates (or newer).

19.7.8 Cloud Content

This section contains recommendations for Cloud Content.

This Group Policy section is provided by the Group Policy template `CloudContent.admx/adml` that is included with the Microsoft Windows 10 version 1607 & Server 2016 Administrative Templates (or newer).

19.7.8.1 Ensure 'Configure Windows spotlight on lock screen' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting lets you configure Windows Spotlight on the lock screen.

The recommended state for this setting is: `Disabled`.

Note: Per Microsoft TechNet, this policy setting only applies to Windows 10 Enterprise and Windows 10 Education editions.

Rationale:

Enabling this setting will help ensure your data is not shared with any third party. The Windows Spotlight feature collects data and uses that data to display suggested apps as well as images from the internet.

Impact:

Windows Spotlight will be turned off and users will no longer be able to select it as their lock screen.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `2`.

```
HKU\[USER
SID]\Software\Policies\Microsoft\Windows\CloudContent:ConfigureWindowsSpotlig
ht
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
User Configuration\Policies\Administrative Templates\Windows Components\Cloud
Content\Configure Windows spotlight on lock screen
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `CloudContent.admx/adml` that is included with the Microsoft Windows 10 version 1607 & Server 2016 Administrative Templates (or newer).

Default Value:

Enabled. (Windows Spotlight is set as the lock screen provider.)

References:

1. GRID: MS-00000561

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

19.7.8.2 Ensure 'Do not suggest third-party content in Windows spotlight' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether Windows will suggest apps and content from third-party software publishers.

The recommended state for this setting is: `Enabled`.

Rationale:

Enabling this setting will help ensure your data is not shared with any third party. The Windows Spotlight feature collects data and uses that data to display suggested apps as well as images from the internet.

Impact:

Windows Spotlight on lock screen, Windows tips, Microsoft consumer features and other related features will no longer suggest apps and content from third-party software publishers. Users may still see suggestions and tips to make them more productive with Microsoft features and apps.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKU\[USER SID]\Software\Policies\Microsoft\Windows\CloudContent:DisableThirdPartySuggestions
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
User Configuration\Policies\Administrative Templates\Windows Components\Cloud Content\Do not suggest third-party content in Windows spotlight
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `CloudContent.admx/adml` that is included with the Microsoft Windows 10 version 1607 & Server 2016 Administrative Templates (or newer).

Default Value:

Disabled. (Apps and content from third-party software publishers will be suggested in addition to Microsoft apps and content.)

References:

1. GRID: MS-00000562

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

19.7.8.3 Ensure 'Do not use diagnostic data for tailored experiences' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This setting determines if Windows can use diagnostic data to provide tailored experiences to the user.

The recommended state for this setting is: `Enabled`.

Rationale:

Tracking, collection and utilization of personalized data is a privacy and security issue that is of concern to many organizations.

Impact:

Windows will not use diagnostic data from this device (this data may include browser, app and feature usage, depending on the "Diagnostic and usage data" setting value) to customize content shown on the lock screen, Windows tips, Microsoft consumer features and other related features. If these features are enabled, users will still see recommendations, tips and offers, but they may be less personalized.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKU\[USER SID]\Software\Policies\Microsoft\Windows\CloudContent:DisableTailoredExperiencesWithDiagnosticData
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
User Configuration\Policies\Administrative Templates\Windows Components\Cloud Content\Do not use diagnostic data for tailored experiences
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `CloudContent.admx/adml` that is included with the Microsoft Windows 10 version 1703 Administrative Templates (or newer).

Default Value:

Disabled. (Microsoft will use diagnostic data to provide personalized recommendations, tips and offers.)

References:

1. GRID: MS-00000563

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

19.7.8.4 Ensure 'Turn off all Windows spotlight features' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This policy setting lets you turn off all Windows Spotlight features at once.

The recommended state for this setting is: `Enabled`.

Note: Per Microsoft TechNet, this policy setting only applies to Windows 10 Enterprise and Windows 10 Education editions.

Rationale:

Enabling this setting will help ensure your data is not shared with any third party. The Windows Spotlight feature collects data and uses that data to display suggested apps as well as images from the internet.

Impact:

Windows Spotlight on lock screen, Windows tips, Microsoft consumer features and other related features will be turned off.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKU\[USER
SID]\Software\Policies\Microsoft\Windows\CloudContent:DisableWindowsSpotlight
Features
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
User Configuration\Policies\Administrative Templates\Windows Components\Cloud
Content\Turn off all Windows spotlight features
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `CloudContent.admx/adml` that is included with the Microsoft Windows 10 version 1607 & Server 2016 Administrative Templates (or newer).

Default Value:

Disabled. (Windows Spotlight features are allowed.)

References:

1. GRID: MS-00000564

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

19.7.8.5 Ensure 'Turn off Spotlight collection on Desktop' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting removes the Spotlight collection setting in Personalization, rendering the user unable to select and subsequently download daily images from Microsoft to the system desktop.

The recommended state for this setting is: `Enabled`.

Rationale:

Enabling this setting will help ensure your data is not shared with any third party. The Windows Spotlight feature collects data and uses that data to display images from Microsoft.

Impact:

The `Spotlight collection` feature will not be available as an option in Personalization settings, so users will not be able to download daily images from Microsoft.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKU\[USER SID]\SOFTWARE\Policies\Microsoft\Windows\CloudContent:DisableSpotlightCollectionOnDesktop
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
User Configuration\Policies\Administrative Templates\Windows Components\Cloud Content\Turn off Spotlight collection on Desktop
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `CloudContent.admx/adml` that is included with the Microsoft Windows 11 version 21H2 Administrative Templates (or newer).

Default Value:

Disabled. (`Spotlight collection` will appear as an option in Personalization settings, allowing the user to select `Spotlight collection` as the Desktop provider and display daily images from Microsoft on the desktop.)

References:

1. https://docs.microsoft.com/en-us/windows/configuration/windows-spotlight
2. GRID: MS-00000565

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

19.7.9 Credential User Interface

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `CredUI.admx/adml` that is included with the Microsoft Windows 10 version 1607 & Server 2016 Administrative Templates (or newer).

19.7.10 Data Collection and Preview Builds

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `DataCollection.admx/adml` that is included with the Microsoft Windows 10 version 1607 & Server 2016 Administrative Templates (or newer).

19.7.11 Desktop Gadgets

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Sidebar.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

19.7.12 Desktop Window Manager

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `DWM.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.13 Digital Locker

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `DigitalLocker.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.14 Edge UI

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `EdgeUI.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

19.7.15 File Explorer (formerly Windows Explorer)

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note: This section was initially named *Windows Explorer* but was renamed by Microsoft to *File Explorer* starting with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

19.7.16 File Revocation

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `FileRevocation.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

19.7.17 IME

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `EAIME.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

19.7.18 Instant Search

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WordWheel.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.19 Internet Explorer

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `InetRes.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.20 Location and Sensors

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Sensors.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

19.7.21 Microsoft Edge

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `MicrosoftEdge.admx/adml` that is included with the Microsoft Windows 10 RTM (version 1507) Administrative Templates (or newer).

19.7.22 Microsoft Management Console

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `MMC.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.23 Microsoft User Experience Virtualization

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `UserExperienceVirtualization.admx/adml` that is included with the Microsoft Windows 10 version 1607 & Server 2016 Administrative Templates (or newer).

19.7.24 Multitasking

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Multitasking.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.25 NetMeeting

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Conf.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.26 Network Sharing

This section contains recommendations related to Network Sharing.

This Group Policy section is provided by the Group Policy template `Sharing.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.26.1 Ensure 'Prevent users from sharing files within their profile.' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines whether users can share files within their profile. By default, users are allowed to share files within their profile to other users on their network after an administrator opts in the computer. An administrator can opt in the computer by using the sharing wizard to share a file within their profile.

The recommended state for this setting is: `Enabled`.

Rationale:

If not properly configured, a user could accidentally share sensitive data with unauthorized users. In an enterprise managed environment, the company should provide a managed location for file sharing, such as a file server or SharePoint, instead of the user sharing files directly from their own user profile.

Impact:

Users cannot share files within their profile using the sharing wizard. Also, the sharing wizard cannot create a share at `%root%\Users` and can only be used to create SMB shares on folders.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKU\[USER
SID]\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer:NoInplaceSha
ring
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled:`

```
User Configuration\Policies\Administrative Templates\Windows
Components\Network Sharing\Prevent users from sharing files within their
profile.
```

Note: This Group Policy path is provided by the Group Policy template `Sharing.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Users can share files out of their user profile after an administrator has opted in the computer.)

References:

1. GRID: MS-00000566

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

19.7.27 OOBE

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `OOBE.admx/adml` that is included with the Microsoft Windows 10 version 1809 and Server 2019 Administrative Templates (or newer).

19.7.28 Presentation Settings

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `MobilePCPresentationSettings.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.29 Remote Desktop Services (formerly Terminal Services)

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note: This section was initially named *Terminal Services* but was renamed by Microsoft to *Remote Desktop Services* starting with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates.

19.7.30 RSS Feeds

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `InetRes.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.31 Search

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Search.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

19.7.32 Snipping Tool

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Programs.admx/adml` that is included with the Microsoft Windows 11 version 23H2 v2.0 Administrative Templates (or newer).

19.7.33 Sound Recorder

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `SoundRec.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.34 Store

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WinStoreUI.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates and Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates, or by the Group Policy template `WindowsStore.admx/adml` that is included with the Microsoft Windows 10 version 1511 Administrative Templates (or newer).

19.7.35 Tablet PC

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.36 Task Scheduler

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `TaskScheduler.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.37 Windows AI

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsCopilot.admx/adml` that is included with the Microsoft Windows 11 version 24H2 Administrative Templates (or newer).

19.7.38 Windows Calendar

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WinCal.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.39 Windows Color System

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsColorSystem.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.40 Windows Copilot

This section contains recommendations for Windows Copilot settings.

This Group Policy section is provided by the Group Policy template `WindowsCopilot.admx/adml` that is included with the Microsoft Windows 11 version 23H2 Administrative Templates (or newer).

19.7.41 Windows Defender SmartScreen

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `SmartScreen.admx/adml` that is included with the Microsoft Windows 10 version 1703 Administrative Templates (or newer).

19.7.42 Windows Error Reporting

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `ErrorReporting.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.43 Windows Hello for Business (formerly Microsoft Passport for Work)

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Passport.admx/adml` that is included with the Microsoft Windows 10 RTM (version 1507) Administrative Templates (or newer).

Note: This section was initially named *Microsoft Passport for Work* but was renamed by Microsoft to *Windows Hello for Business* starting with the Microsoft Windows 10 version 1607 & Server 2016 Administrative Templates.

19.7.44 Windows Installer

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `MSI.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.45 Windows Logon Options

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WinLogon.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.46 Windows Media Player

This section contains recommendations related to Windows Media Player.

This Group Policy section is provided by the Group Policy template `WindowsMediaPlayer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.46.1 Networking

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsMediaPlayer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.46.2 Playback

This section contains recommendations related to Windows Media Player playback.

This Group Policy section is provided by the Group Policy template `WindowsMediaPlayer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.46.2.1 Ensure 'Prevent Codec Download' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 - Domain Controller
- Level 2 - Member Server

Description:

This setting controls whether Windows Media Player is allowed to download additional codecs for decoding media files it does not already understand.

The recommended state for this setting is: `Enabled`.

Rationale:

This has some potential for risk if a malicious data file is opened in Media Player that requires an additional codec to be installed. If a special codec is required for a necessary job function, then that codec should first be tested to ensure it is legitimate, and it should be supplied by the IT department in the organization.

Impact:

Windows Media Player is prevented from automatically downloading codecs to your computer. In addition, the *Download codecs automatically* check box on the Player tab in the Player is not available.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `1`.

```
HKU\[USER
SID]\Software\Policies\Microsoft\WindowsMediaPlayer:PreventCodecDownload
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled:`

```
User Configuration\Policies\Administrative Templates\Windows
Components\Windows Media Player\Playback\Prevent Codec Download
```

Note: This Group Policy path is provided by the Group Policy template `WindowsMediaPlayer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Users can change the setting for the *Download codecs automatically* check box.

References:

1. GRID: MS-00000569

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**Account Policies**		
1.1	**Password Policy**		
1.1.1	Ensure 'Enforce password history' is set to '24 or more password(s)' (Automated)	☐	☐
1.1.2	Ensure 'Maximum password age' is set to '365 or fewer days, but not 0' (Automated)	☐	☐
1.1.3	Ensure 'Minimum password age' is set to '1 or more day(s)' (Automated)	☐	☐
1.1.4	Ensure 'Minimum password length' is set to '14 or more character(s)' (Automated)	☐	☐
1.1.5	Ensure 'Password must meet complexity requirements' is set to 'Enabled' (Automated)	☐	☐
1.1.6	Ensure 'Relax minimum password length limits' is set to 'Enabled' (Automated)	☐	☐
1.1.7	Ensure 'Store passwords using reversible encryption' is set to 'Disabled' (Automated)	☐	☐
1.2	**Account Lockout Policy**		
1.2.1	Ensure 'Account lockout duration' is set to '15 or more minute(s)' (Automated)	☐	☐
1.2.2	Ensure 'Account lockout threshold' is set to '5 or fewer invalid logon attempt(s), but not 0' (Automated)	☐	☐
1.2.3	Ensure 'Allow Administrator account lockout' is set to 'Enabled' (MS only) (Manual)	☐	☐
1.2.4	Ensure 'Reset account lockout counter after' is set to '15 or more minute(s)' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2	**Local Policies**		
2.1	**Audit Policy**		
2.2	**User Rights Assignment**		
2.2.1	Ensure 'Access Credential Manager as a trusted caller' is set to 'No One' (Automated)	☐	☐
2.2.2	Ensure 'Access this computer from the network' is set to 'Administrators, Authenticated Users, ENTERPRISE DOMAIN CONTROLLERS' (DC only) (Automated)	☐	☐
2.2.3	Ensure 'Access this computer from the network' is set to 'Administrators, Authenticated Users' (MS only) (Automated)	☐	☐
2.2.4	Ensure 'Act as part of the operating system' is set to 'No One' (Automated)	☐	☐
2.2.5	Ensure 'Add workstations to domain' is set to 'Administrators' (DC only) (Automated)	☐	☐
2.2.6	Ensure 'Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE' (Automated)	☐	☐
2.2.7	Ensure 'Allow log on locally' is set to 'Administrators, ENTERPRISE DOMAIN CONTROLLERS' (DC only) (Automated)	☐	☐
2.2.8	Ensure 'Allow log on locally' is set to 'Administrators' (MS only) (Automated)	☐	☐
2.2.9	Ensure 'Allow log on through Remote Desktop Services' is set to 'Administrators' (DC only) (Automated)	☐	☐
2.2.10	Ensure 'Allow log on through Remote Desktop Services' is set to 'Administrators, Remote Desktop Users' (MS only) (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.2.11	Ensure 'Back up files and directories' is set to 'Administrators' (Automated)	☐	☐
2.2.12	Ensure 'Change the system time' is set to 'Administrators, LOCAL SERVICE' (Automated)	☐	☐
2.2.13	Ensure 'Create a pagefile' is set to 'Administrators' (Automated)	☐	☐
2.2.14	Ensure 'Create a token object' is set to 'No One' (Automated)	☐	☐
2.2.15	Ensure 'Create global objects' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' (Automated)	☐	☐
2.2.16	Ensure 'Create permanent shared objects' is set to 'No One' (Automated)	☐	☐
2.2.17	Ensure 'Create symbolic links' is set to 'Administrators' (DC only) (Automated)	☐	☐
2.2.18	Ensure 'Create symbolic links' is set to 'Administrators, NT VIRTUAL MACHINE\Virtual Machines' (MS only) (Automated)	☐	☐
2.2.19	Ensure 'Debug programs' is set to 'Administrators' (Automated)	☐	☐
2.2.20	Ensure 'Deny access to this computer from the network' to include 'Guests' (DC only) (Automated)	☐	☐
2.2.21	Ensure 'Deny access to this computer from the network' to include 'Guests, Local account and member of Administrators group' (MS only) (Automated)	☐	☐
2.2.22	Ensure 'Deny log on as a batch job' to include 'Guests' (Automated)	☐	☐
2.2.23	Ensure 'Deny log on as a service' to include 'Guests' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.2.24	Ensure 'Deny log on locally' to include 'Guests' (Automated)	☐	☐
2.2.25	Ensure 'Deny log on through Remote Desktop Services' to include 'Guests' (DC only) (Automated)	☐	☐
2.2.26	Ensure 'Deny log on through Remote Desktop Services' is set to 'Guests, Local account' (MS only) (Automated)	☐	☐
2.2.27	Ensure 'Enable computer and user accounts to be trusted for delegation' is set to 'Administrators' (DC only) (Automated)	☐	☐
2.2.28	Ensure 'Enable computer and user accounts to be trusted for delegation' is set to 'No One' (MS only) (Automated)	☐	☐
2.2.29	Ensure 'Force shutdown from a remote system' is set to 'Administrators' (Automated)	☐	☐
2.2.30	Ensure 'Generate security audits' is set to 'LOCAL SERVICE, NETWORK SERVICE' (Automated)	☐	☐
2.2.31	Ensure 'Impersonate a client after authentication' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' (DC only) (Automated)	☐	☐
2.2.32	Ensure 'Impersonate a client after authentication' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' (MS only) (Automated)	☐	☐
2.2.33	Ensure 'Increase scheduling priority' is set to 'Administrators, Window Manager\Window Manager Group' (Automated)	☐	☐
2.2.34	Ensure 'Load and unload device drivers' is set to 'Administrators' (Automated)	☐	☐
2.2.35	Ensure 'Lock pages in memory' is set to 'No One' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.2.36	Ensure 'Log on as a batch job' is set to 'Administrators' (DC Only) (Automated)	☐	☐
2.2.37	Ensure 'Manage auditing and security log' is set to 'Administrators' (DC only) (Automated)	☐	☐
2.2.38	Ensure 'Manage auditing and security log' is set to 'Administrators' (MS only) (Automated)	☐	☐
2.2.39	Ensure 'Modify an object label' is set to 'No One' (Automated)	☐	☐
2.2.40	Ensure 'Modify firmware environment values' is set to 'Administrators' (Automated)	☐	☐
2.2.41	Ensure 'Perform volume maintenance tasks' is set to 'Administrators' (Automated)	☐	☐
2.2.42	Ensure 'Profile single process' is set to 'Administrators' (Automated)	☐	☐
2.2.43	Ensure 'Profile system performance' is set to 'Administrators, NT SERVICE\WdiServiceHost' (Automated)	☐	☐
2.2.44	Ensure 'Replace a process level token' is set to 'LOCAL SERVICE, NETWORK SERVICE' (Automated)	☐	☐
2.2.45	Ensure 'Restore files and directories' is set to 'Administrators' (Automated)	☐	☐
2.2.46	Ensure 'Shut down the system' is set to 'Administrators' (Automated)	☐	☐
2.2.47	Ensure 'Synchronize directory service data' is set to 'No One' (DC only) (Automated)	☐	☐
2.2.48	Ensure 'Take ownership of files or other objects' is set to 'Administrators' (Automated)	☐	☐
2.3	**Security Options**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.3.1	**Accounts**		
2.3.1.1	Ensure 'Accounts: Guest account status' is set to 'Disabled' (MS only) (Automated)	☐	☐
2.3.1.2	Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled' (Automated)	☐	☐
2.3.1.3	Configure 'Accounts: Rename administrator account' (Automated)	☐	☐
2.3.1.4	Configure 'Accounts: Rename guest account' (Automated)	☐	☐
2.3.2	**Audit**		
2.3.2.1	Ensure 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' is set to 'Enabled' (Automated)	☐	☐
2.3.2.2	Ensure 'Audit: Shut down system immediately if unable to log security audits' is set to 'Disabled' (Automated)	☐	☐
2.3.3	**DCOM**		
2.3.4	**Devices**		
2.3.4.1	Ensure 'Devices: Prevent users from installing printer drivers' is set to 'Enabled' (Automated)	☐	☐
2.3.5	**Domain controller**		
2.3.5.1	Ensure 'Domain controller: Allow server operators to schedule tasks' is set to 'Disabled' (DC only) (Automated)	☐	☐
2.3.5.2	Ensure 'Domain controller: Allow vulnerable Netlogon secure channel connections' is set to 'Not Configured' (DC Only) (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.3.5.3	Ensure 'Domain controller: LDAP server channel binding token requirements' is set to 'Always' (DC Only) (Automated)	☐	☐
2.3.5.4	Ensure 'Domain controller: LDAP server signing requirements' is set to 'Require signing' (DC only) (Automated)	☐	☐
2.3.5.5	Ensure 'Domain controller: Refuse machine account password changes' is set to 'Disabled' (DC only) (Automated)	☐	☐
2.3.6	**Domain member**		
2.3.6.1	Ensure 'Domain member: Digitally encrypt or sign secure channel data (always)' is set to 'Enabled' (Automated)	☐	☐
2.3.6.2	Ensure 'Domain member: Digitally encrypt secure channel data (when possible)' is set to 'Enabled' (Automated)	☐	☐
2.3.6.3	Ensure 'Domain member: Digitally sign secure channel data (when possible)' is set to 'Enabled' (Automated)	☐	☐
2.3.6.4	Ensure 'Domain member: Disable machine account password changes' is set to 'Disabled' (Automated)	☐	☐
2.3.6.5	Ensure 'Domain member: Maximum machine account password age' is set to '30 or fewer days, but not 0' (Automated)	☐	☐
2.3.6.6	Ensure 'Domain member: Require strong (Windows 2000 or later) session key' is set to 'Enabled' (Automated)	☐	☐
2.3.7	**Interactive logon**		
2.3.7.1	Ensure 'Interactive logon: Do not require CTRL+ALT+DEL' is set to 'Disabled' (Automated)	☐	☐
2.3.7.2	Ensure 'Interactive logon: Don't display last signed-in' is set to 'Enabled' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.3.7.3	Ensure 'Interactive logon: Machine inactivity limit' is set to '900 or fewer second(s), but not 0' (Automated)	☐	☐
2.3.7.4	Configure 'Interactive logon: Message text for users attempting to log on' (Automated)	☐	☐
2.3.7.5	Configure 'Interactive logon: Message title for users attempting to log on' (Automated)	☐	☐
2.3.7.6	Ensure 'Interactive logon: Number of previous logons to cache (in case domain controller is not available)' is set to '4 or fewer logon(s)' (MS only) (Automated)	☐	☐
2.3.7.7	Ensure 'Interactive logon: Prompt user to change password before expiration' is set to 'between 5 and 14 days' (Automated)	☐	☐
2.3.7.8	Ensure 'Interactive logon: Require Domain Controller Authentication to unlock workstation' is set to 'Enabled' (MS only) (Automated)	☐	☐
2.3.7.9	Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or higher (Automated)	☐	☐
2.3.8	**Microsoft network client**		
2.3.8.1	Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled' (Automated)	☐	☐
2.3.8.2	Ensure 'Microsoft network client: Send unencrypted password to third-party SMB servers' is set to 'Disabled' (Automated)	☐	☐
2.3.9	**Microsoft network server**		
2.3.9.1	Ensure 'Microsoft network server: Amount of idle time required before suspending session' is set to '15 or fewer minute(s)' (Automated)	☐	☐
2.3.9.2	Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.3.9.3	Ensure 'Microsoft network server: Disconnect clients when logon hours expire' is set to 'Enabled' (Automated)	☐	☐
2.3.9.4	Ensure 'Microsoft network server: Server SPN target name validation level' is set to 'Accept if provided by client' or higher (MS only) (Automated)	☐	☐
2.3.10	**Network access**		
2.3.10.1	Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled' (Automated)	☐	☐
2.3.10.2	Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts' is set to 'Enabled' (MS only) (Automated)	☐	☐
2.3.10.3	Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled' (MS only) (Automated)	☐	☐
2.3.10.4	Ensure 'Network access: Do not allow storage of passwords and credentials for network authentication' is set to 'Enabled' (Automated)	☐	☐
2.3.10.5	Ensure 'Network access: Let Everyone permissions apply to anonymous users' is set to 'Disabled' (Automated)	☐	☐
2.3.10.6	Ensure 'Network access: Named Pipes that can be accessed anonymously' is configured (DC only) (Automated)	☐	☐
2.3.10.7	Ensure 'Network access: Named Pipes that can be accessed anonymously' is configured (MS only) (Automated)	☐	☐
2.3.10.8	Ensure 'Network access: Remotely accessible registry paths' is configured (Automated)	☐	☐
2.3.10.9	Ensure 'Network access: Remotely accessible registry paths and sub-paths' is configured (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.3.10.10	Ensure 'Network access: Restrict anonymous access to Named Pipes and Shares' is set to 'Enabled' (Automated)	☐	☐
2.3.10.11	Ensure 'Network access: Restrict clients allowed to make remote calls to SAM' is set to 'Administrators: Remote Access: Allow' (MS only) (Automated)	☐	☐
2.3.10.12	Ensure 'Network access: Shares that can be accessed anonymously' is set to 'None' (Automated)	☐	☐
2.3.10.13	Ensure 'Network access: Sharing and security model for local accounts' is set to 'Classic - local users authenticate as themselves' (Automated)	☐	☐
2.3.11	**Network security**		
2.3.11.1	Ensure 'Network security: Allow Local System to use computer identity for NTLM' is set to 'Enabled' (Automated)	☐	☐
2.3.11.2	Ensure 'Network security: Allow LocalSystem NULL session fallback' is set to 'Disabled' (Automated)	☐	☐
2.3.11.3	Ensure 'Network Security: Allow PKU2U authentication requests to this computer to use online identities' is set to 'Disabled' (Automated)	☐	☐
2.3.11.4	Ensure 'Network security: Configure encryption types allowed for Kerberos' is set to 'AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types' (Automated)	☐	☐
2.3.11.5	Ensure 'Network security: Do not store LAN Manager hash value on next password change' is set to 'Enabled' (Automated)	☐	☐
2.3.11.6	Ensure 'Network security: Force logoff when logon hours expire' is set to 'Enabled' (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.3.11.7	Ensure 'Network security: LAN Manager authentication level' is set to 'Send NTLMv2 response only. Refuse LM & NTLM' (Automated)	☐	☐
2.3.11.8	Ensure 'Network security: LDAP client signing requirements' is set to 'Negotiate signing' or higher (Automated)	☐	☐
2.3.11.9	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' (Automated)	☐	☐
2.3.11.10	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' (Automated)	☐	☐
2.3.11.11	Ensure 'Network security: Restrict NTLM: Audit Incoming NTLM Traffic' is set to 'Enable auditing for all accounts' (Automated)	☐	☐
2.3.11.12	Ensure 'Network security: Restrict NTLM: Audit NTLM authentication in this domain' is set to 'Enable all' (DC only) (Automated)	☐	☐
2.3.11.13	Ensure 'Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers' is set to 'Audit all' or higher (Automated)	☐	☐
2.3.12	**Recovery console**		
2.3.13	**Shutdown**		
2.3.13.1	Ensure 'Shutdown: Allow system to be shut down without having to log on' is set to 'Disabled' (Automated)	☐	☐
2.3.14	**System cryptography**		
2.3.15	**System objects**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.3.15.1	Ensure 'System objects: Require case insensitivity for non-Windows subsystems' is set to 'Enabled' (Automated)	☐	☐
2.3.15.2	Ensure 'System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)' is set to 'Enabled' (Automated)	☐	☐
2.3.16	**System settings**		
2.3.17	**User Account Control**		
2.3.17.1	Ensure 'User Account Control: Admin Approval Mode for the Built-in Administrator account' is set to 'Enabled' (Automated)	☐	☐
2.3.17.2	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 (Automated)	☐	☐
2.3.17.3	Ensure 'User Account Control: Behavior of the elevation prompt for standard users' is set to 'Automatically deny elevation requests' (Automated)	☐	☐
2.3.17.4	Ensure 'User Account Control: Detect application installations and prompt for elevation' is set to 'Enabled' (Automated)	☐	☐
2.3.17.5	Ensure 'User Account Control: Only elevate UIAccess applications that are installed in secure locations' is set to 'Enabled' (Automated)	☐	☐
2.3.17.6	Ensure 'User Account Control: Run all administrators in Admin Approval Mode' is set to 'Enabled' (Automated)	☐	☐
2.3.17.7	Ensure 'User Account Control: Switch to the secure desktop when prompting for elevation' is set to 'Enabled' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.3.17.8	Ensure 'User Account Control: Virtualize file and registry write failures to per-user locations' is set to 'Enabled' (Automated)	☐	☐
3	**Event Log**		
4	**Restricted Groups**		
5	**System Services**		
5.1	Ensure 'Print Spooler (Spooler)' is set to 'Disabled' (DC only) (Automated)	☐	☐
5.2	Ensure 'Print Spooler (Spooler)' is set to 'Disabled' (MS only) (Automated)	☐	☐
6	**Registry**		
7	**File System**		
8	**Wired Network (IEEE 802.3) Policies**		
9	**Windows Defender Firewall with Advanced Security (formerly Windows Firewall with Advanced Security)**		
9.1	**Domain Profile**		
9.1.1	Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)' (Automated)	☐	☐
9.1.2	Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)' (Automated)	☐	☐
9.1.3	Ensure 'Windows Firewall: Domain: Settings: Display a notification' is set to 'No' (Automated)	☐	☐
9.1.4	Ensure 'Windows Firewall: Domain: Logging: Name' is configured (Automated)	☐	☐
9.1.5	Ensure 'Windows Firewall: Domain: Logging: Size limit (KB)' is set to '16,384 KB or greater' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
9.1.6	Ensure 'Windows Firewall: Domain: Logging: Log dropped packets' is set to 'Yes' (Automated)	☐	☐
9.1.7	Ensure 'Windows Firewall: Domain: Logging: Log successful connections' is set to 'Yes' (Automated)	☐	☐
9.2	**Private Profile**		
9.2.1	Ensure 'Windows Firewall: Private: Firewall state' is set to 'On (recommended)' (Automated)	☐	☐
9.2.2	Ensure 'Windows Firewall: Private: Inbound connections' is set to 'Block (default)' (Automated)	☐	☐
9.2.3	Ensure 'Windows Firewall: Private: Settings: Display a notification' is set to 'No' (Automated)	☐	☐
9.2.4	Ensure 'Windows Firewall: Private: Logging: Name' is configured (Automated)	☐	☐
9.2.5	Ensure 'Windows Firewall: Private: Logging: Size limit (KB)' is set to '16,384 KB or greater' (Automated)	☐	☐
9.2.6	Ensure 'Windows Firewall: Private: Logging: Log dropped packets' is set to 'Yes' (Automated)	☐	☐
9.2.7	Ensure 'Windows Firewall: Private: Logging: Log successful connections' is set to 'Yes' (Automated)	☐	☐
9.3	**Public Profile**		
9.3.1	Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)' (Automated)	☐	☐
9.3.2	Ensure 'Windows Firewall: Public: Inbound connections' is set to 'Block (default)' (Automated)	☐	☐
9.3.3	Ensure 'Windows Firewall: Public: Settings: Display a notification' is set to 'No' (Automated)	☐	☐
9.3.4	Ensure 'Windows Firewall: Public: Settings: Apply local firewall rules' is set to 'No' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
9.3.5	Ensure 'Windows Firewall: Public: Settings: Apply local connection security rules' is set to 'No' (Automated)	☐	☐
9.3.6	Ensure 'Windows Firewall: Public: Logging: Name' is configured (Automated)	☐	☐
9.3.7	Ensure 'Windows Firewall: Public: Logging: Size limit (KB)' is set to '16,384 KB or greater' (Automated)	☐	☐
9.3.8	Ensure 'Windows Firewall: Public: Logging: Log dropped packets' is set to 'Yes' (Automated)	☐	☐
9.3.9	Ensure 'Windows Firewall: Public: Logging: Log successful connections' is set to 'Yes' (Automated)	☐	☐
10	**Network List Manager Policies**		
11	**Wireless Network (IEEE 802.11) Policies**		
12	**Public Key Policies**		
13	**Software Restriction Policies**		
14	**Network Access Protection NAP Client Configuration**		
15	**Application Control Policies**		
16	**IP Security Policies**		
17	**Advanced Audit Policy Configuration**		
17.1	**Account Logon**		
17.1.1	Ensure 'Audit Credential Validation' is set to 'Success and Failure' (Automated)	☐	☐
17.1.2	Ensure 'Audit Kerberos Authentication Service' is set to 'Success and Failure' (DC Only) (Automated)	☐	☐
17.1.3	Ensure 'Audit Kerberos Service Ticket Operations' is set to 'Success and Failure' (DC Only) (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
17.2	**Account Management**		
17.2.1	Ensure 'Audit Application Group Management' is set to 'Success and Failure' (Automated)	☐	☐
17.2.2	Ensure 'Audit Computer Account Management' is set to include 'Success' (DC only) (Automated)	☐	☐
17.2.3	Ensure 'Audit Distribution Group Management' is set to include 'Success' (DC only) (Automated)	☐	☐
17.2.4	Ensure 'Audit Other Account Management Events' is set to include 'Success' (DC only) (Automated)	☐	☐
17.2.5	Ensure 'Audit Security Group Management' is set to include 'Success' (Automated)	☐	☐
17.2.6	Ensure 'Audit User Account Management' is set to 'Success and Failure' (Automated)	☐	☐
17.3	**Detailed Tracking**		
17.3.1	Ensure 'Audit PNP Activity' is set to include 'Success' (Automated)	☐	☐
17.3.2	Ensure 'Audit Process Creation' is set to include 'Success' (Automated)	☐	☐
17.4	**DS Access**		
17.4.1	Ensure 'Audit Directory Service Access' is set to include 'Failure' (DC only) (Automated)	☐	☐
17.4.2	Ensure 'Audit Directory Service Changes' is set to include 'Success' (DC only) (Automated)	☐	☐
17.5	**Logon/Logoff**		
17.5.1	Ensure 'Audit Account Lockout' is set to include 'Failure' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
17.5.2	Ensure 'Audit Group Membership' is set to include 'Success' (Automated)	☐	☐
17.5.3	Ensure 'Audit Logoff' is set to include 'Success' (Automated)	☐	☐
17.5.4	Ensure 'Audit Logon' is set to 'Success and Failure' (Automated)	☐	☐
17.5.5	Ensure 'Audit Other Logon/Logoff Events' is set to 'Success and Failure' (Automated)	☐	☐
17.5.6	Ensure 'Audit Special Logon' is set to include 'Success' (Automated)	☐	☐
17.6	**Object Access**		
17.6.1	Ensure 'Audit Detailed File Share' is set to include 'Failure' (Automated)	☐	☐
17.6.2	Ensure 'Audit File Share' is set to 'Success and Failure' (Automated)	☐	☐
17.6.3	Ensure 'Audit Other Object Access Events' is set to 'Success and Failure' (Automated)	☐	☐
17.6.4	Ensure 'Audit Removable Storage' is set to 'Success and Failure' (Automated)	☐	☐
17.7	**Policy Change**		
17.7.1	Ensure 'Audit Audit Policy Change' is set to include 'Success' (Automated)	☐	☐
17.7.2	Ensure 'Audit Authentication Policy Change' is set to include 'Success' (Automated)	☐	☐
17.7.3	Ensure 'Audit Authorization Policy Change' is set to include 'Success' (Automated)	☐	☐
17.7.4	Ensure 'Audit MPSSVC Rule-Level Policy Change' is set to 'Success and Failure' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
17.7.5	Ensure 'Audit Other Policy Change Events' is set to include 'Failure' (Automated)	☐	☐
17.8	**Privilege Use**		
17.8.1	Ensure 'Audit Sensitive Privilege Use' is set to 'Success' (Automated)	☐	☐
17.9	**System**		
17.9.1	Ensure 'Audit IPsec Driver' is set to 'Success and Failure' (Automated)	☐	☐
17.9.2	Ensure 'Audit Other System Events' is set to 'Success and Failure' (Automated)	☐	☐
17.9.3	Ensure 'Audit Security State Change' is set to include 'Success' (Automated)	☐	☐
17.9.4	Ensure 'Audit Security System Extension' is set to include 'Success' (Automated)	☐	☐
17.9.5	Ensure 'Audit System Integrity' is set to 'Success and Failure' (Automated)	☐	☐
18	**Administrative Templates (Computer)**		
18.1	**Control Panel**		
18.1.1	**Personalization**		
18.1.1.1	Ensure 'Prevent enabling lock screen camera' is set to 'Enabled' (Automated)	☐	☐
18.1.1.2	Ensure 'Prevent enabling lock screen slide show' is set to 'Enabled' (Automated)	☐	☐
18.1.2	**Regional and Language Options**		
18.1.2.1	**Handwriting personalization**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.1.2.2	Ensure 'Allow users to enable online speech recognition services' is set to 'Disabled' (Automated)	☐	☐
18.1.3	Ensure 'Allow Online Tips' is set to 'Disabled' (Automated)	☐	☐
18.2	**Desktop**		
18.3	**LAPS (legacy)**		
18.4	**MS Security Guide**		
18.4.1	Ensure 'Apply UAC restrictions to local accounts on network logons' is set to 'Enabled' (MS only) (Automated)	☐	☐
18.4.2	Ensure 'Configure SMB v1 client driver' is set to 'Enabled: Disable driver (recommended)' (Automated)	☐	☐
18.4.3	Ensure 'Configure SMB v1 server' is set to 'Disabled' (Automated)	☐	☐
18.4.4	Ensure 'Enable Certificate Padding' is set to 'Enabled' (Automated)	☐	☐
18.4.5	Ensure 'Enable Structured Exception Handling Overwrite Protection (SEHOP)' is set to 'Enabled' (Automated)	☐	☐
18.4.6	Ensure 'NetBT NodeType configuration' is set to 'Enabled: P-node (recommended)' (Automated)	☐	☐
18.5	**MSS (Legacy)**		
18.5.1	Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon' is set to 'Disabled' (Automated)	☐	☐
18.5.2	Ensure 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level' is set to 'Enabled: Highest protection, source routing is completely disabled' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.5.3	Ensure 'MSS: (DisableIPSourceRouting) IP source routing protection level' is set to 'Enabled: Highest protection, source routing is completely disabled' (Automated)	☐	☐
18.5.4	Ensure 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' is set to 'Disabled' (Automated)	☐	☐
18.5.5	Ensure 'MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds' is set to 'Enabled: 300,000 or 5 minutes' (Automated)	☐	☐
18.5.6	Ensure 'MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers' is set to 'Enabled' (Automated)	☐	☐
18.5.7	Ensure 'MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses' is set to 'Disabled' (Automated)	☐	☐
18.5.8	Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode' is set to 'Enabled' (Automated)	☐	☐
18.5.9	Ensure 'MSS: (TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted' is set to 'Enabled: 3' (Automated)	☐	☐
18.5.10	Ensure 'MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted' is set to 'Enabled: 3' (Automated)	☐	☐
18.5.11	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' (Automated)	☐	☐
18.6	**Network**		
18.6.1	**Background Intelligent Transfer Service (BITS)**		
18.6.2	**BranchCache**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.6.3	**DirectAccess Client Experience Settings**		
18.6.4	**DNS Client**		
18.6.4.1	Ensure 'Configure multicast DNS (mDNS) protocol' is set to 'Disabled' (Automated)	☐	☐
18.6.4.2	Ensure 'Configure NetBIOS settings' is set to 'Enabled: Disable NetBIOS name resolution on public networks' (Automated)	☐	☐
18.6.4.3	Ensure 'Turn off default IPv6 DNS Servers' is set to 'Enabled' (Automated)	☐	☐
18.6.4.4	Ensure 'Turn off multicast name resolution' is set to 'Enabled' (Automated)	☐	☐
18.6.5	**Fonts**		
18.6.5.1	Ensure 'Enable Font Providers' is set to 'Disabled' (Automated)	☐	☐
18.6.6	**Hotspot Authentication**		
18.6.7	**Lanman Server**		
18.6.7.1	Ensure 'Mandate the minimum version of SMB' is set to 'Enabled: 3.1.1' (Automated)	☐	☐
18.6.8	**Lanman Workstation**		
18.6.8.1	Ensure 'Enable insecure guest logons' is set to 'Disabled' (Automated)	☐	☐
18.6.8.2	Ensure 'Require Encryption' is set to 'Enabled' (Automated)	☐	☐
18.6.9	**Link-Layer Topology Discovery**		
18.6.9.1	Ensure 'Turn on Mapper I/O (LLTDIO) driver' is set to 'Disabled' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.6.9.2	Ensure 'Turn on Responder (RSPNDR) driver' is set to 'Disabled' (Automated)	☐	☐
18.6.10	**Microsoft Peer-to-Peer Networking Services**		
18.6.10.1	**Peer Name Resolution Protocol**		
18.6.10.2	Ensure 'Turn off Microsoft Peer-to-Peer Networking Services' is set to 'Enabled' (Automated)	☐	☐
18.6.11	**Network Connections**		
18.6.11.1	**Windows Defender Firewall (formerly Windows Firewall)**		
18.6.11.2	Ensure 'Prohibit installation and configuration of Network Bridge on your DNS domain network' is set to 'Enabled' (Automated)	☐	☐
18.6.11.3	Ensure 'Prohibit use of Internet Connection Sharing on your DNS domain network' is set to 'Enabled' (Automated)	☐	☐
18.6.11.4	Ensure 'Require domain users to elevate when setting a network's location' is set to 'Enabled' (Automated)	☐	☐
18.6.12	**Network Connectivity Status Indicator**		
18.6.13	**Network Isolation**		
18.6.14	**Network Provider**		
18.6.14.1	Ensure 'Hardened UNC Paths' is set to 'Enabled, with "Require Mutual Authentication", "Require Integrity", and "Require Privacy" set for all NETLOGON and SYSVOL shares' (Automated)	☐	☐
18.6.15	**Offline Files**		
18.6.16	**QoS Packet Scheduler**		
18.6.17	**SNMP**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.6.18	**SSL Configuration Settings**		
18.6.19	**TCPIP Settings**		
18.6.19.1	**IPv6 Transition Technologies**		
18.6.19.2	**Parameters**		
18.6.19.2.1	Disable IPv6 (Ensure TCPIP6 Parameter 'DisabledComponents' is set to '0xff (255)') (Automated)	☐	☐
18.6.20	**Windows Connect Now**		
18.6.20.1	Ensure 'Configuration of wireless settings using Windows Connect Now' is set to 'Disabled' (Automated)	☐	☐
18.6.20.2	Ensure 'Prohibit access of the Windows Connect Now wizards' is set to 'Enabled' (Automated)	☐	☐
18.6.21	**Windows Connection Manager**		
18.6.21.1	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' (Automated)	☐	☐
18.6.21.2	Ensure 'Prohibit connection to non-domain networks when connected to domain authenticated network' is set to 'Enabled' (MS only) (Automated)	☐	☐
18.7	**Printers**		
18.7.1	Ensure 'Allow Print Spooler to accept client connections' is set to 'Disabled' (Automated)	☐	☐
18.7.2	Ensure 'Configure Redirection Guard' is set to 'Enabled: Redirection Guard Enabled' (Automated)	☐	☐
18.7.3	Ensure 'Configure RPC connection settings: Protocol to use for outgoing RPC connections' is set to 'Enabled: RPC over TCP' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.7.4	Ensure 'Configure RPC connection settings: Use authentication for outgoing RPC connections' is set to 'Enabled: Default' (Automated)	☐	☐
18.7.5	Ensure 'Configure RPC listener settings: Protocols to allow for incoming RPC connections' is set to 'Enabled: RPC over TCP' (Automated)	☐	☐
18.7.6	Ensure 'Configure RPC listener settings: Authentication protocol to use for incoming RPC connections:' is set to 'Enabled: Negotiate' or higher (Automated)	☐	☐
18.7.7	Ensure 'Configure RPC over TCP port' is set to 'Enabled: 0' (Automated)	☐	☐
18.7.8	Ensure 'Configure RPC packet level privacy setting for incoming connections' is set to 'Enabled' (Automated)	☐	☐
18.7.9	Ensure 'Limits print driver installation to Administrators' is set to 'Enabled' (Automated)	☐	☐
18.7.10	Ensure 'Manage processing of Queue-specific files' is set to 'Enabled: Limit Queue-specific files to Color profiles' (Automated)	☐	☐
18.7.11	Ensure 'Point and Print Restrictions: When installing drivers for a new connection' is set to 'Enabled: Show warning and elevation prompt' (Automated)	☐	☐
18.7.12	Ensure 'Point and Print Restrictions: When updating drivers for an existing connection' is set to 'Enabled: Show warning and elevation prompt' (Automated)	☐	☐
18.8	**Start Menu and Taskbar**		
18.8.1	**Notifications**		
18.8.1.1	Ensure 'Turn off notifications network usage' is set to 'Enabled' (Automated)	☐	☐
18.9	**System**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.9.1	**Access-Denied Assistance**		
18.9.2	**App-V**		
18.9.3	**Audit Process Creation**		
18.9.3.1	Ensure 'Include command line in process creation events' is set to 'Enabled' (Automated)	☐	☐
18.9.4	**Credentials Delegation**		
18.9.4.1	Ensure 'Encryption Oracle Remediation' is set to 'Enabled: Force Updated Clients' (Automated)	☐	☐
18.9.4.2	Ensure 'Remote host allows delegation of non-exportable credentials' is set to 'Enabled' (Automated)	☐	☐
18.9.5	**Device Guard**		
18.9.5.1	Ensure 'Turn On Virtualization Based Security' is set to 'Enabled' (Automated)	☐	☐
18.9.5.2	Ensure 'Turn On Virtualization Based Security: Select Platform Security Level' is set to 'Secure Boot' or higher (Automated)	☐	☐
18.9.5.3	Ensure 'Turn On Virtualization Based Security: Virtualization Based Protection of Code Integrity' is set to 'Enabled with UEFI lock' (Automated)	☐	☐
18.9.5.4	Ensure 'Turn On Virtualization Based Security: Require UEFI Memory Attributes Table' is set to 'True (checked)' (Automated)	☐	☐
18.9.5.5	Ensure 'Turn On Virtualization Based Security: Credential Guard Configuration' is set to 'Enabled with UEFI lock' (MS Only) (Automated)	☐	☐
18.9.5.6	Ensure 'Turn On Virtualization Based Security: Credential Guard Configuration' is set to 'Disabled' (DC Only) (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.9.5.7	Ensure 'Turn On Virtualization Based Security: Secure Launch Configuration' is set to 'Enabled' (Automated)	☐	☐
18.9.6	**Device Health Attestation Service**		
18.9.7	**Device Installation**		
18.9.7.1	**Device Installation Restrictions**		
18.9.7.2	Ensure 'Prevent automatic download of applications associated with device metadata' is set to 'Enabled' (Automated)	☐	☐
18.9.8	**Disk NV Cache**		
18.9.9	**Disk Quotas**		
18.9.10	**Display**		
18.9.11	**Distributed COM**		
18.9.12	**Driver Installation**		
18.9.13	**Early Launch Antimalware**		
18.9.13.1	Ensure 'Boot-Start Driver Initialization Policy' is set to 'Enabled: Good, unknown and bad but critical' (Automated)	☐	☐
18.9.14	**Enhanced Storage Access**		
18.9.15	**File Classification Infrastructure**		
18.9.16	**File Share Shadow Copy Provider**		
18.9.17	**Filesystem (formerly NTFS Filesystem)**		
18.9.17.1	Ensure 'Enable / disable CLFS logfile authentication' is set to 'Enabled' (Automated)	☐	☐
18.9.18	**Folder Redirection**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.9.19	**Group Policy**		
18.9.19.1	**Logging and tracing**		
18.9.19.2	Ensure 'Configure security policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE' (Automated)	☐	☐
18.9.19.3	Ensure 'Configure security policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE' (Automated)	☐	☐
18.9.19.4	Ensure 'Continue experiences on this device' is set to 'Disabled' (Automated)	☐	☐
18.9.19.5	Ensure 'Turn off background refresh of Group Policy' is set to 'Disabled' (Automated)	☐	☐
18.9.20	**Internet Communication Management**		
18.9.20.1	**Internet Communication settings**		
18.9.20.1.1	Ensure 'Turn off downloading of print drivers over HTTP' is set to 'Enabled' (Automated)	☐	☐
18.9.20.1.2	Ensure 'Turn off handwriting personalization data sharing' is set to 'Enabled' (Automated)	☐	☐
18.9.20.1.3	Ensure 'Turn off handwriting recognition error reporting' is set to 'Enabled' (Automated)	☐	☐
18.9.20.1.4	Ensure 'Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com' is set to 'Enabled' (Automated)	☐	☐
18.9.20.1.5	Ensure 'Turn off Internet download for Web publishing and online ordering wizards' is set to 'Enabled' (Automated)	☐	☐
18.9.20.1.6	Ensure 'Turn off printing over HTTP' is set to 'Enabled' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.9.20.1.7	Ensure 'Turn off Registration if URL connection is referring to Microsoft.com' is set to 'Enabled' (Automated)	☐	☐
18.9.20.1.8	Ensure 'Turn off Search Companion content file updates' is set to 'Enabled' (Automated)	☐	☐
18.9.20.1.9	Ensure 'Turn off the "Order Prints" picture task' is set to 'Enabled' (Automated)	☐	☐
18.9.20.1.10	Ensure 'Turn off the "Publish to Web" task for files and folders' is set to 'Enabled' (Automated)	☐	☐
18.9.20.1.11	Ensure 'Turn off the Windows Messenger Customer Experience Improvement Program' is set to 'Enabled' (Automated)	☐	☐
18.9.20.1.12	Ensure 'Turn off Windows Customer Experience Improvement Program' is set to 'Enabled' (Automated)	☐	☐
18.9.20.1.13	Ensure 'Turn off Windows Error Reporting' is set to 'Enabled' (Automated)	☐	☐
18.9.21	**iSCSI**		
18.9.22	**KDC**		
18.9.23	**Kerberos**		
18.9.23.1	Ensure 'Support device authentication using certificate' is set to 'Enabled: Automatic' (Automated)	☐	☐
18.9.24	**Kernel DMA Protection**		
18.9.24.1	Ensure 'Enumeration policy for external devices incompatible with Kernel DMA Protection' is set to 'Enabled: Block All' (Automated)	☐	☐
18.9.25	**Keyboard Filter**		
18.9.26	**LAPS**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.9.26.1	Ensure 'Configure password backup directory' is set to 'Enabled: Active Directory' or 'Enabled: Azure Active Directory' (MS only) (Automated)	☐	☐
18.9.26.2	Ensure 'Do not allow password expiration time longer than required by policy' is set to 'Enabled' (MS only) (Automated)	☐	☐
18.9.26.3	Ensure 'Enable password encryption' is set to 'Enabled' (MS only) (Automated)	☐	☐
18.9.26.4	Ensure 'Password Settings: Password Complexity' is set to 'Enabled: Large letters + small letters + numbers + specials' (MS only) (Automated)	☐	☐
18.9.26.5	Ensure 'Password Settings: Password Length' is set to 'Enabled: 15 or more' (MS only) (Automated)	☐	☐
18.9.26.6	Ensure 'Password Settings: Password Age (Days)' is set to 'Enabled: 30 or fewer' (MS only) (Automated)	☐	☐
18.9.26.7	Ensure 'Post-authentication actions: Grace period (hours)' is set to 'Enabled: 8 or fewer hours, but not 0' (MS only) (Automated)	☐	☐
18.9.26.8	Ensure 'Post-authentication actions: Actions' is set to 'Enabled: Reset the password and logoff the managed account' or higher (MS only) (Automated)	☐	☐
18.9.27	**Local Security Authority**		
18.9.27.1	Ensure 'Allow Custom SSPs and APs to be loaded into LSASS' is set to 'Disabled' (DC only) (Automated)	☐	☐
18.9.27.2	Ensure 'Configures LSASS to run as a protected process' is set to 'Enabled: Enabled with UEFI Lock' (Automated)	☐	☐
18.9.28	**Locale Services**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.9.28.1	Ensure 'Disallow copying of user input methods to the system account for sign-in' is set to 'Enabled' (Automated)	☐	☐
18.9.29	**Logon**		
18.9.29.1	Ensure 'Block user from showing account details on sign-in' is set to 'Enabled' (Automated)	☐	☐
18.9.29.2	Ensure 'Do not display network selection UI' is set to 'Enabled' (Automated)	☐	☐
18.9.29.3	Ensure 'Do not enumerate connected users on domain-joined computers' is set to 'Enabled' (Automated)	☐	☐
18.9.29.4	Ensure 'Enumerate local users on domain-joined computers' is set to 'Disabled' (MS only) (Automated)	☐	☐
18.9.29.5	Ensure 'Turn off app notifications on the lock screen' is set to 'Enabled' (Automated)	☐	☐
18.9.29.6	Ensure 'Turn on convenience PIN sign-in' is set to 'Disabled' (Automated)	☐	☐
18.9.30	**Mitigation Options**		
18.9.31	**Net Logon**		
18.9.32	**NTLM**		
18.9.33	**OS Policies**		
18.9.33.1	Ensure 'Allow Clipboard synchronization across devices' is set to 'Disabled' (Automated)	☐	☐
18.9.33.2	Ensure 'Allow upload of User Activities' is set to 'Disabled' (Automated)	☐	☐
18.9.34	**PIN Complexity**		
18.9.35	**Power Management**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.9.35.1	**Button Settings**		
18.9.35.2	**Energy Saver Settings**		
18.9.35.3	**Hard Disk Settings**		
18.9.35.4	**Notification Settings**		
18.9.35.5	**Power Throttling Settings**		
18.9.35.6	**Sleep Settings**		
18.9.35.6.1	Ensure 'Allow network connectivity during connected-standby (on battery)' is set to 'Disabled' (Automated)	☐	☐
18.9.35.6.2	Ensure 'Allow network connectivity during connected-standby (plugged in)' is set to 'Disabled' (Automated)	☐	☐
18.9.35.6.3	Ensure 'Require a password when a computer wakes (on battery)' is set to 'Enabled' (Automated)	☐	☐
18.9.35.6.4	Ensure 'Require a password when a computer wakes (plugged in)' is set to 'Enabled' (Automated)	☐	☐
18.9.36	**Recovery**		
18.9.37	**Remote Assistance**		
18.9.37.1	Ensure 'Configure Offer Remote Assistance' is set to 'Disabled' (Automated)	☐	☐
18.9.37.2	Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled' (Automated)	☐	☐
18.9.38	**Remote Procedure Call**		
18.9.38.1	Ensure 'Enable RPC Endpoint Mapper Client Authentication' is set to 'Enabled' (MS only) (Automated)	☐	☐
18.9.38.2	Ensure 'Restrict Unauthenticated RPC clients' is set to 'Enabled: Authenticated' (MS only) (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.9.39	**Removable Storage Access**		
18.9.40	**Scripts**		
18.9.41	**Security Account Manager**		
18.9.41.1	Ensure 'Configure validation of ROCA-vulnerable WHfB keys during authentication' is set to 'Enabled: Block' (DC only) (Automated)	☐	☐
18.9.42	**Server Manager**		
18.9.43	**Service Control Manager Settings**		
18.9.44	**Shutdown**		
18.9.45	**Shutdown Options**		
18.9.46	**Storage Health**		
18.9.47	**Storage Sense**		
18.9.48	**System Restore**		
18.9.49	**Troubleshooting and Diagnostics**		
18.9.49.1	**Application Compatibility Diagnostics**		
18.9.49.2	**Corrupted File Recovery**		
18.9.49.3	**Disk Diagnostic**		
18.9.49.4	**Fault Tolerant Heap**		
18.9.49.5	**Microsoft Support Diagnostic Tool**		
18.9.49.5.1	Ensure 'Microsoft Support Diagnostic Tool: Turn on MSDT interactive communication with support provider' is set to 'Disabled' (Automated)	☐	☐
18.9.49.6	**MSI Corrupted File Recovery**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.9.49.7	**Scheduled Maintenance**		
18.9.49.8	**Scripted Diagnostics**		
18.9.49.9	**Windows Boot Performance Diagnostics**		
18.9.49.10	**Windows Memory Leak Diagnosis**		
18.9.49.11	**Windows Performance PerfTrack**		
18.9.49.11.1	Ensure 'Enable/Disable PerfTrack' is set to 'Disabled' (Automated)	☐	☐
18.9.50	**Trusted Platform Module Services**		
18.9.51	**User Profiles**		
18.9.51.1	Ensure 'Turn off the advertising ID' is set to 'Enabled' (Automated)	☐	☐
18.9.52	**Windows File Protection**		
18.9.53	**Windows Time Service**		
18.9.53.1	**Time Providers**		
18.9.53.1.1	Ensure 'Enable Windows NTP Client' is set to 'Enabled' (Automated)	☐	☐
18.9.53.1.2	Ensure 'Enable Windows NTP Server' is set to 'Disabled' (MS only) (Automated)	☐	☐
18.10	**Windows Components**		
18.10.1	**ActiveX Installer Service**		
18.10.2	**Add features to Windows 10 (formerly Windows Anytime Upgrade)**		
18.10.3	**App and Device Inventory**		
18.10.4	**App Package Deployment**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.10.4.1	Ensure 'Allow a Windows app to share application data between users' is set to 'Disabled' (Automated)	☐	☐
18.10.5	**App Privacy**		
18.10.6	**App runtime**		
18.10.6.1	Ensure 'Allow Microsoft accounts to be optional' is set to 'Enabled' (Automated)	☐	☐
18.10.7	**Application Compatibility**		
18.10.8	**AutoPlay Policies**		
18.10.8.1	Ensure 'Disallow Autoplay for non-volume devices' is set to 'Enabled' (Automated)	☐	☐
18.10.8.2	Ensure 'Set the default behavior for AutoRun' is set to 'Enabled: Do not execute any autorun commands' (Automated)	☐	☐
18.10.8.3	Ensure 'Turn off Autoplay' is set to 'Enabled: All drives' (Automated)	☐	☐
18.10.9	**Biometrics**		
18.10.9.1	**Facial Features**		
18.10.9.1.1	Ensure 'Configure enhanced anti-spoofing' is set to 'Enabled' (Automated)	☐	☐
18.10.10	**BitLocker Drive Encryption**		
18.10.11	**Camera**		
18.10.11.1	Ensure 'Allow Use of Camera' is set to 'Disabled' (Automated)	☐	☐
18.10.12	**Chat**		
18.10.13	**Cloud Content**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.10.13.1	Ensure 'Turn off cloud consumer account state content' is set to 'Enabled' (Automated)	☐	☐
18.10.13.2	Ensure 'Turn off cloud optimized content' is set to 'Enabled' (Automated)	☐	☐
18.10.14	**Connect**		
18.10.14.1	Ensure 'Require pin for pairing' is set to 'Enabled: First Time' OR 'Enabled: Always' (Automated)	☐	☐
18.10.15	**Credential User Interface**		
18.10.15.1	Ensure 'Do not display the password reveal button' is set to 'Enabled' (Automated)	☐	☐
18.10.15.2	Ensure 'Enumerate administrator accounts on elevation' is set to 'Disabled' (Automated)	☐	☐
18.10.16	**Data Collection and Preview Builds**		
18.10.16.1	Ensure 'Allow Diagnostic Data' is set to 'Enabled: Diagnostic data off (not recommended)' or 'Enabled: Send required diagnostic data' (Automated)	☐	☐
18.10.16.2	Ensure 'Configure Authenticated Proxy usage for the Connected User Experience and Telemetry service' is set to 'Enabled: Disable Authenticated Proxy usage' (Automated)	☐	☐
18.10.16.3	Ensure 'Do not show feedback notifications' is set to 'Enabled' (Automated)	☐	☐
18.10.16.4	Ensure 'Enable OneSettings Auditing' is set to 'Enabled' (Automated)	☐	☐
18.10.16.5	Ensure 'Limit Diagnostic Log Collection' is set to 'Enabled' (Automated)	☐	☐
18.10.16.6	Ensure 'Limit Dump Collection' is set to 'Enabled' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.10.17	**Delivery Optimization**		
18.10.18	**Desktop App Installer**		
18.10.18.1	Ensure 'Enable App Installer' is set to 'Disabled' (Automated)	☐	☐
18.10.18.2	Ensure 'Enable App Installer Experimental Features' is set to 'Disabled' (Automated)	☐	☐
18.10.18.3	Ensure 'Enable App Installer Hash Override' is set to 'Disabled' (Automated)	☐	☐
18.10.18.4	Ensure 'Enable App Installer Local Archive Malware Scan Override' is set to 'Disabled' (Automated)	☐	☐
18.10.18.5	Ensure 'Enable App Installer Microsoft Store Source Certificate Validation Bypass' is set to 'Disabled' (Automated)	☐	☐
18.10.18.6	Ensure 'Enable App Installer ms-appinstaller protocol' is set to 'Disabled' (Automated)	☐	☐
18.10.18.7	Ensure 'Enable Windows Package Manager command line interfaces' is set to 'Disabled' (Automated)	☐	☐
18.10.19	**Desktop Gadgets**		
18.10.20	**Desktop Window Manager**		
18.10.21	**Device and Driver Compatibility**		
18.10.22	**Device Registration (formerly Workplace Join)**		
18.10.23	**Digital Locker**		
18.10.24	**Edge UI**		
18.10.25	**Event Forwarding**		
18.10.26	**Event Log Service**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.10.26.1	**Application**		
18.10.26.1.1	Ensure 'Application: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Automated)	☐	☐
18.10.26.1.2	Ensure 'Application: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (Automated)	☐	☐
18.10.26.2	**Security**		
18.10.26.2.1	Ensure 'Security: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Automated)	☐	☐
18.10.26.2.2	Ensure 'Security: Specify the maximum log file size (KB)' is set to 'Enabled: 196,608 or greater' (Automated)	☐	☐
18.10.26.3	**Setup**		
18.10.26.3.1	Ensure 'Setup: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Automated)	☐	☐
18.10.26.3.2	Ensure 'Setup: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (Automated)	☐	☐
18.10.26.4	**System**		
18.10.26.4.1	Ensure 'System: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Automated)	☐	☐
18.10.26.4.2	Ensure 'System: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (Automated)	☐	☐
18.10.27	**Event Logging**		
18.10.28	**Event Viewer**		
18.10.29	**File Explorer (formerly Windows Explorer)**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.10.29.1	**Previous Versions**		
18.10.29.2	Ensure 'Do not apply the Mark of the Web tag to files copied from insecure sources' is set to 'Disabled' (Automated)	☐	☐
18.10.29.3	Ensure 'Turn off Data Execution Prevention for Explorer' is set to 'Disabled' (Automated)	☐	☐
18.10.29.4	Ensure 'Turn off heap termination on corruption' is set to 'Disabled' (Automated)	☐	☐
18.10.29.5	Ensure 'Turn off shell protocol protected mode' is set to 'Disabled' (Automated)	☐	☐
18.10.30	**File History**		
18.10.31	**Find My Device**		
18.10.32	**Handwriting**		
18.10.33	**HomeGroup**		
18.10.34	**Human Presence**		
18.10.35	**Internet Explorer**		
18.10.36	**Location and Sensors**		
18.10.36.1	Ensure 'Turn off location' is set to 'Enabled' (Automated)	☐	☐
18.10.37	**Maintenance Scheduler**		
18.10.38	**Maps**		
18.10.39	**MDM**		
18.10.40	**Messaging**		
18.10.40.1	Ensure 'Allow Message Service Cloud Sync' is set to 'Disabled' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.10.41	**Microsoft account**		
18.10.41.1	Ensure 'Block all consumer Microsoft account user authentication' is set to 'Enabled' (Automated)	☐	☐
18.10.42	**Microsoft Defender Antivirus (formerly Windows Defender and Windows Defender Antivirus)**		
18.10.43	**Microsoft Defender Application Guard (formerly Windows Defender Application Guard)**		
18.10.44	**Microsoft Defender Exploit Guard (formerly Windows Defender Exploit Guard)**		
18.10.45	**Microsoft Edge**		
18.10.46	**Microsoft Secondary Authentication Factor**		
18.10.47	**Microsoft User Experience Virtualization**		
18.10.48	**NetMeeting**		
18.10.49	**News and interests**		
18.10.50	**OneDrive (formerly SkyDrive)**		
18.10.51	**Online Assistance**		
18.10.52	**OOBE**		
18.10.53	**Paint**		
18.10.54	**Portable Operating System**		
18.10.55	**Presentation Settings**		
18.10.56	**Push To Install**		
18.10.56.1	Ensure 'Turn off Push To Install service' is set to 'Enabled' (Automated)	☐	☐
18.10.57	**Remote Desktop Services (formerly Terminal Services)**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.10.57.1	**RD Licensing (formerly TS Licensing)**		
18.10.57.2	**Remote Desktop Connection Client**		
18.10.57.2.1	**RemoteFX USB Device Redirection**		
18.10.57.2.2	Ensure 'Do not allow passwords to be saved' is set to 'Enabled' (Automated)	☐	☐
18.10.57.3	**Remote Desktop Session Host (formerly Terminal Server)**		
18.10.57.3.1	**Application Compatibility**		
18.10.57.3.2	**Connections**		
18.10.57.3.2.1	Ensure 'Restrict Remote Desktop Services users to a single Remote Desktop Services session' is set to 'Enabled' (Automated)	☐	☐
18.10.57.3.3	**Device and Resource Redirection**		
18.10.57.3.3.1	Ensure 'Allow UI Automation redirection' is set to 'Disabled' (Automated)	☐	☐
18.10.57.3.3.2	Ensure 'Do not allow COM port redirection' is set to 'Enabled' (Automated)	☐	☐
18.10.57.3.3.3	Ensure 'Do not allow drive redirection' is set to 'Enabled' (Automated)	☐	☐
18.10.57.3.3.4	Ensure 'Do not allow location redirection' is set to 'Enabled' (Automated)	☐	☐
18.10.57.3.3.5	Ensure 'Do not allow LPT port redirection' is set to 'Enabled' (Automated)	☐	☐
18.10.57.3.3.6	Ensure 'Do not allow supported Plug and Play device redirection' is set to 'Enabled' (Automated)	☐	☐
18.10.57.3.3.7	Ensure 'Do not allow WebAuthn redirection' is set to 'Enabled' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.10.57.3.4	**Licensing**		
18.10.57.3.5	**Printer Redirection**		
18.10.57.3.6	**Profiles**		
18.10.57.3.7	**RD Connection Broker (formerly TS Connection Broker)**		
18.10.57.3.8	**Remote Session Environment**		
18.10.57.3.9	**Security**		
18.10.57.3.9.1	Ensure 'Always prompt for password upon connection' is set to 'Enabled' (Automated)	☐	☐
18.10.57.3.9.2	Ensure 'Require secure RPC communication' is set to 'Enabled' (Automated)	☐	☐
18.10.57.3.9.3	Ensure 'Require use of specific security layer for remote (RDP) connections' is set to 'Enabled: SSL' (Automated)	☐	☐
18.10.57.3.9.4	Ensure 'Require user authentication for remote connections by using Network Level Authentication' is set to 'Enabled' (Automated)	☐	☐
18.10.57.3.9.5	Ensure 'Set client connection encryption level' is set to 'Enabled: High Level' (Automated)	☐	☐
18.10.57.3.10	**Session Time Limits**		
18.10.57.3.10.1	Ensure 'Set time limit for active but idle Remote Desktop Services sessions' is set to 'Enabled: 15 minutes or less, but not Never (0)' (Automated)	☐	☐
18.10.57.3.11	**Temporary folders**		
18.10.57.3.11.1	Ensure 'Do not delete temp folders upon exit' is set to 'Disabled' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.10.57.3.11.2	Ensure 'Do not use temporary folders per session' is set to 'Disabled' (Automated)	☐	☐
18.10.58	**RSS Feeds**		
18.10.58.1	Ensure 'Prevent downloading of enclosures' is set to 'Enabled' (Automated)	☐	☐
18.10.58.2	Ensure 'Turn on Basic feed authentication over HTTP' is set to 'Disabled' (Automated)	☐	☐
18.10.59	**Search**		
18.10.59.1	**OCR**		
18.10.59.2	Ensure 'Allow Cloud Search' is set to 'Enabled: Disable Cloud Search' (Automated)	☐	☐
18.10.59.3	Ensure 'Allow indexing of encrypted files' is set to 'Disabled' (Automated)	☐	☐
18.10.59.4	Ensure 'Allow search highlights' is set to 'Disabled' (Automated)	☐	☐
18.10.60	**Security Center**		
18.10.61	**Shutdown Options**		
18.10.62	**Smart Card**		
18.10.63	**Software Protection Platform**		
18.10.63.1	Ensure 'Turn off KMS Client Online AVS Validation' is set to 'Enabled' (Automated)	☐	☐
18.10.64	**Sound Recorder**		
18.10.65	**Speech**		
18.10.66	**Store**		
18.10.67	**Sync your settings**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.10.68	**Tablet PC**		
18.10.69	**Task Scheduler**		
18.10.70	**Tenant Restrictions**		
18.10.71	**Text Input**		
18.10.72	**Widgets**		
18.10.73	**Windows AI**		
18.10.74	**Windows Calendar**		
18.10.75	**Windows Color System**		
18.10.76	**Windows Customer Experience Improvement Program**		
18.10.77	**Windows Defender SmartScreen**		
18.10.77.1	**Enhanced Phishing Protection**		
18.10.77.2	**Explorer**		
18.10.77.2.1	Ensure 'Configure Windows Defender SmartScreen' is set to 'Enabled: Warn and prevent bypass' (Automated)	☐	☐
18.10.78	**Windows Error Reporting**		
18.10.79	**Windows Game Recording and Broadcasting**		
18.10.80	**Windows Hello for Business (formerly Microsoft Passport for Work)**		
18.10.81	**Windows Ink Workspace**		
18.10.81.1	Ensure 'Allow suggested apps in Windows Ink Workspace' is set to 'Disabled' (Automated)	☐	☐
18.10.81.2	Ensure 'Allow Windows Ink Workspace' is set to 'Enabled: On, but disallow access above lock' OR 'Enabled: Disabled' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.10.82	**Windows Installer**		
18.10.82.1	Ensure 'Allow user control over installs' is set to 'Disabled' (Automated)	☐	☐
18.10.82.2	Ensure 'Always install with elevated privileges' is set to 'Disabled' (Automated)	☐	☐
18.10.82.3	Ensure 'Prevent Internet Explorer security prompt for Windows Installer scripts' is set to 'Disabled' (Automated)	☐	☐
18.10.83	**Windows Logon Options**		
18.10.83.1	Ensure 'Configure the transmission of the user's password in the content of MPR notifications sent by winlogon.' is set to 'Disabled' (Automated)	☐	☐
18.10.83.2	Ensure 'Sign-in and lock last interactive user automatically after a restart' is set to 'Disabled' (Automated)	☐	☐
18.10.84	**Windows Media Digital Rights Management**		
18.10.85	**Windows Media Player**		
18.10.86	**Windows Messenger**		
18.10.87	**Windows Mobility Center**		
18.10.88	**Windows PowerShell**		
18.10.88.1	Ensure 'Turn on PowerShell Script Block Logging' is set to 'Enabled' (Automated)	☐	☐
18.10.88.2	Ensure 'Turn on PowerShell Transcription' is set to 'Enabled' (Automated)	☐	☐
18.10.89	**Windows Reliability Analysis**		
18.10.90	**Windows Remote Management (WinRM)**		
18.10.90.1	**WinRM Client**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.10.90.1.1	Ensure 'Allow Basic authentication' is set to 'Disabled' (Automated)	☐	☐
18.10.90.1.2	Ensure 'Allow unencrypted traffic' is set to 'Disabled' (Automated)	☐	☐
18.10.90.1.3	Ensure 'Disallow Digest authentication' is set to 'Enabled' (Automated)	☐	☐
18.10.90.2	**WinRM Service**		
18.10.90.2.1	Ensure 'Allow Basic authentication' is set to 'Disabled' (Automated)	☐	☐
18.10.90.2.2	Ensure 'Allow remote server management through WinRM' is set to 'Disabled' (Automated)	☐	☐
18.10.90.2.3	Ensure 'Allow unencrypted traffic' is set to 'Disabled' (Automated)	☐	☐
18.10.90.2.4	Ensure 'Disallow WinRM from storing RunAs credentials' is set to 'Enabled' (Automated)	☐	☐
18.10.91	**Windows Remote Shell**		
18.10.91.1	Ensure 'Allow Remote Shell Access' is set to 'Disabled' (Automated)	☐	☐
18.10.92	**Windows Sandbox**		
18.10.93	**Windows Security (formerly Windows Defender Security Center)**		
18.10.93.1	**Account protection**		
18.10.93.2	**App and browser protection**		
18.10.93.2.1	Ensure 'Prevent users from modifying settings' is set to 'Enabled' (Automated)	☐	☐
18.10.94	**Windows Update**		
18.10.94.1	**Legacy Policies**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18.10.94.1.1	Ensure 'No auto-restart with logged on users for scheduled automatic updates installations' is set to 'Disabled' (Automated)	☐	☐
18.10.94.2	**Manage end user experience**		
18.10.94.2.1	Ensure 'Configure Automatic Updates' is set to 'Enabled' (Automated)	☐	☐
18.10.94.2.2	Ensure 'Configure Automatic Updates: Scheduled install day' is set to '0 - Every day' (Automated)	☐	☐
18.10.94.3	**Manage updates offered from Windows Server Update Service**		
18.10.94.4	**Manage updates offered from Windows Update (formerly Defer Windows Updates and Windows Update for Business)**		
18.10.94.4.1	Ensure 'Manage preview builds' is set to 'Disabled' (Automated)	☐	☐
18.10.94.4.2	Ensure 'Select when Quality Updates are received' is set to 'Enabled: 0 days' (Automated)	☐	☐
18.11	**Custom Settings**		
18.11.1	Ensure 'Disable HTTP proxy features: Disable WPAD' is set to 'Enabled: Checked' (Automated)	☐	☐
18.11.2	Ensure 'Disable HTTP proxy features: Disable proxy authentication' is set to 'Enabled: Disable authentication over loopback interfaces' or higher (Automated)	☐	☐
19	**Administrative Templates (User)**		
19.1	**Control Panel**		
19.2	**Desktop**		
19.3	**Network**		
19.4	**Shared Folders**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
19.5	**Start Menu and Taskbar**		
19.5.1	**Notifications**		
19.5.1.1	Ensure 'Turn off toast notifications on the lock screen' is set to 'Enabled' (Automated)	☐	☐
19.6	**System**		
19.6.1	**Ctrl+Alt+Del Options**		
19.6.2	**Display**		
19.6.3	**Driver Installation**		
19.6.4	**Folder Redirection**		
19.6.5	**Group Policy**		
19.6.6	**Internet Communication Management**		
19.6.6.1	**Internet Communication settings**		
19.6.6.1.1	Ensure 'Turn off Help Experience Improvement Program' is set to 'Enabled' (Automated)	☐	☐
19.6.7	**Keyboard Filter**		
19.7	**Windows Components**		
19.7.1	**Account Notifications**		
19.7.2	**Add features to Windows 8 / 8.1 / 10 (formerly Windows Anytime Upgrade)**		
19.7.3	**App runtime**		
19.7.4	**Application Compatibility**		
19.7.5	**Attachment Manager**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
19.7.5.1	Ensure 'Do not preserve zone information in file attachments' is set to 'Disabled' (Automated)	☐	☐
19.7.5.2	Ensure 'Notify antivirus programs when opening attachments' is set to 'Enabled' (Automated)	☐	☐
19.7.6	**AutoPlay Policies**		
19.7.7	**Calculator**		
19.7.8	**Cloud Content**		
19.7.8.1	Ensure 'Configure Windows spotlight on lock screen' is set to 'Disabled' (Automated)	☐	☐
19.7.8.2	Ensure 'Do not suggest third-party content in Windows spotlight' is set to 'Enabled' (Automated)	☐	☐
19.7.8.3	Ensure 'Do not use diagnostic data for tailored experiences' is set to 'Enabled' (Automated)	☐	☐
19.7.8.4	Ensure 'Turn off all Windows spotlight features' is set to 'Enabled' (Automated)	☐	☐
19.7.8.5	Ensure 'Turn off Spotlight collection on Desktop' is set to 'Enabled' (Automated)	☐	☐
19.7.9	**Credential User Interface**		
19.7.10	**Data Collection and Preview Builds**		
19.7.11	**Desktop Gadgets**		
19.7.12	**Desktop Window Manager**		
19.7.13	**Digital Locker**		
19.7.14	**Edge UI**		
19.7.15	**File Explorer (formerly Windows Explorer)**		
19.7.16	**File Revocation**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
19.7.17	**IME**		
19.7.18	**Instant Search**		
19.7.19	**Internet Explorer**		
19.7.20	**Location and Sensors**		
19.7.21	**Microsoft Edge**		
19.7.22	**Microsoft Management Console**		
19.7.23	**Microsoft User Experience Virtualization**		
19.7.24	**Multitasking**		
19.7.25	**NetMeeting**		
19.7.26	**Network Sharing**		
19.7.26.1	Ensure 'Prevent users from sharing files within their profile.' is set to 'Enabled' (Automated)	☐	☐
19.7.27	**OOBE**		
19.7.28	**Presentation Settings**		
19.7.29	**Remote Desktop Services (formerly Terminal Services)**		
19.7.30	**RSS Feeds**		
19.7.31	**Search**		
19.7.32	**Snipping Tool**		
19.7.33	**Sound Recorder**		
19.7.34	**Store**		
19.7.35	**Tablet PC**		
19.7.36	**Task Scheduler**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
19.7.37	**Windows AI**		
19.7.38	**Windows Calendar**		
19.7.39	**Windows Color System**		
19.7.40	**Windows Copilot**		
19.7.41	**Windows Defender SmartScreen**		
19.7.42	**Windows Error Reporting**		
19.7.43	**Windows Hello for Business (formerly Microsoft Passport for Work)**		
19.7.44	**Windows Installer**		
19.7.45	**Windows Logon Options**		
19.7.46	**Windows Media Player**		
19.7.46.1	**Networking**		
19.7.46.2	**Playback**		
19.7.46.2.1	Ensure 'Prevent Codec Download' is set to 'Enabled' (Automated)	☐	☐

Appendix: Change History

Date: 07/28/2026 Version 5.1.0
REMOVE - Recommendations from 18.10.43 Microsoft Defender Antivirus (formerly Windows Defender and Windows Defender Antivirus) Ticket # 27270
UPDATE - 18.10.57.3.10 Ensure 'Set time limit for active but idle Remote Desktop Services sessions' is set to 'Enabled: 15 minutes or less, but not Never (0)' TO (L2 -> L1) Ticket # 27272
REMOVE - 18.10.57.3.10 Ensure 'Set time limit for disconnected sessions' is set to 'Enabled: 1 minute' Ticket # 27275
UPDATE - Controls Mappings Ticket # 28160
UPDATE - Recommendation Titles Section 18.9.26 LAPS Ticket # 28249
Date: 02/20/2026 Version: 5.0.0
UPDATE - 18.7.1 Ensure 'Allow Print Spooler to accept client connections' is set to 'Disabled' TO MS L2 -> MS L1 Ticket # 28247
UPDATE - 18.10.16 Ensure 'Enable OneSettings Auditing' is set to 'Enabled' Ticket #27156
REMOVE - 18.9.27 Ensure 'Allow Custom SSPs and APs to be loaded into LSASS' is set to 'Disabled' from MS profile Ticket #26884
UPDATE - 18.10.16 Ensure 'Limit Dump Collection' is set to 'Enabled' TO L1->L2 Ticket #26883

UPDATE - 18.10.16 Ensure 'Limit Diagnostic Log Collection' is set to 'Enabled' TO L1->L2 Ticket #26882
UPDATE - 18.9.41 Ensure 'Configure validation of ROCA-vulnerable WHfB keys during authentication' is set to 'Enabled: Audit' or higher (DC only) TO 'Block' Ticket #26881
REMOVE - 18.5 Ensure 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires' is set to 'Enabled: 5 or fewer seconds' Ticket #26880
UPDATE - 18.9.26 Ensure 'Post-authentication actions: Actions' is set to 'Enabled: Reset the password and logoff the managed account' or higher Ticket #26878
ADD - 18.11 Ensure 'Disable HTTP proxy features: Disable proxy authentication' is set to 'Enabled: Disable authentication over loopback interfaces' Ticket #26861
ADD - 18.11 Ensure 'Disable HTTP proxy features: Disable WPAD' is set to 'Enabled: Checked' Ticket #26860
ADD - 18.9.17 Ensure 'Enable / disable CLFS logfile authentication' is set to 'Enabled' Ticket #26810
UPDATE - User Section Artifacts Ticket #26553
UPDATE - Recommendation Titles Ticket #26462
REMOVE - 18.9.19 (L1) Ensure 'Configure registry policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE' Ticket #26431
REMOVE - 18.9.19 (L1) Ensure 'Configure registry policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE' Ticket #26430

REMOVE - 2.2 (L1) Ensure 'Change the time zone' is set to 'Administrators, LOCAL SERVICE, Users' Ticket #26345
REMOVE 19.7.44 (L1) Ensure 'Always install with elevated privileges' is set to 'Disabled' FROM User Section Ticket #26339
REMOVE - 18.10.16 (L1) Ensure 'Disable OneSettings Downloads' is set to 'Enabled' Ticket #26336
REMOVE - 18.9.28 (L1) Ensure 'Turn off picture password sign-in' is set to 'Enabled' Ticket #26334
REMOVE - 18.10.51 (L1) Ensure 'Prevent the usage of OneDrive for file storage' is set to 'Enabled' Ticket #26333
UPDATE - 9 (L1) Ensure 'Windows Firewall: Public: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\publicfw.log' TO is configured Ticket #26327
UPDATE - 9 (L1) Ensure 'Windows Firewall: Private: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\privatefw.log' TO is configured Ticket #26326
UPDATE - 9 (L1) Ensure 'Windows Firewall: Domain: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\domainfw.log' TO is configured Ticket #26325
REMOVE - 18.10.93.4 (L1) Ensure 'Select when Preview Builds and Feature Updates are received' is set to 'Enabled: 180 or more days' Ticket #26311
RENAME - 18.9.7 (L1) Ensure 'Prevent device metadata retrieval from the Internet' TO 'Prevent automatic download of applications associated with device metadata' Ticket #26306
UPDATE - Section changes from Windows 11 Release 25H2 Administrative Templates Ticket #26305

UPDATE - 2.3.7 (L1->L2) Ensure 'Interactive logon: Do not require CTRL+ALT+DEL' is set to 'Disabled' Ticket #26130
REMOVE - 18.4.8 (L1) Ensure 'WDigest Authentication' is set to 'Disabled' Ticket #26094
REMOVE - 2.3.11 (L1) Ensure 'Network security: LDAP client encryption requirements' is set to 'Negotiate sealing' or higher Ticket #25882
UPDATE - 17.8 (L1) Ensure 'Audit Sensitive Privilege Use' is set to 'Success and Failure' TO 'Success' Ticket #25745
REMOVE - 18.10.13 (L1) Ensure 'Turn off Microsoft consumer experiences' is set to 'Enabled' Ticket #25727
UPDATE - 18.10.43.5 (L2) Ensure 'Join Microsoft MAPS' is set to 'Disabled' TO 'L2->L1' and 'Disabled->Enabled' Ticket #25586
REMOVE - 2.3.9 (L1) Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled' Ticket #25347
REMOVE - 2.3.8 (L1) Ensure 'Microsoft network client: Digitally sign communications (if server agrees)' is set to 'Enabled' Ticket #25346
UPDATE - 2.3.10 (L1) Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled' Ticket #25334
Date: 05/23/2025 Version: 4.0.0
UPDATE - 18.9.26 Ensure 'Configures LSASS to run as a protected process' is set to 'Enabled: Enabled with UEFI Lock' Ticket #23961

ADD - 18.6.8 (L1) Ensure 'Require Encryption' is set to 'Enabled' Ticket #23960
RENAME - 18.10.82.1 (L1) Ensure 'Enable MPR notifications for the system' TO 'Configure the transmission of the user's password in the content of MPR notifications sent by winlogon.' Ticket #23764
ADD - 18.10.43.13 (L1) Ensure 'Trigger a quick scan after X days without any scans' is set to 'Enabled: 7' Ticket #23762
ADD - 18.10.43.13 (L1) Ensure 'Scan excluded files and directories during quick scans' is set to 'Enabled: 1' Ticket #23761
ADD - 18.10.43.11.1.2 (L2) Ensure 'Configure how aggressively Remote Encryption Protection blocks threats' is set to 'Enabled: Medium' or higher Ticket #23760
ADD - 18.10.43.11.1.1 (L1) Ensure 'Configure Remote Encryption Protection Mode' is set to 'Enabled: Audit' or higher Ticket #23759
ADD - 18.10.43.11.1.1 (L2) Ensure 'Configure Brute-Force Protection aggressiveness' is set to 'Enabled: Medium' or higher Ticket #23758
ADD - 18.10.43.10 (L1) Ensure 'Configure real-time protection and Security Intelligence Updates during OOBE' is set to 'Enabled' Ticket #23757
ADD - 18.10.43.8 (L2) Ensure 'Convert warn verdict to block' is set to 'Enabled' Ticket #23756
ADD - 18.10.43.4 (L1) Ensure 'Enable EDR in block mode' is set to 'Enabled' Ticket #23755

ADD - 18.10.43 (L1) Ensure 'Control whether exclusions are visible to local users' is set to 'Enabled' Ticket #23754
ADD - 18.10.29 (L1) Ensure 'Do not apply the Mark of the Web tag to files copied from insecure sources' is set to 'Disabled' Ticket #23753
ADD - 18.10.18 (L2) Ensure 'Enable Windows Package Manager command line interfaces' is set to 'Disabled' Ticket #23752
ADD - 18.10.18 (L1) Ensure 'Enable App Installer Microsoft Store Source Certificate Validation Bypass' is set to 'Disabled' Ticket #23751
ADD - 18.10.18 (L1) Ensure 'Enable App Installer Local Archive Malware Scan Override' is set to 'Disabled' Ticket #23750
MOVE - 18.4.1 (L1) Ensure 'Configure RPC packet level privacy setting for incoming connections' is set to 'Enabled' TO 18.7 Ticket #23724
ADD - 18.6.7 (L1) Ensure 'Mandate the minimum version of SMB' is set to 'Enabled: 3.1.1' Ticket #23714
ADD - 18.6.4 (L2) Ensure 'Turn off default IPv6 DNS Servers' is set to 'Enabled' Ticket #23708
ADD - 18.6.4 (L1) Ensure 'Configure multicast DNS (mDNS) protocol' is set to 'Disabled' Ticket #23707
UPDATE - User Overview (Section 19) Ticket #23605

REMOVE - 2.3.1 (L1) Ensure 'Accounts: Block Microsoft accounts' is set to 'Users can't add or log on with Microsoft accounts' Ticket #23560
UPDATE - 18.4 (L1) Ensure 'Enable Certificate Padding' TO Allow REG_DWORD or REG_SZ Ticket #23527
ADD - 18.10.58 (L1) Ensure 'Turn on Basic feed authentication over HTTP' is set to 'Disabled' Ticket #23024
UPDATE - Section changes from Windows 11 Release 24H2 Administrative Templates Ticket #22776
UPDATE - 18.10.42.6.1 (L1) Ensure 'Configure Attack Surface Reduction rules: Set the state for each ASR rule' is configured Ticket #22565
UPDATE - Section changes from Windows 11 Release 23H2 v2.0 Administrative Templates Ticket #22040
REMOVE - 18.10.15 (L1) Ensure 'Toggle user control over Insider builds' is set to 'Disabled' Ticket #21817
UPDATE - 18.10.17 (L1 -> L2) Ensure 'Enable App Installer' is set to 'Disabled' Ticket #21676
UPDATE - 18.4 (L1) Ensure 'Enable Certificate Padding' is set to 'Enabled' Ticket #21625
RENAME 2.3.10 Configure 'Network access: Remotely accessible registry paths and sub-paths' is configured TO Ensure 'Network access: Remotely accessible registry paths and sub-paths' is configured Ticket #21581

RENAME - 2.3.10 Configure 'Network access: Remotely accessible registry paths' is configured TO Ensure 'Network access: Remotely accessible registry paths' is configured Ticket #21580
RENAME - 2.3.10 Configure 'Network access: Named Pipes that can be accessed anonymously' (MS only) TO Ensure 'Network access: Named Pipes that can be accessed anonymously' is configured (MS only) Ticket #21579
RENAME - 2.3.10 Configure 'Network access: Named Pipes that can be accessed anonymously' (DC only) TO Ensure 'Network access: Named Pipes that can be accessed anonymously' is configured (DC only) Ticket #21578
UPDATE - Section 17 Auditpol commands to use Policy GUIDs Ticket #21446
UPDATE - General Overview and Intended Audience Section Ticket #24012
REMOVE - 18.10.42 Ensure 'Turn off Microsoft Defender AntiVirus' is set to 'Disabled' Ticket #14183
REMOVE - 18.6.4 (L1) Ensure ‘Configure DNS over HTTPS (DoH) name resolution' is set to 'Enabled: Allow DoH' or higher Ticket #24182
Date: 03/19/2024 Version: 3.0.0
UPDATE - 18.9.50.1 (L2 -> L1) Ensure 'Enable Windows NTP Client' is set to 'Enabled' Ticket #18467
UPDATE - 18.9.50.1 (L2 -> L1) Ensure 'Enable Windows NTP Server' is set to 'Disabled' Ticket #18468
UPDATE - 9 Windows Firewall with Advanced Security TO Windows Defender Firewall with Advanced Security Ticket #18532

UPDATE - 18.10.42.7 (L2 -> L1) Ensure 'Enable file hash computation feature' is set to 'Enabled' Ticket #19207
ADD - 18.9.19 (L1) 'Configure security policy processing: Do not apply during periodic background processing' is set to 'False' Ticket #19358
ADD - 18.9.19 (L1) 'Configure security policy processing: Process even if the Group Policy objects have not changed' is set to 'True' Ticket #19359
REMOVE - 19.1.3 Accepted (L1) Ensure 'Password protect the screen saver' is set to 'Enabled' Ticket #19361
REMOVE - 19.1.3 Accepted (L1) Ensure 'Screen saver timeout' is set to 'Enabled: 900 seconds or fewer, but not 0' Ticket #19362
ADD - 2.3.11 (L1) Ensure 'Network security: Restrict NTLM: Audit Incoming NTLM Traffic' is set to 'Enable auditing for all accounts' Ticket #19740
ADD - 2.3.11 (L1) Ensure 'Network security: Restrict NTLM: Audit NTLM authentication in this domain' is set to 'Enable all' (DC only) Ticket #19741
ADD - 2.3.11 (L1) Ensure 'Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers' is set to 'Audit all' or higher Ticket #19742
REMOVE - 2.3.4 (L1) Ensure 'Devices: Allowed to format and eject removable media' is set Ticket #20103
UPDATE - Section changes from Windows 11 Release 22H2 v3.0 Administrative Templates Ticket #20220

UPDATE - Section changes from Windows 11 Release 23H2 Administrative Templates Ticket #20324
ADD - 18.9.25 (L1) Ensure 'Configure password backup directory' is set to 'Enabled: Active Directory' or 'Enabled: Azure Active Directory' Ticket #20329
ADD - 18.9.25 (L1) Ensure 'Do not allow password expiration time longer than required by policy' is set to 'Enabled' Ticket #20330
ADD - 18.9.25 (L1) Ensure 'Enable password encryption' is set to 'Enabled' Ticket #20331
ADD - 18.9.25 (L1) Ensure 'Password Settings: Password Complexity' is set to 'Enabled: Large letters + small letters + numbers + special characters' Ticket #20332
ADD - 18.9.25 (L1) Ensure 'Password Settings: Password Length' is set to 'Enabled: 15 or more' Ticket #20333
ADD - 18.9.25 (L1) Ensure 'Password Settings: Password Age (Days)' is set to 'Enabled: 30 or fewer' Ticket #20334
ADD - 18.9.25 (L1) Ensure 'Post-authentication actions: Grace period (hours)' is set to 'Enabled: 8 or fewer hours, but not 0' Ticket #20335
ADD - 18.9.25 (L1) Ensure 'Post-authentication actions: Actions' is set to 'Enabled: Reset the password and logoff the managed account' or higher Ticket #20336
ADD - 18.10.42.13 (L1) Ensure 'Scan packed executables' is set to 'Enabled' Ticket #20337
UPDATE - 2.2 (L1) Ensure 'Allow log on locally' is set to 'Administrators' TO 'Administrators, ENTERPRISE DOMAIN CONTROLLERS' (DC only) Ticket #20339

UPDATE - 18.5 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' TO 'MSS: (AutoAdminLogon) Enable Automatic Logon' Ticket #20355
UPDATE - 18.5 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' TO 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level' Ticket #20357
UPDATE - 18.5 'MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)' TO 'MSS: (DisableIPSourceRouting) IP source routing protection level' Ticket #20358
UPDATE - 18.5 'MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)' TO 'MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses' Ticket #23059
UPDATE - 18.5 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' TO 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode' Ticket #20360
UPDATE - 18.5 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)' TO 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires' Ticket #20361
UPDATE - 18.5 'MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds' is set to 'Enabled: 300,000 or 5 minutes (recommended)' TO 'Enabled: 300,000 or 5 minutes' Ticket #20362
REMOVE - 18.10.24 EMET Ticket #20472
ADD - 18.4 (L1) Ensure 'Enable Certificate Padding' is set to 'Enabled' Ticket #20521

REMOVE - 9.1 (L1) Ensure 'Windows Firewall: Domain: Outbound connections' is set to 'Allow (default)' Ticket #20526
REMOVE - 9.2 (L1) Ensure 'Windows Firewall: Private: Outbound connections' is set to 'Allow (default)' Ticket #20527
REMOVE - 9.3 (L1) Ensure 'Windows Firewall: Public: Outbound connections' is set to 'Allow (default)' Ticket #20528
REMOVE - 18.3 (L1) Ensure LAPS AdmPwd GPO Extension / CSE is installed Ticket #20588
REMOVE - 18.3 (L1) Ensure 'Do not allow password expiration time longer than required by policy' is set to 'Enabled' Ticket #20589
REMOVE - 18.3 (L1) Ensure 'Enable Local Admin Password Management' is set to 'Enabled' Ticket #20590
REMOVE - 18.3 (L1) Ensure 'Password Settings: Password Complexity' is set to 'Enabled: Large letters + small letters + numbers + special characters' Ticket #20591
REMOVE - 18.3 (L1) Ensure 'Password Settings: Password Length' is set to 'Enabled: 15 or more' Ticket #20592
REMOVE - 18.3 (L1) Ensure 'Password Settings: Password Age (Days)' is set to 'Enabled: 30 or fewer' Ticket #20593
REMOVE - 19.1.3 (L1) Ensure 'Enable screen saver' is set to 'Enabled' Ticket #20634

UPDATE - 18.10.86 (L1 -> L2) Ensure 'Turn on PowerShell Script Block Logging' is set to 'Enabled' Ticket #20717
UPDATE - 18.10.86 (L1 -> L2) Ensure 'Turn on PowerShell Transcription' is set to 'Enabled' Ticket #20718
UPDATE - 18.6.14 (L1) Ensure 'Hardened UNC Paths' is set to 'Enabled, with "Require Mutual Authentication" and "Require Integrity" for all NETLOGON and SYSVOL shares' TO add “Require Privacy” Ticket #20785
Date: 04/14/2023 Version: 2.0.0
ADD - 18.9.13 (L2) Ensure 'Turn off cloud optimized content' is set to 'Enabled' Ticket #11925
UPDATE - 18.9.89 (L1) 'Allow Windows Ink Workspace' TO 'Enabled: On, but disallow access above lock' OR 'Enabled: Disabled' Ticket #16103
UPDATE - Section changes from Windows 11 Release 22H2 Administrative Templates Ticket #17124
UPDATE – 18.10.87 (L1) 'Turn on PowerShell Transcription' is set to 'Disabled' TO 'Enabled' Ticket #17516
ADD - 1.2 (L1) Ensure 'Allow Administrator account lockout' is set to 'Enabled' Ticket #17564
REMOVE - 2.3.1 (L1) Ensure 'Accounts: Administrator account status' is set to 'Disabled' Ticket #17565
ADD - 18.4 (L1) Ensure 'Configure RPC packet level privacy setting for incoming connections' is set to 'Enabled' Ticket #17566

MOVE - 18.4 (L1) Ensure 'Limits print driver installation to Administrators' is set to 'Enabled' TO 18.7 Ticket #17567
ADD - 18.6.4 (L1) Ensure 'Configure NetBIOS settings' is set to 'Enabled: Disable NetBIOS name resolution on public networks' Ticket #17569
ADD - 18.7 (L1) Ensure 'Configure Redirection Guard' is set to 'Enabled: Redirection Guard Enabled' Ticket #17570
ADD - 18.7 (L1) Ensure 'Configure RPC connection settings: Protocol to use for outgoing RPC connections' is set to 'Enabled: RPC over TCP' Ticket #17572
ADD - 18.7 (L1) Ensure 'Configure RPC connection settings: Use authentication for outgoing RPC connections' is set to 'Enabled: Default' Ticket #17573
ADD - 18.7 (L1) Ensure 'Configure RPC listener settings: Protocols to allow for incoming RPC connections' is set to 'Enabled: RPC over TCP' Ticket #17575
ADD - 18.7 (L1) Ensure 'Configure RPC listener settings: Authentication protocol to use for incoming RPC connections' is set to 'Enabled: Negotiate' or higher Ticket #17576
ADD - 18.7 (L1) Ensure 'Manage processing of Queue-specific files' is set to 'Enabled: Limit Queue-specific files to Color profiles' Ticket #17577
ADD - 18.9.25 (L1) Ensure 'Allow Custom SSPs and APs to be loaded into LSASS' is set to 'Disabled' Ticket #17580
ADD - 18.9.25 (NG) Ensure 'Configures LSASS to run as a protected process' is set to 'Enabled: Enabled with UEFI Lock' Ticket #17582

ADD - 18.10.17 (L1) Ensure 'Enable App Installer' is set to 'Disabled' Ticket #17583
ADD - 18.10.17 (L1) Ensure 'Enable App Installer Experimental Features' is set to 'Disabled' Ticket #17584
ADD - 18.10.17 (L1) Ensure 'Enable App Installer Hash Override' is set to 'Disabled' Ticket #17585
ADD - 18.10.17 (L1) Ensure 'Enable App Installer ms-appinstaller protocol' is set to 'Disabled' Ticket #17586
UPDATE - 18.10.43.6.1 (L1) Ensure 'Configure Attack Surface Reduction rules' with additional ASR rule for "Block abuse of exploited vulnerable signed drivers" Ticket #17588
ADD - 18.10.57.3.3 (L2) Ensure 'Do not allow WebAuthn redirection' is set to 'Enabled' Ticket #17590
ADD - 18.10.59 (L2) Ensure 'Allow search highlights' is set to 'Disabled' Ticket #17591
ADD - 18.10.82 (L1) Ensure 'Enable MPR notifications for the system' is set to 'Disabled' Ticket #17597
ADD - 18.7 (L1) Ensure 'Configure RPC over TCP port' is set to 'Enabled: 0' Ticket #17715
Date: 02/14/2022 Version: 1.0.0
Initial Public Release