

CIS Microsoft Windows 11 Enterprise Benchmark

v1.0.0 - 02-14-2022

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/>

Table of Contents

Terms of Use	1
Overview	48
Intended Audience.....	48
Consensus Guidance.....	49
Typographical Conventions	50
Assessment Status.....	50
Profile Definitions	51
Acknowledgements	53
Recommendations	54
1 Account Policies	54
1.1 Password Policy.....	54
1.1.1 (L1) Ensure 'Enforce password history' is set to '24 or more password(s)' (Automated)	54
1.1.2 (L1) Ensure 'Maximum password age' is set to '365 or fewer days, but not 0' (Automated)	57
1.1.3 (L1) Ensure 'Minimum password age' is set to '1 or more day(s)' (Automated)	59
1.1.4 (L1) Ensure 'Minimum password length' is set to '14 or more character(s)' (Automated)	61
1.1.5 (L1) Ensure 'Password must meet complexity requirements' is set to 'Enabled' (Automated)	64
1.1.6 (L1) Ensure 'Relax minimum password length limits' is set to 'Enabled' (Automated)	67
1.1.7 (L1) Ensure 'Store passwords using reversible encryption' is set to 'Disabled' (Automated)	69
1.2 Account Lockout Policy.....	71
1.2.1 (L1) Ensure 'Account lockout duration' is set to '15 or more minute(s)' (Automated)	71
1.2.2 (L1) Ensure 'Account lockout threshold' is set to '5 or fewer invalid logon attempt(s), but not 0' (Automated)	74

1.2.3 (L1) Ensure 'Reset account lockout counter after' is set to '15 or more minute(s)' (Automated).....	77
2 Local Policies.....	80
2.1 Audit Policy.....	80
2.2 User Rights Assignment.....	81
2.2.1 (L1) Ensure 'Access Credential Manager as a trusted caller' is set to 'No One' (Automated)	81
2.2.2 (L1) Ensure 'Access this computer from the network' is set to 'Administrators, Remote Desktop Users' (Automated).....	83
2.2.3 (L1) Ensure 'Act as part of the operating system' is set to 'No One' (Automated)	85
2.2.4 (L1) Ensure 'Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE' (Automated)	87
2.2.5 (L1) Ensure 'Allow log on locally' is set to 'Administrators, Users' (Automated)	89
2.2.6 (L1) Ensure 'Allow log on through Remote Desktop Services' is set to 'Administrators, Remote Desktop Users' (Automated).....	91
2.2.7 (L1) Ensure 'Back up files and directories' is set to 'Administrators' (Automated)	93
2.2.8 (L1) Ensure 'Change the system time' is set to 'Administrators, LOCAL SERVICE' (Automated)	95
2.2.9 (L1) Ensure 'Change the time zone' is set to 'Administrators, LOCAL SERVICE, Users' (Automated)	98
2.2.10 (L1) Ensure 'Create a pagefile' is set to 'Administrators' (Automated)	99
2.2.11 (L1) Ensure 'Create a token object' is set to 'No One' (Automated) ..	100
2.2.12 (L1) Ensure 'Create global objects' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' (Automated)	102
2.2.13 (L1) Ensure 'Create permanent shared objects' is set to 'No One' (Automated)	104
2.2.14 (L1) Configure 'Create symbolic links' (Automated)	105
2.2.15 (L1) Ensure 'Debug programs' is set to 'Administrators' (Automated)	107

2.2.16 (L1) Ensure 'Deny access to this computer from the network' to include 'Guests, Local account' (Automated)	109
2.2.17 (L1) Ensure 'Deny log on as a batch job' to include 'Guests' (Automated)	111
2.2.18 (L1) Ensure 'Deny log on as a service' to include 'Guests' (Automated)	113
2.2.19 (L1) Ensure 'Deny log on locally' to include 'Guests' (Automated)....	115
2.2.20 (L1) Ensure 'Deny log on through Remote Desktop Services' to include 'Guests, Local account' (Automated)	117
2.2.21 (L1) Ensure 'Enable computer and user accounts to be trusted for delegation' is set to 'No One' (Automated)	119
2.2.22 (L1) Ensure 'Force shutdown from a remote system' is set to 'Administrators' (Automated)	121
2.2.23 (L1) Ensure 'Generate security audits' is set to 'LOCAL SERVICE, NETWORK SERVICE' (Automated)	123
2.2.24 (L1) Ensure 'Impersonate a client after authentication' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' (Automated)	125
2.2.25 (L1) Ensure 'Increase scheduling priority' is set to 'Administrators, Window Manager\Window Manager Group' (Automated).....	127
2.2.26 (L1) Ensure 'Load and unload device drivers' is set to 'Administrators' (Automated)	129
2.2.27 (L1) Ensure 'Lock pages in memory' is set to 'No One' (Automated)	131
2.2.28 (L2) Ensure 'Log on as a batch job' is set to 'Administrators' (Automated)	132
2.2.29 (L2) Configure 'Log on as a service' (Automated)	134
2.2.30 (L1) Ensure 'Manage auditing and security log' is set to 'Administrators' (Automated)	136
2.2.31 (L1) Ensure 'Modify an object label' is set to 'No One' (Automated).138	
2.2.32 (L1) Ensure 'Modify firmware environment values' is set to 'Administrators' (Automated)	139
2.2.33 (L1) Ensure 'Perform volume maintenance tasks' is set to 'Administrators' (Automated)	141

2.2.34 (L1) Ensure 'Profile single process' is set to 'Administrators' (Automated)	143
2.2.35 (L1) Ensure 'Profile system performance' is set to 'Administrators, NT SERVICE\WdiServiceHost' (Automated)	145
2.2.36 (L1) Ensure 'Replace a process level token' is set to 'LOCAL SERVICE, NETWORK SERVICE' (Automated)	147
2.2.37 (L1) Ensure 'Restore files and directories' is set to 'Administrators' (Automated)	149
2.2.38 (L1) Ensure 'Shut down the system' is set to 'Administrators, Users' (Automated)	151
2.2.39 (L1) Ensure 'Take ownership of files or other objects' is set to 'Administrators' (Automated)	153
2.3 Security Options	155
2.3.1 Accounts	155
2.3.1.1 (L1) Ensure 'Accounts: Administrator account status' is set to 'Disabled' (Automated)	155
2.3.1.2 (L1) Ensure 'Accounts: Block Microsoft accounts' is set to 'Users can't add or log on with Microsoft accounts' (Automated).....	158
2.3.1.3 (L1) Ensure 'Accounts: Guest account status' is set to 'Disabled' (Automated)	160
2.3.1.4 (L1) Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled' (Automated).....	162
2.3.1.5 (L1) Configure 'Accounts: Rename administrator account' (Automated)	164
2.3.1.6 (L1) Configure 'Accounts: Rename guest account' (Automated)	166
2.3.2 Audit.....	168
2.3.2.1 (L1) Ensure 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' is set to 'Enabled' (Automated)	168
2.3.2.2 (L1) Ensure 'Audit: Shut down system immediately if unable to log security audits' is set to 'Disabled' (Automated)	170
2.3.3 DCOM	171
2.3.4 Devices	172

2.3.4.1 (L1) Ensure 'Devices: Allowed to format and eject removable media' is set to 'Administrators and Interactive Users' (Automated)	172
2.3.4.2 (L2) Ensure 'Devices: Prevent users from installing printer drivers' is set to 'Enabled' (Automated).....	174
2.3.5 Domain controller	175
2.3.6 Domain member.....	176
2.3.6.1 (L1) Ensure 'Domain member: Digitally encrypt or sign secure channel data (always)' is set to 'Enabled' (Automated).....	176
2.3.6.2 (L1) Ensure 'Domain member: Digitally encrypt secure channel data (when possible)' is set to 'Enabled' (Automated).....	179
2.3.6.3 (L1) Ensure 'Domain member: Digitally sign secure channel data (when possible)' is set to 'Enabled' (Automated).....	181
2.3.6.4 (L1) Ensure 'Domain member: Disable machine account password changes' is set to 'Disabled' (Automated)	183
2.3.6.5 (L1) Ensure 'Domain member: Maximum machine account password age' is set to '30 or fewer days, but not 0' (Automated).....	185
2.3.6.6 (L1) Ensure 'Domain member: Require strong (Windows 2000 or later) session key' is set to 'Enabled' (Automated).....	187
2.3.7 Interactive logon	189
2.3.7.1 (L1) Ensure 'Interactive logon: Do not require CTRL+ALT+DEL' is set to 'Disabled' (Automated).....	189
2.3.7.2 (L1) Ensure 'Interactive logon: Don't display last signed-in' is set to 'Enabled' (Automated)	191
2.3.7.3 (BL) Ensure 'Interactive logon: Machine account lockout threshold' is set to '10 or fewer invalid logon attempts, but not 0' (Automated)	193
2.3.7.4 (L1) Ensure 'Interactive logon: Machine inactivity limit' is set to '900 or fewer second(s), but not 0' (Automated)	195
2.3.7.5 (L1) Configure 'Interactive logon: Message text for users attempting to log on' (Automated)	197
2.3.7.6 (L1) Configure 'Interactive logon: Message title for users attempting to log on' (Automated)	199
2.3.7.7 (L2) Ensure 'Interactive logon: Number of previous logons to cache (in case domain controller is not available)' is set to '4 or fewer logon(s)' (Automated)	201

2.3.7.8 (L1) Ensure 'Interactive logon: Prompt user to change password before expiration' is set to 'between 5 and 14 days' (Automated)	203
2.3.7.9 (L1) Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or higher (Automated).....	205
2.3.8 Microsoft network client.....	208
2.3.8.1 (L1) Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled' (Automated).....	208
2.3.8.2 (L1) Ensure 'Microsoft network client: Digitally sign communications (if server agrees)' is set to 'Enabled' (Automated).....	211
2.3.8.3 (L1) Ensure 'Microsoft network client: Send unencrypted password to third-party SMB servers' is set to 'Disabled' (Automated)	214
2.3.9 Microsoft network server	216
2.3.9.1 (L1) Ensure 'Microsoft network server: Amount of idle time required before suspending session' is set to '15 or fewer minute(s)' (Automated)..	216
2.3.9.2 (L1) Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled' (Automated).....	218
2.3.9.3 (L1) Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled' (Automated)	221
2.3.9.4 (L1) Ensure 'Microsoft network server: Disconnect clients when logon hours expire' is set to 'Enabled' (Automated).....	224
2.3.9.5 (L1) Ensure 'Microsoft network server: Server SPN target name validation level' is set to 'Accept if provided by client' or higher (Automated)	226
2.3.10 Network access	228
2.3.10.1 (L1) Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled' (Automated).....	228
2.3.10.2 (L1) Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts' is set to 'Enabled' (Automated)	230
2.3.10.3 (L1) Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled' (Automated)	232
2.3.10.4 (L1) Ensure 'Network access: Do not allow storage of passwords and credentials for network authentication' is set to 'Enabled' (Automated)....	234
2.3.10.5 (L1) Ensure 'Network access: Let Everyone permissions apply to anonymous users' is set to 'Disabled' (Automated).....	236

2.3.10.6 (L1) Ensure 'Network access: Named Pipes that can be accessed anonymously' is set to 'None' (Automated)	238
2.3.10.7 (L1) Ensure 'Network access: Remotely accessible registry paths' is configured (Automated)	240
2.3.10.8 (L1) Ensure 'Network access: Remotely accessible registry paths and sub-paths' is configured (Automated)	242
2.3.10.9 (L1) Ensure 'Network access: Restrict anonymous access to Named Pipes and Shares' is set to 'Enabled' (Automated)	245
2.3.10.10 (L1) Ensure 'Network access: Restrict clients allowed to make remote calls to SAM' is set to 'Administrators: Remote Access: Allow' (Automated)	248
2.3.10.11 (L1) Ensure 'Network access: Shares that can be accessed anonymously' is set to 'None' (Automated)	250
2.3.10.12 (L1) Ensure 'Network access: Sharing and security model for local accounts' is set to 'Classic - local users authenticate as themselves' (Automated)	252
2.3.11 Network security.....	254
2.3.11.1 (L1) Ensure 'Network security: Allow Local System to use computer identity for NTLM' is set to 'Enabled' (Automated)	254
2.3.11.2 (L1) Ensure 'Network security: Allow LocalSystem NULL session fallback' is set to 'Disabled' (Automated)	256
2.3.11.3 (L1) Ensure 'Network Security: Allow PKU2U authentication requests to this computer to use online identities' is set to 'Disabled' (Automated)	258
2.3.11.4 (L1) Ensure 'Network security: Configure encryption types allowed for Kerberos' is set to 'AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types' (Automated).....	260
2.3.11.5 (L1) Ensure 'Network security: Do not store LAN Manager hash value on next password change' is set to 'Enabled' (Automated)	263
2.3.11.6 (L1) Ensure 'Network security: Force logoff when logon hours expire' is set to 'Enabled' (Manual)	265
2.3.11.7 (L1) Ensure 'Network security: LAN Manager authentication level' is set to 'Send NTLMv2 response only. Refuse LM & NTLM' (Automated)	267
2.3.11.8 (L1) Ensure 'Network security: LDAP client signing requirements' is set to 'Negotiate signing' or higher (Automated)	270

2.3.11.9 (L1) 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)	272
2.3.11.10 (L1) 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)	274
2.3.12 Recovery console.....	275
2.3.13 Shutdown	275
2.3.14 System cryptography.....	276
2.3.14.1 (L2) Ensure 'System cryptography: Force strong key protection for user keys stored on the computer' is set to 'User is prompted when the key is first used' or higher (Automated)	276
2.3.15 System objects.....	279
2.3.15.1 (L1) Ensure 'System objects: Require case insensitivity for non-Windows subsystems' is set to 'Enabled' (Automated)	279
2.3.15.2 (L1) Ensure 'System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)' is set to 'Enabled' (Automated)	281
2.3.16 System settings	282
2.3.17 User Account Control.....	283
2.3.17.1 (L1) Ensure 'User Account Control: Admin Approval Mode for the Built-in Administrator account' is set to 'Enabled' (Automated)	283
2.3.17.2 (L1) 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' (Automated).....	285
2.3.17.3 (L1) Ensure 'User Account Control: Behavior of the elevation prompt for standard users' is set to 'Automatically deny elevation requests' (Automated)	287
2.3.17.4 (L1) Ensure 'User Account Control: Detect application installations and prompt for elevation' is set to 'Enabled' (Automated).....	289
2.3.17.5 (L1) Ensure 'User Account Control: Only elevate UIAccess applications that are installed in secure locations' is set to 'Enabled' (Automated)	291
2.3.17.6 (L1) Ensure 'User Account Control: Run all administrators in Admin Approval Mode' is set to 'Enabled' (Automated)	293

2.3.17.7 (L1) Ensure 'User Account Control: Switch to the secure desktop when prompting for elevation' is set to 'Enabled' (Automated).....	295
2.3.17.8 (L1) Ensure 'User Account Control: Virtualize file and registry write failures to per-user locations' is set to 'Enabled' (Automated)	297
3 Event Log	298
4 Restricted Groups.....	298
5 System Services.....	299
5.1 (L2) Ensure 'Bluetooth Audio Gateway Service (BTAGService)' is set to 'Disabled' (Automated)	299
5.2 (L2) Ensure 'Bluetooth Support Service (bthserv)' is set to 'Disabled' (Automated)	301
5.3 (L1) Ensure 'Computer Browser (Browser)' is set to 'Disabled' or 'Not Installed' (Automated)	303
5.4 (L2) Ensure 'Downloaded Maps Manager (MapsBroker)' is set to 'Disabled' (Automated)	305
5.5 (L2) Ensure 'Geolocation Service (lfsvc)' is set to 'Disabled' (Automated)	307
5.6 (L1) Ensure 'IIS Admin Service (IISADMIN)' is set to 'Disabled' or 'Not Installed' (Automated)	309
5.7 (L1) Ensure 'Infrared monitor service (irmon)' is set to 'Disabled' or 'Not Installed' (Automated)	311
5.8 (L1) Ensure 'Internet Connection Sharing (ICS) (SharedAccess)' is set to 'Disabled' (Automated)	313
5.9 (L2) Ensure 'Link-Layer Topology Discovery Mapper (lltdsvc)' is set to 'Disabled' (Automated)	315
5.10 (L1) Ensure 'LxssManager (LxssManager)' is set to 'Disabled' or 'Not Installed' (Automated)	317
5.11 (L1) Ensure 'Microsoft FTP Service (FTPSVC)' is set to 'Disabled' or 'Not Installed' (Automated)	319
5.12 (L2) Ensure 'Microsoft iSCSI Initiator Service (MSiSCSI)' is set to 'Disabled' (Automated)	321
5.13 (L1) Ensure 'OpenSSH SSH Server (sshd)' is set to 'Disabled' or 'Not Installed' (Automated)	323

5.14 (L2) Ensure 'Peer Name Resolution Protocol (PNRPsvc)' is set to 'Disabled' (Automated)	325
5.15 (L2) Ensure 'Peer Networking Grouping (p2psvc)' is set to 'Disabled' (Automated)	327
5.16 (L2) Ensure 'Peer Networking Identity Manager (p2pimsvc)' is set to 'Disabled' (Automated)	329
5.17 (L2) Ensure 'PNRP Machine Name Publication Service (PNRPAutoReg)' is set to 'Disabled' (Automated).....	331
5.18 (L2) Ensure 'Print Spooler (Spooler)' is set to 'Disabled' (Automated)	333
5.19 (L2) Ensure 'Problem Reports and Solutions Control Panel Support (wercplsupport)' is set to 'Disabled' (Automated).....	335
5.20 (L2) Ensure 'Remote Access Auto Connection Manager (RasAuto)' is set to 'Disabled' (Automated)	337
5.21 (L2) Ensure 'Remote Desktop Configuration (SessionEnv)' is set to 'Disabled' (Automated)	339
5.22 (L2) Ensure 'Remote Desktop Services (TermService)' is set to 'Disabled' (Automated)	341
5.23 (L2) Ensure 'Remote Desktop Services UserMode Port Redirector (UmRdpService)' is set to 'Disabled' (Automated).....	343
5.24 (L1) Ensure 'Remote Procedure Call (RPC) Locator (RpcLocator)' is set to 'Disabled' (Automated)	345
5.25 (L2) Ensure 'Remote Registry (RemoteRegistry)' is set to 'Disabled' (Automated)	347
5.26 (L1) Ensure 'Routing and Remote Access (RemoteAccess)' is set to 'Disabled' (Automated)	349
5.27 (L2) Ensure 'Server (LanmanServer)' is set to 'Disabled' (Automated)	351
5.28 (L1) Ensure 'Simple TCP/IP Services (simptcp)' is set to 'Disabled' or 'Not Installed' (Automated).....	353
5.29 (L2) Ensure 'SNMP Service (SNMP)' is set to 'Disabled' or 'Not Installed' (Automated)	355
5.30 (L1) Ensure 'Special Administration Console Helper (sacsrvr)' is set to 'Disabled' or 'Not Installed' (Automated)	357

5.31 (L1) Ensure 'SSDP Discovery (SSDPSRV)' is set to 'Disabled' (Automated)	359
5.32 (L1) Ensure 'UPnP Device Host (upnphost)' is set to 'Disabled' (Automated)	361
5.33 (L1) Ensure 'Web Management Service (WMSvc)' is set to 'Disabled' or 'Not Installed' (Automated)	363
5.34 (L2) Ensure 'Windows Error Reporting Service (WerSvc)' is set to 'Disabled' (Automated)	365
5.35 (L2) Ensure 'Windows Event Collector (Webservice)' is set to 'Disabled' (Automated)	367
5.36 (L1) Ensure 'Windows Media Player Network Sharing Service (WMPNetworkSvc)' is set to 'Disabled' or 'Not Installed' (Automated)	369
5.37 (L1) Ensure 'Windows Mobile Hotspot Service (icssvc)' is set to 'Disabled' (Automated)	371
5.38 (L2) Ensure 'Windows Push Notifications System Service (WpnService)' is set to 'Disabled' (Automated)	373
5.39 (L2) Ensure 'Windows PushToInstall Service (PushToInstall)' is set to 'Disabled' (Automated)	375
5.40 (L2) Ensure 'Windows Remote Management (WS-Management) (WinRM)' is set to 'Disabled' (Automated)	377
5.41 (L1) Ensure 'World Wide Web Publishing Service (W3SVC)' is set to 'Disabled' or 'Not Installed' (Automated)	379
5.42 (L1) Ensure 'Xbox Accessory Management Service (XboxGipSvc)' is set to 'Disabled' (Automated)	381
5.43 (L1) Ensure 'Xbox Live Auth Manager (XblAuthManager)' is set to 'Disabled' (Automated)	383
5.44 (L1) Ensure 'Xbox Live Game Save (XblGameSave)' is set to 'Disabled' (Automated)	385
5.45 (L1) Ensure 'Xbox Live Networking Service (XboxNetApiSvc)' is set to 'Disabled' (Automated)	387
6 Registry.....	388
7 File System	388
8 Wired Network (IEEE 802.3) Policies	388

9 Windows Defender Firewall with Advanced Security (formerly Windows Firewall with Advanced Security).....	389
9.1 Domain Profile.....	389
9.1.1 (L1) Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)' (Automated)	389
9.1.2 (L1) Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)' (Automated).....	391
9.1.3 (L1) Ensure 'Windows Firewall: Domain: Outbound connections' is set to 'Allow (default)' (Automated)	393
9.1.4 (L1) Ensure 'Windows Firewall: Domain: Settings: Display a notification' is set to 'No' (Automated)	395
9.1.5 (L1) Ensure 'Windows Firewall: Domain: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\domainfw.log' (Automated)	397
9.1.6 (L1) Ensure 'Windows Firewall: Domain: Logging: Size limit (KB)' is set to '16,384 KB or greater' (Automated)	399
9.1.7 (L1) Ensure 'Windows Firewall: Domain: Logging: Log dropped packets' is set to 'Yes' (Automated)	401
9.1.8 (L1) Ensure 'Windows Firewall: Domain: Logging: Log successful connections' is set to 'Yes' (Automated)	403
9.2 Private Profile.....	405
9.2.1 (L1) Ensure 'Windows Firewall: Private: Firewall state' is set to 'On (recommended)' (Automated)	405
9.2.2 (L1) Ensure 'Windows Firewall: Private: Inbound connections' is set to 'Block (default)' (Automated).....	407
9.2.3 (L1) Ensure 'Windows Firewall: Private: Outbound connections' is set to 'Allow (default)' (Automated)	409
9.2.4 (L1) Ensure 'Windows Firewall: Private: Settings: Display a notification' is set to 'No' (Automated)	411
9.2.5 (L1) Ensure 'Windows Firewall: Private: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\privatefw.log' (Automated).....	413
9.2.6 (L1) Ensure 'Windows Firewall: Private: Logging: Size limit (KB)' is set to '16,384 KB or greater' (Automated)	415

9.2.7 (L1) Ensure 'Windows Firewall: Private: Logging: Log dropped packets' is set to 'Yes' (Automated)	417
9.2.8 (L1) Ensure 'Windows Firewall: Private: Logging: Log successful connections' is set to 'Yes' (Automated)	419
9.3 Public Profile	421
9.3.1 (L1) Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)' (Automated)	421
9.3.2 (L1) Ensure 'Windows Firewall: Public: Inbound connections' is set to 'Block (default)' (Automated).....	423
9.3.3 (L1) Ensure 'Windows Firewall: Public: Outbound connections' is set to 'Allow (default)' (Automated)	425
9.3.4 (L1) Ensure 'Windows Firewall: Public: Settings: Display a notification' is set to 'No' (Automated)	427
9.3.5 (L1) Ensure 'Windows Firewall: Public: Settings: Apply local firewall rules' is set to 'No' (Automated)	429
9.3.6 (L1) Ensure 'Windows Firewall: Public: Settings: Apply local connection security rules' is set to 'No' (Automated).....	431
9.3.7 (L1) Ensure 'Windows Firewall: Public: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\publicfw.log' (Automated)..	433
9.3.8 (L1) Ensure 'Windows Firewall: Public: Logging: Size limit (KB)' is set to '16,384 KB or greater' (Automated)	435
9.3.9 (L1) Ensure 'Windows Firewall: Public: Logging: Log dropped packets' is set to 'Yes' (Automated)	437
9.3.10 (L1) Ensure 'Windows Firewall: Public: Logging: Log successful connections' is set to 'Yes' (Automated)	439
10 Network List Manager Policies.....	441
11 Wireless Network (IEEE 802.11) Policies.....	441
12 Public Key Policies.....	441
13 Software Restriction Policies	441
14 Network Access Protection NAP Client Configuration	441
15 Application Control Policies	441
16 IP Security Policies	441
17 Advanced Audit Policy Configuration	442

17.1 Account Logon	442
17.1.1 (L1) Ensure 'Audit Credential Validation' is set to 'Success and Failure' (Automated)	442
17.2 Account Management	444
17.2.1 (L1) Ensure 'Audit Application Group Management' is set to 'Success and Failure' (Automated)	444
17.2.2 (L1) Ensure 'Audit Security Group Management' is set to include 'Success' (Automated)	446
17.2.3 (L1) Ensure 'Audit User Account Management' is set to 'Success and Failure' (Automated).....	448
17.3 Detailed Tracking	450
17.3.1 (L1) Ensure 'Audit PNP Activity' is set to include 'Success' (Automated)	450
17.3.2 (L1) Ensure 'Audit Process Creation' is set to include 'Success' (Automated)	452
17.4 DS Access	453
17.5 Logon/Logoff.....	454
17.5.1 (L1) Ensure 'Audit Account Lockout' is set to include 'Failure' (Automated)	454
17.5.2 (L1) Ensure 'Audit Group Membership' is set to include 'Success' (Automated)	456
17.5.3 (L1) Ensure 'Audit Logoff' is set to include 'Success' (Automated) ...	458
17.5.4 (L1) Ensure 'Audit Logon' is set to 'Success and Failure' (Automated)	460
17.5.5 (L1) Ensure 'Audit Other Logon/Logoff Events' is set to 'Success and Failure' (Automated).....	462
17.5.6 (L1) Ensure 'Audit Special Logon' is set to include 'Success' (Automated)	464
17.6 Object Access.....	466
17.6.1 (L1) Ensure 'Audit Detailed File Share' is set to include 'Failure' (Automated)	466
17.6.2 (L1) Ensure 'Audit File Share' is set to 'Success and Failure' (Automated)	468

17.6.3 (L1) Ensure 'Audit Other Object Access Events' is set to 'Success and Failure' (Automated).....	470
17.6.4 (L1) Ensure 'Audit Removable Storage' is set to 'Success and Failure' (Automated)	472
17.7 Policy Change	474
17.7.1 (L1) Ensure 'Audit Audit Policy Change' is set to include 'Success' (Automated)	474
17.7.2 (L1) Ensure 'Audit Authentication Policy Change' is set to include 'Success' (Automated)	476
17.7.3 (L1) Ensure 'Audit Authorization Policy Change' is set to include 'Success' (Automated)	478
17.7.4 (L1) Ensure 'Audit MPSSVC Rule-Level Policy Change' is set to 'Success and Failure' (Automated)	480
17.7.5 (L1) Ensure 'Audit Other Policy Change Events' is set to include 'Failure' (Automated)	483
17.8 Privilege Use	485
17.8.1 (L1) Ensure 'Audit Sensitive Privilege Use' is set to 'Success and Failure' (Automated).....	485
17.9 System.....	487
17.9.1 (L1) Ensure 'Audit IPsec Driver' is set to 'Success and Failure' (Automated)	487
17.9.2 (L1) Ensure 'Audit Other System Events' is set to 'Success and Failure' (Automated)	490
17.9.3 (L1) Ensure 'Audit Security State Change' is set to include 'Success' (Automated)	492
17.9.4 (L1) Ensure 'Audit Security System Extension' is set to include 'Success' (Automated)	494
17.9.5 (L1) Ensure 'Audit System Integrity' is set to 'Success and Failure' (Automated)	496
18 Administrative Templates (Computer)	498
18.1 Control Panel.....	498
18.1.1 Personalization	498
18.1.1.1 (L1) Ensure 'Prevent enabling lock screen camera' is set to 'Enabled' (Automated)	499

18.1.1.2 (L1) Ensure 'Prevent enabling lock screen slide show' is set to 'Enabled' (Automated)	501
18.1.2 Regional and Language Options	503
18.1.2.1 Handwriting personalization	503
18.1.2.2 (L1) Ensure 'Allow users to enable online speech recognition services' is set to 'Disabled' (Automated)	503
18.1.3 (L2) Ensure 'Allow Online Tips' is set to 'Disabled' (Automated)	505
18.2 LAPS	507
18.2.1 (L1) Ensure LAPS AdmPwd GPO Extension / CSE is installed (Automated)	507
18.2.2 (L1) Ensure 'Do not allow password expiration time longer than required by policy' is set to 'Enabled' (Automated)	510
18.2.3 (L1) Ensure 'Enable Local Admin Password Management' is set to 'Enabled' (Automated)	512
18.2.4 (L1) Ensure 'Password Settings: Password Complexity' is set to 'Enabled: Large letters + small letters + numbers + special characters' (Automated)	515
18.2.5 (L1) Ensure 'Password Settings: Password Length' is set to 'Enabled: 15 or more' (Automated)	518
18.2.6 (L1) Ensure 'Password Settings: Password Age (Days)' is set to 'Enabled: 30 or fewer' (Automated)	520
18.3 MS Security Guide.....	522
18.3.1 (L1) Ensure 'Apply UAC restrictions to local accounts on network logons' is set to 'Enabled' (Automated)	522
18.3.2 (L1) Ensure 'Configure SMB v1 client driver' is set to 'Enabled: Disable driver (recommended)' (Automated)	525
18.3.3 (L1) Ensure 'Configure SMB v1 server' is set to 'Disabled' (Automated)	527
18.3.4 (L1) Ensure 'Enable Structured Exception Handling Overwrite Protection (SEHOP)' is set to 'Enabled' (Automated)	529
18.3.5 (L1) Ensure 'Limits print driver installation to Administrators' is set to 'Enabled' (Automated)	531
18.3.6 (L1) Ensure 'NetBT NodeType configuration' is set to 'Enabled: P-node (recommended)' (Automated)	533

18.3.7 (L1) Ensure 'WDigest Authentication' is set to 'Disabled' (Automated)	535
18.4 MSS (Legacy)	537
18.4.1 (L1) Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled' (Automated)	537
18.4.2 (L1) Ensure 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled' (Automated).....	539
18.4.3 (L1) Ensure 'MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled' (Automated).....	541
18.4.4 (L2) Ensure 'MSS: (DisableSavePassword) Prevent the dial-up password from being saved' is set to 'Enabled' (Automated)	543
18.4.5 (L1) Ensure 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' is set to 'Disabled' (Automated)	545
18.4.6 (L2) Ensure 'MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds' is set to 'Enabled: 300,000 or 5 minutes (recommended)' (Automated)	547
18.4.7 (L1) Ensure 'MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers' is set to 'Enabled' (Automated)	549
18.4.8 (L2) Ensure 'MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)' is set to 'Disabled' (Automated)	551
18.4.9 (L1) Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' is set to 'Enabled' (Automated)	553
18.4.10 (L1) Ensure 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)' is set to 'Enabled: 5 or fewer seconds' (Automated).....	555
18.4.11 (L2) Ensure 'MSS: (TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted' is set to 'Enabled: 3' (Automated)	557
18.4.12 (L2) Ensure 'MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted' is set to 'Enabled: 3' (Automated)	559

18.4.13 (L1) 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)	561
18.5 Network.....	563
18.5.1 Background Intelligent Transfer Service (BITS).....	563
18.5.2 BranchCache	563
18.5.3 DirectAccess Client Experience Settings.....	563
18.5.4 DNS Client	564
18.5.4.1 (L1) Ensure 'Configure DNS over HTTPS (DoH) name resolution' is set to 'Enabled: Allow DoH' or higher (Automated)	564
18.5.4.2 (L1) Ensure 'Turn off multicast name resolution' is set to 'Enabled' (Automated)	567
18.5.5 Fonts.....	569
18.5.5.1 (L2) Ensure 'Enable Font Providers' is set to 'Disabled' (Automated)	569
18.5.6 Hotspot Authentication.....	571
18.5.7 Lanman Server	571
18.5.8 Lanman Workstation	572
18.5.8.1 (L1) Ensure 'Enable insecure guest logons' is set to 'Disabled' (Automated)	572
18.5.9 Link-Layer Topology Discovery	574
18.5.9.1 (L2) Ensure 'Turn on Mapper I/O (LLTDIO) driver' is set to 'Disabled' (Automated)	574
18.5.9.2 (L2) Ensure 'Turn on Responder (RSPNDR) driver' is set to 'Disabled' (Automated)	576
18.5.10 Microsoft Peer-to-Peer Networking Services.....	578
18.5.10.1 Peer Name Resolution Protocol.....	578
18.5.10.2 (L2) Ensure 'Turn off Microsoft Peer-to-Peer Networking Services' is set to 'Enabled' (Automated).....	578
18.5.11 Network Connections	580
18.5.11.1 Windows Defender Firewall (formerly Windows Firewall)	580
18.5.11.2 (L1) Ensure 'Prohibit installation and configuration of Network Bridge on your DNS domain network' is set to 'Enabled' (Automated).....	581

18.5.11.3 (L1) Ensure 'Prohibit use of Internet Connection Sharing on your DNS domain network' is set to 'Enabled' (Automated)	583
18.5.11.4 (L1) Ensure 'Require domain users to elevate when setting a network's location' is set to 'Enabled' (Automated).....	585
18.5.12 Network Connectivity Status Indicator.....	586
18.5.13 Network Isolation.....	586
18.5.14 Network Provider.....	587
18.5.14.1 (L1) Ensure 'Hardened UNC Paths' is set to 'Enabled, with "Require Mutual Authentication" and "Require Integrity" set for all NETLOGON and SYSVOL shares' (Automated).....	587
18.5.15 Offline Files	590
18.5.16 QoS Packet Scheduler.....	590
18.5.17 SNMP	590
18.5.18 SSL Configuration Settings.....	590
18.5.19 TCPIP Settings.....	591
18.5.19.1 IPv6 Transition Technologies.....	591
18.5.19.2 Parameters.....	592
18.5.19.2.1 (L2) Disable IPv6 (Ensure TCPIP6 Parameter 'DisabledComponents' is set to '0xff (255)') (Automated)	592
18.5.20 Windows Connect Now	594
18.5.20.1 (L2) Ensure 'Configuration of wireless settings using Windows Connect Now' is set to 'Disabled' (Automated)	594
18.5.20.2 (L2) Ensure 'Prohibit access of the Windows Connect Now wizards' is set to 'Enabled' (Automated).....	596
18.5.21 Windows Connection Manager	598
18.5.21.1 (L1) 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).....	598
18.5.21.2 (L1) Ensure 'Prohibit connection to non-domain networks when connected to domain authenticated network' is set to 'Enabled' (Automated)	600
18.5.22 Wireless Display.....	602
18.5.23 WLAN Service	602

18.5.23.1 WLAN Media Cost.....	602
18.5.23.2 WLAN Settings.....	603
18.5.23.2.1 (L1) Ensure 'Allow Windows to automatically connect to suggested open hotspots, to networks shared by contacts, and to hotspots offering paid services' is set to 'Disabled' (Automated).....	603
18.6 Printers.....	606
18.6.1 (L1) Ensure 'Allow Print Spooler to accept client connections' is set to 'Disabled' (Automated)	606
18.6.2 (L1) Ensure 'Point and Print Restrictions: When installing drivers for a new connection' is set to 'Enabled: Show warning and elevation prompt' (Automated)	608
18.6.3 (L1) Ensure 'Point and Print Restrictions: When updating drivers for an existing connection' is set to 'Enabled: Show warning and elevation prompt' (Automated).....	610
18.7 Start Menu and Taskbar.....	612
18.7.1 Notifications.....	612
18.7.1.1 (L2) Ensure 'Turn off notifications network usage' is set to 'Enabled' (Automated)	612
18.8 System.....	614
18.8.1 Access-Denied Assistance	614
18.8.2 App-V	614
18.8.3 Audit Process Creation.....	615
18.8.3.1 (L1) Ensure 'Include command line in process creation events' is set to 'Enabled' (Automated)	615
18.8.4 Credentials Delegation	617
18.8.4.1 (L1) Ensure 'Encryption Oracle Remediation' is set to 'Enabled: Force Updated Clients' (Automated)	617
18.8.4.2 (L1) Ensure 'Remote host allows delegation of non-exportable credentials' is set to 'Enabled' (Automated).....	619
18.8.5 Device Guard	621
18.8.5.1 (NG) Ensure 'Turn On Virtualization Based Security' is set to 'Enabled' (Automated)	621
18.8.5.2 (NG) Ensure 'Turn On Virtualization Based Security: Select Platform Security Level' is set to 'Secure Boot and DMA Protection' (Automated).....	624

18.8.5.3 (NG) Ensure 'Turn On Virtualization Based Security: Virtualization Based Protection of Code Integrity' is set to 'Enabled with UEFI lock' (Automated)	626
18.8.5.4 (NG) Ensure 'Turn On Virtualization Based Security: Require UEFI Memory Attributes Table' is set to 'True (checked)' (Automated)	629
18.8.5.5 (NG) Ensure 'Turn On Virtualization Based Security: Credential Guard Configuration' is set to 'Enabled with UEFI lock' (Automated)	631
18.8.5.6 (NG) Ensure 'Turn On Virtualization Based Security: Secure Launch Configuration' is set to 'Enabled' (Automated)	634
18.8.6 Device Health Attestation Service	635
18.8.7 Device Installation	636
18.8.7.1 Device Installation Restrictions	636
18.8.7.1.1 (BL) Ensure 'Prevent installation of devices that match any of these device IDs' is set to 'Enabled' (Automated)	637
18.8.7.1.2 (BL) Ensure 'Prevent installation of devices that match any of these device IDs: Prevent installation of devices that match any of these device IDs' is set to 'PCI\CC_0C0A' (Automated)	639
18.8.7.1.3 (BL) Ensure 'Prevent installation of devices that match any of these device IDs: Also apply to matching devices that are already installed.' is set to 'True' (checked) (Automated)	642
18.8.7.1.4 (BL) Ensure 'Prevent installation of devices using drivers that match these device setup classes' is set to 'Enabled' (Automated)	644
18.8.7.1.5 (BL) Ensure 'Prevent installation of devices using drivers that match these device setup classes: Prevent installation of devices using drivers for these device setup' is set to 'IEEE 1394 device setup classes' (Automated)	646
18.8.7.1.6 (BL) Ensure 'Prevent installation of devices using drivers that match these device setup classes: Also apply to matching devices that are already installed.' is set to 'True' (checked) (Automated)	649
18.8.7.2 (L1) Ensure 'Prevent device metadata retrieval from the Internet' is set to 'Enabled' (Automated)	651
18.8.8 Device Redirection.....	653
18.8.9 Disk NV Cache.....	653
18.8.10 Disk Quotas	653

18.8.11 Display	653
18.8.12 Distributed COM	654
18.8.13 Driver Installation	654
18.8.14 Early Launch Antimalware	655
18.8.14.1 (L1) Ensure 'Boot-Start Driver Initialization Policy' is set to 'Enabled: Good, unknown and bad but critical' (Automated)	655
18.8.15 Enhanced Storage Access	658
18.8.16 File Classification Infrastructure	658
18.8.17 File Share Shadow Copy Agent.....	658
18.8.18 File Share Shadow Copy Provider	658
18.8.19 Filesystem (formerly NTFS Filesystem)	659
18.8.20 Folder Redirection	659
18.8.21 Group Policy	660
18.8.21.1 Logging and tracing.....	660
18.8.21.2 (L1) Ensure 'Configure registry policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE' (Automated)	660
18.8.21.3 (L1) Ensure 'Configure registry policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE' (Automated)	662
18.8.21.4 (L1) Ensure 'Continue experiences on this device' is set to 'Disabled' (Automated)	664
18.8.21.5 (L1) Ensure 'Turn off background refresh of Group Policy' is set to 'Disabled' (Automated)	666
18.8.22 Internet Communication Management.....	668
18.8.22.1 Internet Communication settings	668
18.8.22.1.1 (L2) Ensure 'Turn off access to the Store' is set to 'Enabled' (Automated)	668
18.8.22.1.2 (L1) Ensure 'Turn off downloading of print drivers over HTTP' is set to 'Enabled' (Automated)	670
18.8.22.1.3 (L2) Ensure 'Turn off handwriting personalization data sharing' is set to 'Enabled' (Automated).....	672

18.8.22.1.4 (L2) Ensure 'Turn off handwriting recognition error reporting' is set to 'Enabled' (Automated)	674
18.8.22.1.5 (L2) Ensure 'Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com' is set to 'Enabled' (Automated)	676
18.8.22.1.6 (L1) Ensure 'Turn off Internet download for Web publishing and online ordering wizards' is set to 'Enabled' (Automated)	678
18.8.22.1.7 (L2) Ensure 'Turn off printing over HTTP' is set to 'Enabled' (Automated)	680
18.8.22.1.8 (L2) Ensure 'Turn off Registration if URL connection is referring to Microsoft.com' is set to 'Enabled' (Automated)	682
18.8.22.1.9 (L2) Ensure 'Turn off Search Companion content file updates' is set to 'Enabled' (Automated)	684
18.8.22.1.10 (L2) Ensure 'Turn off the "Order Prints" picture task' is set to 'Enabled' (Automated)	686
18.8.22.1.11 (L2) Ensure 'Turn off the "Publish to Web" task for files and folders' is set to 'Enabled' (Automated)	688
18.8.22.1.12 (L2) Ensure 'Turn off the Windows Messenger Customer Experience Improvement Program' is set to 'Enabled' (Automated)	690
18.8.22.1.13 (L2) Ensure 'Turn off Windows Customer Experience Improvement Program' is set to 'Enabled' (Automated)	692
18.8.22.1.14 (L2) Ensure 'Turn off Windows Error Reporting' is set to 'Enabled' (Automated)	694
18.8.23 iSCSI	696
18.8.24 KDC	696
18.8.25 Kerberos	697
18.8.25.1 (L2) Ensure 'Support device authentication using certificate' is set to 'Enabled: Automatic' (Automated)	697
18.8.26 Kernel DMA Protection	699
18.8.26.1 (BL) Ensure 'Enumeration policy for external devices incompatible with Kernel DMA Protection' is set to 'Enabled: Block All' (Automated)	699
18.8.27 Locale Services	701
18.8.27.1 (L2) Ensure 'Disallow copying of user input methods to the system account for sign-in' is set to 'Enabled' (Automated)	701
18.8.28 Logon	703

18.8.28.1 (L1) Ensure 'Block user from showing account details on sign-in' is set to 'Enabled' (Automated)	703
18.8.28.2 (L1) Ensure 'Do not display network selection UI' is set to 'Enabled' (Automated)	705
18.8.28.3 (L1) Ensure 'Do not enumerate connected users on domain-joined computers' is set to 'Enabled' (Automated)	707
18.8.28.4 (L1) Ensure 'Enumerate local users on domain-joined computers' is set to 'Disabled' (Automated)	709
18.8.28.5 (L1) Ensure 'Turn off app notifications on the lock screen' is set to 'Enabled' (Automated)	711
18.8.28.6 (L1) Ensure 'Turn off picture password sign-in' is set to 'Enabled' (Automated)	713
18.8.28.7 (L1) Ensure 'Turn on convenience PIN sign-in' is set to 'Disabled' (Automated)	715
18.8.29 Mitigation Options.....	716
18.8.30 Net Logon.....	716
18.8.31 OS Policies	717
18.8.31.1 (L2) Ensure 'Allow Clipboard synchronization across devices' is set to 'Disabled' (Automated)	717
18.8.31.2 (L2) Ensure 'Allow upload of User Activities' is set to 'Disabled' (Automated)	719
18.8.32 Performance Control Panel	720
18.8.33 PIN Complexity.....	720
18.8.34 Power Management.....	721
18.8.34.1 Button Settings.....	721
18.8.34.2 Energy Saver Settings.....	721
18.8.34.3 Hard Disk Settings	721
18.8.34.4 Notification Settings.....	721
18.8.34.5 Power Throttling Settings.....	722
18.8.34.6 Sleep Settings.....	723
18.8.34.6.1 (L1) Ensure 'Allow network connectivity during connected-standby (on battery)' is set to 'Disabled' (Automated)	723

18.8.34.6.2 (L1) Ensure 'Allow network connectivity during connected-standby (plugged in)' is set to 'Disabled' (Automated)	725
18.8.34.6.3 (BL) Ensure 'Allow standby states (S1-S3) when sleeping (on battery)' is set to 'Disabled' (Automated)	727
18.8.34.6.4 (BL) Ensure 'Allow standby states (S1-S3) when sleeping (plugged in)' is set to 'Disabled' (Automated)	729
18.8.34.6.5 (L1) Ensure 'Require a password when a computer wakes (on battery)' is set to 'Enabled' (Automated).....	731
18.8.34.6.6 (L1) Ensure 'Require a password when a computer wakes (plugged in)' is set to 'Enabled' (Automated).....	733
18.8.35 Recovery	734
18.8.36 Remote Assistance	735
18.8.36.1 (L1) Ensure 'Configure Offer Remote Assistance' is set to 'Disabled' (Automated)	735
18.8.36.2 (L1) Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled' (Automated)	737
18.8.37 Remote Procedure Call.....	739
18.8.37.1 (L1) Ensure 'Enable RPC Endpoint Mapper Client Authentication' is set to 'Enabled' (Automated).....	739
18.8.37.2 (L1) Ensure 'Restrict Unauthenticated RPC clients' is set to 'Enabled: Authenticated' (Automated)	741
18.8.38 Removable Storage Access.....	743
18.8.39 Scripts	743
18.8.40 Security Account Manager	743
18.8.41 Server Manager	743
18.8.42 Service Control Manager Settings	744
18.8.43 Shutdown.....	744
18.8.44 Shutdown Options.....	744
18.8.45 Storage Health.....	744
18.8.46 Storage Sense	745
18.8.47 System Restore	745
18.8.48 Troubleshooting and Diagnostics	745
18.8.48.1 Application Compatibility Diagnostics	745

18.8.48.2 Corrupted File Recovery.....	745
18.8.48.3 Disk Diagnostic.....	746
18.8.48.4 Fault Tolerant Heap	746
18.8.48.5 Microsoft Support Diagnostic Tool.....	747
18.8.48.5.1 (L2) Ensure 'Microsoft Support Diagnostic Tool: Turn on MSDT interactive communication with support provider' is set to 'Disabled' (Automated).....	747
18.8.48.6 MSI Corrupted File Recovery.....	749
18.8.48.7 Scheduled Maintenance.....	749
18.8.48.8 Scripted Diagnostics.....	749
18.8.48.9 Windows Boot Performance Diagnostics	749
18.8.48.10 Windows Memory Leak Diagnosis.....	750
18.8.48.11 Windows Performance PerfTrack.....	751
18.8.48.11.1 (L2) Ensure 'Enable/Disable PerfTrack' is set to 'Disabled' (Automated)	751
18.8.49 Trusted Platform Module Services	752
18.8.50 User Profiles	753
18.8.50.1 (L2) Ensure 'Turn off the advertising ID' is set to 'Enabled' (Automated)	753
18.8.51 Windows File Protection	755
18.8.52 Windows HotStart.....	755
18.8.53 Windows Time Service.....	756
18.8.53.1 Time Providers.....	756
18.8.53.1.1 (L2) Ensure 'Enable Windows NTP Client' is set to 'Enabled' (Automated)	756
18.8.53.1.2 (L2) Ensure 'Enable Windows NTP Server' is set to 'Disabled' (Automated)	758
18.9 Windows Components.....	760
18.9.1 Active Directory Federation Services.....	760
18.9.2 ActiveX Installer Service.....	760
18.9.3 Add features to Windows 8 / 8.1 / 10 (formerly Windows Anytime Upgrade)	760

18.9.4 App Package Deployment	761
18.9.4.1 (L2) Ensure 'Allow a Windows app to share application data between users' is set to 'Disabled' (Automated)	761
18.9.4.2 (L1) Ensure 'Prevent non-admin users from installing packaged Windows apps' is set to 'Enabled' (Automated)	763
18.9.5 App Privacy.....	765
18.9.5.1 (L1) Ensure 'Let Windows apps activate with voice while the system is locked' is set to 'Enabled: Force Deny' (Automated)	765
18.9.6 App runtime	767
18.9.6.1 (L1) Ensure 'Allow Microsoft accounts to be optional' is set to 'Enabled' (Automated)	767
18.9.6.2 (L2) Ensure 'Block launching Universal Windows apps with Windows Runtime API access from hosted content.' is set to 'Enabled' (Automated)	769
18.9.7 Application Compatibility.....	771
18.9.8 AutoPlay Policies	772
18.9.8.1 (L1) Ensure 'Disallow Autoplay for non-volume devices' is set to 'Enabled' (Automated)	772
18.9.8.2 (L1) Ensure 'Set the default behavior for AutoRun' is set to 'Enabled: Do not execute any autorun commands' (Automated).....	774
18.9.8.3 (L1) Ensure 'Turn off Autoplay' is set to 'Enabled: All drives' (Automated)	776
18.9.9 Backup	777
18.9.10 Biometrics	778
18.9.10.1 Facial Features	778
18.9.10.1.1 (L1) Ensure 'Configure enhanced anti-spoofing' is set to 'Enabled' (Automated)	778
18.9.11 BitLocker Drive Encryption.....	780
18.9.11.1 Fixed Data Drives	780
18.9.11.1.1 (BL) Ensure 'Allow access to BitLocker-protected fixed data drives from earlier versions of Windows' is set to 'Disabled' (Automated)	781
18.9.11.1.2 (BL) Ensure 'Choose how BitLocker-protected fixed drives can be recovered' is set to 'Enabled' (Automated)	783

18.9.11.1.3 (BL) Ensure 'Choose how BitLocker-protected fixed drives can be recovered: Allow data recovery agent' is set to 'Enabled: True' (Automated)	786
18.9.11.1.4 (BL) Ensure 'Choose how BitLocker-protected fixed drives can be recovered: Recovery Password' is set to 'Enabled: Allow 48-digit recovery password' (Automated)	788
18.9.11.1.5 (BL) Ensure 'Choose how BitLocker-protected fixed drives can be recovered: Recovery Key' is set to 'Enabled: Allow 256-bit recovery key' (Automated)	790
18.9.11.1.6 (BL) Ensure 'Choose how BitLocker-protected fixed drives can be recovered: Omit recovery options from the BitLocker setup wizard' is set to 'Enabled: True' (Automated)	792
18.9.11.1.7 (BL) Ensure 'Choose how BitLocker-protected fixed drives can be recovered: Save BitLocker recovery information to AD DS for fixed data drives' is set to 'Enabled: False' (Automated)	794
18.9.11.1.8 (BL) Ensure 'Choose how BitLocker-protected fixed drives can be recovered: Configure storage of BitLocker recovery information to AD DS' is set to 'Enabled: Backup recovery passwords and key packages' (Automated)	796
18.9.11.1.9 (BL) Ensure 'Choose how BitLocker-protected fixed drives can be recovered: Do not enable BitLocker until recovery information is stored to AD DS for fixed data drives' is set to 'Enabled: False' (Automated)	798
18.9.11.1.10 (BL) Ensure 'Configure use of hardware-based encryption for fixed data drives' is set to 'Disabled' (Automated)	800
18.9.11.1.11 (BL) Ensure 'Configure use of passwords for fixed data drives' is set to 'Disabled' (Automated)	802
18.9.11.1.12 (BL) Ensure 'Configure use of smart cards on fixed data drives' is set to 'Enabled' (Automated)	804
18.9.11.1.13 (BL) Ensure 'Configure use of smart cards on fixed data drives: Require use of smart cards on fixed data drives' is set to 'Enabled: True' (Automated)	806
18.9.11.2 Operating System Drives	808
18.9.11.2.1 (BL) Ensure 'Allow enhanced PINs for startup' is set to 'Enabled' (Automated)	808
18.9.11.2.2 (BL) Ensure 'Allow Secure Boot for integrity validation' is set to 'Enabled' (Automated)	810

18.9.11.2.3 (BL) Ensure 'Choose how BitLocker-protected operating system drives can be recovered' is set to 'Enabled' (Automated)	812
18.9.11.2.4 (BL) Ensure 'Choose how BitLocker-protected operating system drives can be recovered: Allow data recovery agent' is set to 'Enabled: False' (Automated)	815
18.9.11.2.5 (BL) Ensure 'Choose how BitLocker-protected operating system drives can be recovered: Recovery Password' is set to 'Enabled: Require 48-digit recovery password' (Automated).....	817
18.9.11.2.6 (BL) Ensure 'Choose how BitLocker-protected operating system drives can be recovered: Recovery Key' is set to 'Enabled: Do not allow 256-bit recovery key' (Automated)	819
18.9.11.2.7 (BL) Ensure 'Choose how BitLocker-protected operating system drives can be recovered: Omit recovery options from the BitLocker setup wizard' is set to 'Enabled: True' (Automated)	821
18.9.11.2.8 (BL) Ensure 'Choose how BitLocker-protected operating system drives can be recovered: Save BitLocker recovery information to AD DS for operating system drives' is set to 'Enabled: True' (Automated)	823
18.9.11.2.9 (BL) Ensure 'Choose how BitLocker-protected operating system drives can be recovered: Configure storage of BitLocker recovery information to AD DS:' is set to 'Enabled: Store recovery passwords and key packages' (Automated)	825
18.9.11.2.10 (BL) Ensure 'Choose how BitLocker-protected operating system drives can be recovered: Do not enable BitLocker until recovery information is stored to AD DS for operating system drives' is set to 'Enabled: True' (Automated)	827
18.9.11.2.11 (BL) Ensure 'Configure use of hardware-based encryption for operating system drives' is set to 'Disabled' (Automated)	830
18.9.11.2.12 (BL) Ensure 'Configure use of passwords for operating system drives' is set to 'Disabled' (Automated).....	832
18.9.11.2.13 (BL) Ensure 'Require additional authentication at startup' is set to 'Enabled' (Automated)	834
18.9.11.2.14 (BL) Ensure 'Require additional authentication at startup: Allow BitLocker without a compatible TPM' is set to 'Enabled: False' (Automated)	837
18.9.11.3 Removable Data Drives.....	839

18.9.11.3.1 (BL) Ensure 'Allow access to BitLocker-protected removable data drives from earlier versions of Windows' is set to 'Disabled' (Automated)	839
18.9.11.3.2 (BL) Ensure 'Choose how BitLocker-protected removable drives can be recovered' is set to 'Enabled' (Automated)	841
18.9.11.3.3 (BL) Ensure 'Choose how BitLocker-protected removable drives can be recovered: Allow data recovery agent' is set to 'Enabled: True' (Automated)	844
18.9.11.3.4 (BL) Ensure 'Choose how BitLocker-protected removable drives can be recovered: Recovery Password' is set to 'Enabled: Do not allow 48-digit recovery password' (Automated)	846
18.9.11.3.5 (BL) Ensure 'Choose how BitLocker-protected removable drives can be recovered: Recovery Key' is set to 'Enabled: Do not allow 256-bit recovery key' (Automated)	848
18.9.11.3.6 (BL) Ensure 'Choose how BitLocker-protected removable drives can be recovered: Omit recovery options from the BitLocker setup wizard' is set to 'Enabled: True' (Automated)	850
18.9.11.3.7 (BL) Ensure 'Choose how BitLocker-protected removable drives can be recovered: Save BitLocker recovery information to AD DS for removable data drives' is set to 'Enabled: False' (Automated)	852
18.9.11.3.8 (BL) Ensure 'Choose how BitLocker-protected removable drives can be recovered: Configure storage of BitLocker recovery information to AD DS:' is set to 'Enabled: Backup recovery passwords and key packages' (Automated)	854
18.9.11.3.9 (BL) Ensure 'Choose how BitLocker-protected removable drives can be recovered: Do not enable BitLocker until recovery information is stored to AD DS for removable data drives' is set to 'Enabled: False' (Automated)	856
18.9.11.3.10 (BL) Ensure 'Configure use of hardware-based encryption for removable data drives' is set to 'Disabled' (Automated)	858
18.9.11.3.11 (BL) Ensure 'Configure use of passwords for removable data drives' is set to 'Disabled' (Automated)	860
18.9.11.3.12 (BL) Ensure 'Configure use of smart cards on removable data drives' is set to 'Enabled' (Automated)	862
18.9.11.3.13 (BL) Ensure 'Configure use of smart cards on removable data drives: Require use of smart cards on removable data drives' is set to 'Enabled: True' (Automated)	864

18.9.11.3.14 (BL) Ensure 'Deny write access to removable drives not protected by BitLocker' is set to 'Enabled' (Automated)	866
18.9.11.3.15 (BL) Ensure 'Deny write access to removable drives not protected by BitLocker: Do not allow write access to devices configured in another organization' is set to 'Enabled: False' (Automated)	868
18.9.11.4 (BL) Ensure 'Disable new DMA devices when this computer is locked' is set to 'Enabled' (Automated)	870
18.9.12 Camera	872
18.9.12.1 (L2) Ensure 'Allow Use of Camera' is set to 'Disabled' (Automated)	872
18.9.13 Chat	873
18.9.14 Cloud Content	874
18.9.14.1 (L1) Ensure 'Turn off cloud consumer account state content' is set to 'Enabled' (Automated)	874
18.9.14.2 (L2) Ensure 'Turn off cloud optimized content' is set to 'Enabled' (Automated)	876
18.9.14.3 (L1) Ensure 'Turn off Microsoft consumer experiences' is set to 'Enabled' (Automated)	878
18.9.15 Connect	880
18.9.15.1 (L1) Ensure 'Require pin for pairing' is set to 'Enabled: First Time' OR 'Enabled: Always' (Automated)	880
18.9.16 Credential User Interface	882
18.9.16.1 (L1) Ensure 'Do not display the password reveal button' is set to 'Enabled' (Automated)	882
18.9.16.2 (L1) Ensure 'Enumerate administrator accounts on elevation' is set to 'Disabled' (Automated)	884
18.9.16.3 (L1) Ensure 'Prevent the use of security questions for local accounts' is set to 'Enabled' (Automated)	885
18.9.17 Data Collection and Preview Builds	887
18.9.17.1 (L1) Ensure 'Allow Diagnostic Data' is set to 'Enabled: Diagnostic data off (not recommended)' or 'Enabled: Send required diagnostic data' (Automated)	888

18.9.17.2 (L2) Ensure 'Configure Authenticated Proxy usage for the Connected User Experience and Telemetry service' is set to 'Enabled: Disable Authenticated Proxy usage' (Automated).....	891
18.9.17.3 (L1) Ensure 'Disable OneSettings Downloads' is set to 'Enabled' (Automated)	893
18.9.17.4 (L1) Ensure 'Do not show feedback notifications' is set to 'Enabled' (Automated)	895
18.9.17.5 (L1) Ensure 'Enable OneSettings Auditing' is set to 'Enabled' (Automated)	897
18.9.17.6 (L1) Ensure 'Limit Diagnostic Log Collection' is set to 'Enabled' (Automated)	899
18.9.17.7 (L1) Ensure 'Limit Dump Collection' is set to 'Enabled' (Automated)	901
18.9.17.8 (L1) Ensure 'Toggle user control over Insider builds' is set to 'Disabled' (Automated)	903
18.9.18 Delivery Optimization.....	905
18.9.18.1 (L1) Ensure 'Download Mode' is NOT set to 'Enabled: Internet' (Automated)	905
18.9.19 Desktop Gadgets	907
18.9.20 Desktop Window Manager.....	907
18.9.21 Device and Driver Compatibility	907
18.9.22 Device Registration (formerly Workplace Join)	908
18.9.23 Digital Locker	908
18.9.24 Edge UI.....	908
18.9.25 EMET	909
18.9.26 Event Forwarding.....	909
18.9.27 Event Log Service	910
18.9.27.1 Application.....	910
18.9.27.1.1 (L1) Ensure 'Application: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Automated)	910
18.9.27.1.2 (L1) Ensure 'Application: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (Automated).....	912
18.9.27.2 Security	914

18.9.27.2.1 (L1) Ensure 'Security: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Automated).....	914
18.9.27.2.2 (L1) Ensure 'Security: Specify the maximum log file size (KB)' is set to 'Enabled: 196,608 or greater' (Automated)	916
18.9.27.3 Setup.....	918
18.9.27.3.1 (L1) Ensure 'Setup: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Automated)	918
18.9.27.3.2 (L1) Ensure 'Setup: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (Automated)	920
18.9.27.4 System	922
18.9.27.4.1 (L1) Ensure 'System: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Automated)	922
18.9.27.4.2 (L1) Ensure 'System: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (Automated)	924
18.9.28 Event Logging.....	926
18.9.29 Event Viewer	926
18.9.30 Family Safety (formerly Parental Controls).....	926
18.9.31 File Explorer (formerly Windows Explorer)	927
18.9.31.1 Previous Versions	927
18.9.31.2 (L1) Ensure 'Turn off Data Execution Prevention for Explorer' is set to 'Disabled' (Automated)	927
18.9.31.3 (L1) Ensure 'Turn off heap termination on corruption' is set to 'Disabled' (Automated)	930
18.9.31.4 (L1) Ensure 'Turn off shell protocol protected mode' is set to 'Disabled' (Automated)	932
18.9.32 File History.....	934
18.9.33 Find My Device	934
18.9.34 Game Explorer	934
18.9.35 Handwriting.....	934
18.9.36 HomeGroup.....	935
18.9.36.1 (L1) Ensure 'Prevent the computer from joining a homegroup' is set to 'Enabled' (Automated)	935
18.9.37 Human Presence	937

18.9.38 Import Video	937
18.9.39 Internet Explorer	937
18.9.40 Internet Information Services	937
18.9.41 Location and Sensors	938
18.9.41.1 (L2) Ensure 'Turn off location' is set to 'Enabled' (Automated) ...	938
18.9.42 Maintenance Scheduler	940
18.9.43 Maps.....	940
18.9.44 MDM.....	940
18.9.45 Messaging	941
18.9.45.1 (L2) Ensure 'Allow Message Service Cloud Sync' is set to 'Disabled' (Automated)	941
18.9.46 Microsoft account	943
18.9.46.1 (L1) Ensure 'Block all consumer Microsoft account user authentication' is set to 'Enabled' (Automated).....	943
18.9.47 Microsoft Defender Antivirus (formerly Windows Defender and Windows Defender Antivirus)	945
18.9.47.1 Client Interface.....	945
18.9.47.2 Device Control	945
18.9.47.3 Exclusions	945
18.9.47.4 MAPS	946
18.9.47.4.1 (L1) Ensure 'Configure local setting override for reporting to Microsoft MAPS' is set to 'Disabled' (Automated)	946
18.9.47.4.2 (L2) Ensure 'Join Microsoft MAPS' is set to 'Disabled' (Automated)	948
18.9.47.5 Microsoft Defender Exploit Guard (formerly Windows Defender Exploit Guard).....	951
18.9.47.5.1 Attack Surface Reduction.....	951
18.9.47.5.1.1 (L1) Ensure 'Configure Attack Surface Reduction rules' is set to 'Enabled' (Automated)	951
18.9.47.5.1.2 (L1) Ensure 'Configure Attack Surface Reduction rules: Set the state for each ASR rule' is configured (Automated).....	953
18.9.47.5.2 Controlled Folder Access	956

18.9.47.5.3 Network Protection	957
18.9.47.5.3.1 (L1) Ensure 'Prevent users and apps from accessing dangerous websites' is set to 'Enabled: Block' (Automated)	957
18.9.47.6 MpEngine.....	959
18.9.47.6.1 (L2) Ensure 'Enable file hash computation feature' is set to 'Enabled' (Automated)	959
18.9.47.7 Network Inspection System	961
18.9.47.8 Quarantine	961
18.9.47.9 Real-time Protection	962
18.9.47.9.1 (L1) Ensure 'Scan all downloaded files and attachments' is set to 'Enabled' (Automated)	962
18.9.47.9.2 (L1) Ensure 'Turn off real-time protection' is set to 'Disabled' (Automated)	964
18.9.47.9.3 (L1) Ensure 'Turn on behavior monitoring' is set to 'Enabled' (Automated)	966
18.9.47.9.4 (L1) Ensure 'Turn on script scanning' is set to 'Enabled' (Automated)	968
18.9.47.10 Remediation	969
18.9.47.11 Reporting	970
18.9.47.11.1 (L2) Ensure 'Configure Watson events' is set to 'Disabled' (Automated)	970
18.9.47.12 Scan	972
18.9.47.12.1 (L1) Ensure 'Scan removable drives' is set to 'Enabled' (Automated)	972
18.9.47.12.2 (L1) Ensure 'Turn on e-mail scanning' is set to 'Enabled' (Automated)	974
18.9.47.13 Security Intelligence Updates (formerly Signature Updates)	975
18.9.47.14 Threats.....	975
18.9.47.15 (L1) Ensure 'Configure detection for potentially unwanted applications' is set to 'Enabled: Block' (Automated)	976
18.9.47.16 (L1) Ensure 'Turn off Microsoft Defender AntiVirus' is set to 'Disabled' (Automated)	978

18.9.48 Microsoft Defender Application Guard (formerly Windows Defender Application Guard).....	980
18.9.48.1 (NG) Ensure 'Allow auditing events in Microsoft Defender Application Guard' is set to 'Enabled' (Automated).....	981
18.9.48.2 (NG) Ensure 'Allow camera and microphone access in Microsoft Defender Application Guard' is set to 'Disabled' (Automated)	984
18.9.48.3 (NG) Ensure 'Allow data persistence for Microsoft Defender Application Guard' is set to 'Disabled' (Automated)	986
18.9.48.4 (NG) Ensure 'Allow files to download and save to the host operating system from Microsoft Defender Application Guard' is set to 'Disabled' (Automated)	989
18.9.48.5 (NG) Ensure 'Configure Microsoft Defender Application Guard clipboard settings: Clipboard behavior setting' is set to 'Enabled: Enable clipboard operation from an isolated session to the host' (Automated).....	992
18.9.48.6 (NG) Ensure 'Turn on Microsoft Defender Application Guard in Managed Mode' is set to 'Enabled: 1' (Automated).....	995
18.9.49 Microsoft Defender Exploit Guard (formerly Windows Defender Exploit Guard)	998
18.9.50 Microsoft Edge	998
18.9.51 Microsoft FIDO Authentication	998
18.9.52 Microsoft Secondary Authentication Factor	999
18.9.53 Microsoft User Experience Virtualization.....	999
18.9.54 NetMeeting.....	999
18.9.55 Network Access Protection.....	999
18.9.56 Network Projector.....	1000
18.9.57 News and interests.....	1001
18.9.57.1 (L2) Ensure 'Enable news and interests on the taskbar' is set to 'Disabled' (Automated)	1001
18.9.58 OneDrive (formerly SkyDrive)	1003
18.9.58.1 (L1) Ensure 'Prevent the usage of OneDrive for file storage' is set to 'Enabled' (Automated)	1003
18.9.59 Online Assistance.....	1006
18.9.60 OOBE.....	1006

18.9.61 Password Synchronization	1006
18.9.62 Portable Operating System.....	1006
18.9.63 Presentation Settings	1007
18.9.64 Push To Install	1008
18.9.64.1 (L2) Ensure 'Turn off Push To Install service' is set to 'Enabled' (Automated)	1008
18.9.65 Remote Desktop Services (formerly Terminal Services).....	1010
18.9.65.1 RD Licensing (formerly TS Licensing)	1010
18.9.65.2 Remote Desktop Connection Client	1011
18.9.65.2.1 RemoteFX USB Device Redirection.....	1011
18.9.65.2.2 (L1) Ensure 'Do not allow passwords to be saved' is set to 'Enabled' (Automated)	1012
18.9.65.3 Remote Desktop Session Host (formerly Terminal Server)	1014
18.9.65.3.1 Application Compatibility.....	1014
18.9.65.3.2 Connections.....	1015
18.9.65.3.2.1 (L2) Ensure 'Allow users to connect remotely by using Remote Desktop Services' is set to 'Disabled' (Automated).....	1015
18.9.65.3.3 Device and Resource Redirection.....	1017
18.9.65.3.3.1 (L2) Ensure 'Allow UI Automation redirection' is set to 'Disabled' (Automated)	1017
18.9.65.3.3.2 (L2) Ensure 'Do not allow COM port redirection' is set to 'Enabled' (Automated)	1019
18.9.65.3.3.3 (L1) Ensure 'Do not allow drive redirection' is set to 'Enabled' (Automated)	1021
18.9.65.3.3.4 (L2) Ensure 'Do not allow location redirection' is set to 'Enabled' (Automated)	1023
18.9.65.3.3.5 (L2) Ensure 'Do not allow LPT port redirection' is set to 'Enabled' (Automated)	1025
18.9.65.3.3.6 (L2) Ensure 'Do not allow supported Plug and Play device redirection' is set to 'Enabled' (Automated).....	1027
18.9.65.3.4 Licensing	1029
18.9.65.3.5 Printer Redirection	1029
18.9.65.3.6 Profiles	1029

18.9.65.3.7 RD Connection Broker (formerly TS Connection Broker)	1029
18.9.65.3.8 Remote Session Environment.....	1030
18.9.65.3.9 Security	1031
18.9.65.3.9.1 (L1) Ensure 'Always prompt for password upon connection' is set to 'Enabled' (Automated)	1031
18.9.65.3.9.2 (L1) Ensure 'Require secure RPC communication' is set to 'Enabled' (Automated)	1033
18.9.65.3.9.3 (L1) Ensure 'Require use of specific security layer for remote (RDP) connections' is set to 'Enabled: SSL' (Automated)	1035
18.9.65.3.9.4 (L1) Ensure 'Require user authentication for remote connections by using Network Level Authentication' is set to 'Enabled' (Automated)	1038
18.9.65.3.9.5 (L1) Ensure 'Set client connection encryption level' is set to 'Enabled: High Level' (Automated)	1040
18.9.65.3.10 Session Time Limits	1042
18.9.65.3.10.1 (L2) 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)	1042
18.9.65.3.10.2 (L2) Ensure 'Set time limit for disconnected sessions' is set to 'Enabled: 1 minute' (Automated).....	1044
18.9.65.3.11 Temporary folders.....	1046
18.9.65.3.11.1 (L1) Ensure 'Do not delete temp folders upon exit' is set to 'Disabled' (Automated)	1046
18.9.66 RSS Feeds.....	1048
18.9.66.1 (L1) Ensure 'Prevent downloading of enclosures' is set to 'Enabled' (Automated)	1048
18.9.67 Search.....	1050
18.9.67.1 OCR	1050
18.9.67.2 (L2) Ensure 'Allow Cloud Search' is set to 'Enabled: Disable Cloud Search' (Automated)	1050
18.9.67.3 (L1) Ensure 'Allow Cortana' is set to 'Disabled' (Automated)	1052
18.9.67.4 (L1) Ensure 'Allow Cortana above lock screen' is set to 'Disabled' (Automated)	1054

18.9.67.5 (L1) Ensure 'Allow indexing of encrypted files' is set to 'Disabled' (Automated)	1056
18.9.67.6 (L1) Ensure 'Allow search and Cortana to use location' is set to 'Disabled' (Automated)	1058
18.9.68 Security Center	1060
18.9.69 Server for NIS	1060
18.9.70 Shutdown Options.....	1060
18.9.71 Smart Card.....	1060
18.9.72 Software Protection Platform	1061
18.9.72.1 (L2) Ensure 'Turn off KMS Client Online AVS Validation' is set to 'Enabled' (Automated)	1061
18.9.73 Sound Recorder.....	1063
18.9.74 Speech	1063
18.9.75 Store.....	1064
18.9.75.1 (L2) Ensure 'Disable all apps from Microsoft Store' is set to 'Disabled' (Automated)	1064
18.9.75.2 (L1) Ensure 'Only display the private store within the Microsoft Store' is set to 'Enabled' (Automated).....	1067
18.9.75.3 (L1) Ensure 'Turn off Automatic Download and Install of updates' is set to 'Disabled' (Automated)	1069
18.9.75.4 (L1) Ensure 'Turn off the offer to update to the latest version of Windows' is set to 'Enabled' (Automated)	1071
18.9.75.5 (L2) Ensure 'Turn off the Store application' is set to 'Enabled' (Automated)	1073
18.9.76 Sync your settings	1075
18.9.77 Tablet PC	1075
18.9.78 Task Scheduler	1075
18.9.79 Tenant Restrictions.....	1075
18.9.80 Text Input	1076
18.9.81 Widgets.....	1077
18.9.81.1 (L1) Ensure 'Allow widgets' is set to 'Disabled' (Automated)	1077
18.9.82 Windows Calendar	1079

18.9.83 Windows Color System	1079
18.9.84 Windows Customer Experience Improvement Program.....	1079
18.9.85 Windows Defender SmartScreen	1080
18.9.85.1 Explorer	1080
18.9.85.1.1 (L1) Ensure 'Configure Windows Defender SmartScreen' is set to 'Enabled: Warn and prevent bypass' (Automated)	1080
18.9.85.2 Microsoft Edge.....	1083
18.9.85.2.1 (L1) Ensure 'Configure Windows Defender SmartScreen' is set to 'Enabled' (Automated)	1083
18.9.85.2.2 (L1) Ensure 'Prevent bypassing Windows Defender SmartScreen prompts for sites' is set to 'Enabled' (Automated).....	1085
18.9.86 Windows Error Reporting.....	1087
18.9.87 Windows Game Recording and Broadcasting.....	1088
18.9.87.1 (L1) Ensure 'Enables or disables Windows Game Recording and Broadcasting' is set to 'Disabled' (Automated).....	1088
18.9.88 Windows Hello for Business (formerly Microsoft Passport for Work)	1089
18.9.89 Windows Ink Workspace.....	1090
18.9.89.1 (L2) Ensure 'Allow suggested apps in Windows Ink Workspace' is set to 'Disabled' (Automated).....	1090
18.9.89.2 (L1) Ensure 'Allow Windows Ink Workspace' is set to 'Enabled: On, but disallow access above lock' OR 'Disabled' but not 'Enabled: On' (Automated)	1092
18.9.90 Windows Installer	1094
18.9.90.1 (L1) Ensure 'Allow user control over installs' is set to 'Disabled' (Automated)	1094
18.9.90.2 (L1) Ensure 'Always install with elevated privileges' is set to 'Disabled' (Automated)	1096
18.9.90.3 (L2) Ensure 'Prevent Internet Explorer security prompt for Windows Installer scripts' is set to 'Disabled' (Automated)	1098
18.9.91 Windows Logon Options.....	1100
18.9.91.1 (L1) Ensure 'Sign-in and lock last interactive user automatically after a restart' is set to 'Disabled' (Automated)	1100
18.9.92 Windows Mail	1102

18.9.93 Windows Media Center	1102
18.9.94 Windows Media Digital Rights Management.....	1102
18.9.95 Windows Media Player.....	1102
18.9.96 Windows Meeting Space.....	1103
18.9.97 Windows Messenger	1103
18.9.98 Windows Mobility Center.....	1103
18.9.99 Windows Movie Maker.....	1103
18.9.100 Windows PowerShell	1104
18.9.100.1 (L1) Ensure 'Turn on PowerShell Script Block Logging' is set to 'Enabled' (Automated)	1104
18.9.100.2 (L1) Ensure 'Turn on PowerShell Transcription' is set to 'Disabled' (Automated)	1107
18.9.101 Windows Reliability Analysis.....	1108
18.9.102 Windows Remote Management (WinRM)	1109
18.9.102.1 WinRM Client	1109
18.9.102.1.1 (L1) Ensure 'Allow Basic authentication' is set to 'Disabled' (Automated)	1109
18.9.102.1.2 (L1) Ensure 'Allow unencrypted traffic' is set to 'Disabled' (Automated)	1111
18.9.102.1.3 (L1) Ensure 'Disallow Digest authentication' is set to 'Enabled' (Automated)	1113
18.9.102.2 WinRM Service	1115
18.9.102.2.1 (L1) Ensure 'Allow Basic authentication' is set to 'Disabled' (Automated)	1115
18.9.102.2.2 (L2) Ensure 'Allow remote server management through WinRM' is set to 'Disabled' (Automated).....	1117
18.9.102.2.3 (L1) Ensure 'Allow unencrypted traffic' is set to 'Disabled' (Automated)	1119
18.9.102.2.4 (L1) Ensure 'Disallow WinRM from storing RunAs credentials' is set to 'Enabled' (Automated).....	1121
18.9.103 Windows Remote Shell.....	1123
18.9.103.1 (L2) Ensure 'Allow Remote Shell Access' is set to 'Disabled' (Automated)	1123

18.9.104 Windows Sandbox	1125
18.9.104.1 (L1) Ensure 'Allow clipboard sharing with Windows Sandbox' is set to 'Disabled' (Automated)	1125
18.9.104.2 (L1) Ensure 'Allow networking in Windows Sandbox' is set to 'Disabled' (Automated)	1127
18.9.105 Windows Security (formerly Windows Defender Security Center).....	1129
18.9.105.1 Account protection.....	1129
18.9.105.2 App and browser protection	1130
18.9.105.2.1 (L1) Ensure 'Prevent users from modifying settings' is set to 'Enabled' (Automated)	1130
18.9.106 Windows SideShow.....	1132
18.9.107 Windows System Resource Manager	1132
18.9.108 Windows Update.....	1133
18.9.108.1 Legacy Policies.....	1133
18.9.108.1.1 (L1) Ensure 'No auto-restart with logged on users for scheduled automatic updates installations' is set to 'Disabled' (Automated).....	1133
18.9.108.2 Manage end user experience.....	1136
18.9.108.2.1 (L1) Ensure 'Configure Automatic Updates' is set to 'Enabled' (Automated)	1137
18.9.108.2.2 (L1) Ensure 'Configure Automatic Updates: Scheduled install day' is set to '0 - Every day' (Automated)	1140
18.9.108.2.3 (L1) Ensure 'Remove access to "Pause updates" feature' is set to 'Enabled' (Automated)	1142
18.9.108.3 Manage updates offered from Windows Server Update Service	1143
18.9.108.4 Manage updates offered from Windows Update (formerly Defer Windows Updates and Windows Update for Business)	1144
18.9.108.4.1 (L1) Ensure 'Manage preview builds' is set to 'Disabled' (Automated)	1145
18.9.108.4.2 (L1) Ensure 'Select when Preview Builds and Feature Updates are received' is set to 'Enabled: 180 or more days' (Automated)	1147
18.9.108.4.3 (L1) Ensure 'Select when Quality Updates are received' is set to 'Enabled: 0 days' (Automated)	1150
19 Administrative Templates (User)	1152

19.1 Control Panel.....	1152
19.1.1 Add or Remove Programs.....	1152
19.1.2 Display.....	1152
19.1.3 Personalization (formerly Desktop Themes).....	1153
19.1.3.1 (L1) Ensure 'Enable screen saver' is set to 'Enabled' (Automated)	1153
19.1.3.2 (L1) Ensure 'Password protect the screen saver' is set to 'Enabled' (Automated)	1155
19.1.3.3 (L1) Ensure 'Screen saver timeout' is set to 'Enabled: 900 seconds or fewer, but not 0' (Automated).....	1157
19.2 Desktop.....	1159
19.3 Network.....	1159
19.4 Shared Folders.....	1159
19.5 Start Menu and Taskbar.....	1160
19.5.1 Notifications	1160
19.5.1.1 (L1) Ensure 'Turn off toast notifications on the lock screen' is set to 'Enabled' (Automated)	1160
19.6 System.....	1162
19.6.1 Ctrl+Alt+Del Options.....	1162
19.6.2 Display.....	1162
19.6.3 Driver Installation.....	1162
19.6.4 Folder Redirection.....	1162
19.6.5 Group Policy	1163
19.6.6 Internet Communication Management.....	1164
19.6.6.1 Internet Communication settings.....	1164
19.6.6.1.1 (L2) Ensure 'Turn off Help Experience Improvement Program' is set to 'Enabled' (Automated)	1164
19.7 Windows Components.....	1166
19.7.1 Add features to Windows 8 / 8.1 / 10 (formerly Windows Anytime Upgrade)	1166
19.7.2 App runtime	1166
19.7.3 Application Compatibility.....	1166

19.7.4 Attachment Manager	1167
19.7.4.1 (L1) Ensure 'Do not preserve zone information in file attachments' is set to 'Disabled' (Automated).....	1167
19.7.4.2 (L1) Ensure 'Notify antivirus programs when opening attachments' is set to 'Enabled' (Automated).....	1169
19.7.5 AutoPlay Policies	1171
19.7.6 Backup	1171
19.7.7 Calculator	1171
19.7.8 Cloud Content	1172
19.7.8.1 (L1) Ensure 'Configure Windows spotlight on lock screen' is set to 'Disabled' (Automated)	1172
19.7.8.2 (L1) Ensure 'Do not suggest third-party content in Windows spotlight' is set to 'Enabled' (Automated)	1174
19.7.8.3 (L2) Ensure 'Do not use diagnostic data for tailored experiences' is set to 'Enabled' (Automated)	1176
19.7.8.4 (L2) Ensure 'Turn off all Windows spotlight features' is set to 'Enabled' (Automated)	1178
19.7.8.5 (L1) Ensure 'Turn off Spotlight collection on Desktop' is set to 'Enabled' (Automated)	1180
19.7.9 Credential User Interface	1182
19.7.10 Data Collection and Preview Builds	1182
19.7.11 Desktop Gadgets	1182
19.7.12 Desktop Window Manager.....	1182
19.7.13 Digital Locker	1183
19.7.14 Edge UI.....	1183
19.7.15 File Explorer (formerly Windows Explorer)	1183
19.7.16 File Revocation	1183
19.7.17 IME	1184
19.7.18 Import Video	1184
19.7.19 Instant Search	1184
19.7.20 Internet Explorer	1184
19.7.21 Location and Sensors	1184

19.7.22 Microsoft Edge	1185
19.7.23 Microsoft Management Console	1185
19.7.24 Microsoft User Experience Virtualization.....	1185
19.7.25 Multitasking.....	1185
19.7.26 NetMeeting.....	1185
19.7.27 Network Projector.....	1186
19.7.28 Network Sharing.....	1187
19.7.28.1 (L1) Ensure 'Prevent users from sharing files within their profile.' is set to 'Enabled' (Automated).....	1187
19.7.29 OOBE.....	1189
19.7.30 Presentation Settings	1189
19.7.31 Remote Desktop Services (formerly Terminal Services).....	1189
19.7.32 RSS Feeds.....	1189
19.7.33 Search.....	1190
19.7.34 Sound Recorder.....	1190
19.7.35 Store.....	1190
19.7.36 Tablet PC	1190
19.7.37 Task Scheduler	1191
19.7.38 Windows Calendar	1191
19.7.39 Windows Color System	1191
19.7.40 Windows Defender SmartScreen	1191
19.7.41 Windows Error Reporting.....	1192
19.7.42 Windows Hello for Business (formerly Microsoft Passport for Work)	1192
19.7.43 Windows Installer	1193
19.7.43.1 (L1) Ensure 'Always install with elevated privileges' is set to 'Disabled' (Automated)	1193
19.7.44 Windows Logon Options.....	1195
19.7.45 Windows Mail	1195
19.7.46 Windows Media Center	1195
19.7.47 Windows Media Player.....	1195
19.7.47.1 Networking.....	1195

19.7.47.2 Playback.....	1196
19.7.47.2.1 (L2) Ensure 'Prevent Codec Download' is set to 'Enabled' (Automated)	1196
Appendix: Recommendation Summary Table	1198
Appendix: Change History.....	1238

Overview

This document provides prescriptive guidance for establishing a secure configuration posture for Microsoft Windows.

This secure configuration guide is based on the **Microsoft Windows 11 Enterprise Release 21H2** and is intended for all versions of the **Windows 11** operating system, including **older versions**. This secure configuration guide was tested against **Microsoft Windows 11 Enterprise Release 21H2**.

To ensure all new and updated group policy objects (GPOs) are installed on the system, please download the latest version of the ADMX/ADML templates for **Windows 11**. Templates can be downloaded from Microsoft at: [Download ADMX Templates for Windows 11 October 2021 Update \[21H2\] from Official Microsoft Download Center](https://www.microsoft.com/en-us/download/details.aspx?id=102677).

To obtain the latest version of this secure configuration guide, please visit <https://www.cisecurity.org/cis-benchmarks/>. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Intended Audience

The Windows CIS Microsoft Windows Benchmarks are written for **Active Directory domain-joined** systems using Group Policy, **not** standalone/workgroup systems. Adjustments/tailoring to some recommendations will be needed to maintain functionality if attempting to implement CIS hardening on standalone systems or a system running in the cloud.

Consensus Guidance

This benchmark was created using a consensus review process comprised of subject matter experts. 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, or examples. Text should be interpreted exactly as presented.
<i><italic font in brackets></i>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
<i>Italic font</i>	Used to denote the title of a book, article, or other publication.
Note	Additional information or caveats

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 Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1 (L1) - Corporate/Enterprise Environment (general use)**

Items in this profile intend to:

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

- **Level 1 (L1) + BitLocker (BL)**

This profile extends the "Level 1 (L1)" profile and includes BitLocker-related recommendations.

- **Level 1 (L1) + Next Generation Windows Security (NG)**

This profile extends the "Level 1 (L1)" profile and includes Next Generation Windows Security-related recommendations.

- **Level 1 (L1) + BitLocker (BL) + Next Generation Windows Security (NG)**

This profile extends the "Level 1 (L1)" profile and includes BitLocker and Next Generation Windows Security-related recommendations.

- **Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)**

This profile extends the "Level 1 (L1)" profile. Items in this profile exhibit one or more of the following characteristics:

- are intended for environments or use cases where security is more critical than manageability and usability;
- may negatively inhibit the utility or performance of the technology; and
- limit the ability of remote management/access.

Note: Implementation of Level 2 requires that **both** Level 1 and Level 2 settings are applied.

- **Level 2 (L2) + BitLocker (BL)**

This profile extends the "Level 2 (L2)" profile and includes BitLocker-related recommendations.

- **Level 2 (L2) + Next Generation Windows Security (NG)**

This profile extends the "Level 2 (L2)" profile and includes Next Generation Windows Security-related recommendations.

- **Level 2 (L2) + BitLocker (BL) + Next Generation Windows Security (NG)**

This profile extends the "Level 2 (L2)" profile and includes BitLocker and Next Generation Windows Security-related recommendations.

- **BitLocker (BL) - optional add-on for when BitLocker is deployed**

This profile contains BitLocker-related recommendations, if your organization chooses to use it. It is intended be an optional "add-on" to the Level 1 (L1) or Level 2 (L2) profiles.

- **Next Generation Windows Security (NG) - optional add-on for use in the newest hardware and configuration environments**

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 (L1) or Level 2 (L2) 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 Aaron Margosis and 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.

Contributor

Jason Braun

Hardeep Mehrotara CISSP, CISA, CICP

Cliff Moten

Phil White CISSP, PMP

Matt Woods

Kevin Zhang CISSP, CISA, CRISC, CSSLP

Editor

Haemish Edgerton MCSE:Security, MCITP:EA

Jennifer Jarose

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 (L1) Ensure 'Enforce password history' is set to '24 or more password(s)' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 Windows Vista is 0 passwords, but the default setting in 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 user uses the same password, the greater the chance that an attacker can determine the password through brute force attacks. Also, any accounts that may have been compromised will remain exploitable for as long as the password is left unchanged. If password changes are required but password reuse is not prevented, or if users continually reuse a small number of passwords, the effectiveness of a good password policy is greatly reduced.

If you specify a low number for this policy setting, users will be able to use the same small number of passwords repeatedly. If you do not also configure the Minimum password age setting, 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:

24 passwords remembered on domain members. 0 passwords remembered on stand-alone workstations.

References:

1. <https://www.cisecurity.org/white-papers/cis-password-policy-guide/>

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 (L1) Ensure 'Maximum password age' is set to '365 or fewer days, but not 0' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 attackers can crack passwords, the more frequently you change the password the less opportunity an attacker 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, by an attacker 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 malicious user for as long as the valid user has authorized access.

Impact:

If the Maximum password age setting is too low, users are required to change their passwords very 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 potential attackers 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/>

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 (L1) Ensure 'Minimum password age' is set to '1 or more day(s)' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 and they believe that their password choice is secure from compromise. Unfortunately, passwords are compromised and if an attacker 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.

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:

1 day on domain members. 0 days on stand-alone workstations.

References:

1. <https://www.cisecurity.org/white-papers/cis-password-policy-guide/>

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 (L1) Ensure 'Minimum password length' is set to '14 or more character(s)' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

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

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, attackers 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 actually 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.

Note: Older versions of Windows such as Windows 98 and Windows NT 4.0 do not support passwords that are longer than 14 characters. Computers that run these older operating systems are unable to authenticate with computers or domains that use accounts that require long passwords.

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:

7 characters on domain members. 0 characters on stand-alone servers.

References:

1. <https://www.cisecurity.org/white-papers/cis-password-policy-guide/>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>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.</p>	●	●	●
v7	<p>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.</p>		●	●
v7	<p>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.</p>		●	●

1.1.5 (L1) Ensure 'Password must meet complexity requirements' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 267 (approximately 8×10^9 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 527 combinations. A seven-character case-sensitive alphanumeric password without punctuation has 627 combinations. An eight-character password has 268 (or 2×10^{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.

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:

Enabled on domain members. Disabled on stand-alone workstations.

References:

1. <https://www.cisecurity.org/white-papers/cis-password-policy-guide/>

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.	●	●	●
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.	●	●	●

1.1.6 (L1) Ensure 'Relax minimum password length limits' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

```
HKEY_LOCAL_MACHINE\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 Release 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 Release 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>

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	16.4 Encrypt or Hash all Authentication Credentials Encrypt or hash with a salt all authentication credentials when stored.	●	●	●

1.1.7 (L1) Ensure 'Store passwords using reversible encryption' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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/>

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 (L1) Ensure 'Account lockout duration' is set to '15 or more minute(s)' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 an attacker abuses the Account lockout threshold and repeatedly attempts to log on with a specific account. Once you configure the Account lockout threshold setting, the account will be locked out after the specified number of failed attempts. If you configure the Account lockout duration setting 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/>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>4.10 Enforce Automatic Device Lockout on Portable End-User Devices</p> <p>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.</p>		●	●
v7	<p>16.2 Configure Centralized Point of Authentication</p> <p>Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.</p>		●	●
v7	<p>16.11 Lock Workstation Sessions After Inactivity</p> <p>Automatically lock workstation sessions after a standard period of inactivity.</p>	●	●	●

1.2.2 (L1) Ensure 'Account lockout threshold' is set to '5 or fewer invalid logon attempt(s), but not 0' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines the number of failed logon attempts before the account is locked. Setting this policy to 0 does not conform to the benchmark as doing so disables the account lockout threshold.

The recommended state for this setting is: 5 or fewer invalid logon attempt(s), 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:

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 malicious 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 an attacker could cause a denial of service condition by deliberately generating failed logons for multiple user, therefore you should also configure the Account Lockout Duration to a relatively low value.

If you configure the Account Lockout Threshold to 0, there is a possibility that an attacker'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/>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>4.10 Enforce Automatic Device Lockout on Portable End-User Devices</p> <p>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.</p>		●	●
v7	<p>16.2 Configure Centralized Point of Authentication</p> <p>Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.</p>		●	●
v7	<p>16.11 Lock Workstation Sessions After Inactivity</p> <p>Automatically lock workstation sessions after a standard period of inactivity.</p>	●	●	●

1.2.3 (L1) Ensure 'Reset account lockout counter after' is set to '15 or more minute(s)' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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.

If you leave this policy setting at its default value or configure the value to an interval that is too long, your environment could be vulnerable to a DoS attack. An attacker could maliciously perform a number of failed logon attempts on all users in the organization, which will lock out their accounts. If no policy were determined to reset the account lockout, it would be a manual task for administrators. Conversely, if a reasonable time value is configured for this policy setting, users would be locked out for a set period until all of the accounts are unlocked automatically.

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:

Users can accidentally lock themselves out of their accounts if they mistype their password multiple times. To reduce the chance of such accidental lockouts, the Reset account lockout counter after setting determines the number of minutes that must elapse before the counter that tracks failed logon attempts and triggers lockouts is reset to 0.

Impact:

If you do not configure this policy setting or if the value is configured to an interval that is too long, a DoS attack could occur. An attacker could maliciously attempt to log on to each user's account numerous times and lock out their accounts as described in the preceding paragraphs. If you do not configure the Reset account lockout counter after setting, administrators would have to manually unlock all accounts. If you configure this policy setting to a reasonable value the users would be locked out for some period, after which their accounts would unlock automatically. Be sure that you notify users of the values used for this policy setting so that they will wait for the lockout timer to expire before they call the help desk about their inability to log on.

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/>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>4.10 Enforce Automatic Device Lockout on Portable End-User Devices</p> <p>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.</p>		●	●
v7	<p>16.2 Configure Centralized Point of Authentication</p> <p>Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.</p>		●	●
v7	<p>16.11 Lock Workstation Sessions After Inactivity</p> <p>Automatically lock workstation sessions after a standard period of inactivity.</p>	●	●	●

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 (L1) Ensure 'Access Credential Manager as a trusted caller' is set to 'No One' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/access-credential-manager-as-a-trusted-caller>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p><u>4.8 Log and Alert on Changes to Administrative Group Membership</u></p> <p>Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.</p>			

2.2.2 (L1) Ensure 'Access this computer from the network' is set to 'Administrators, Remote Desktop Users' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 is: Administrators, Remote Desktop 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 be 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, set the following UI path to Administrators, Remote Desktop 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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/access-this-computer-from-the-network>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>			

2.2.3 (L1) Ensure 'Act as part of the operating system' is set to 'No One' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/act-as-part-of-the-operating-system>

2.2.4 (L1) Ensure 'Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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.

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 denial of service (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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/adjust-memory-quotas-for-a-process>

2.2.5 (L1) Ensure 'Allow log on locally' is set to 'Administrators, Users' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 is: Administrators, Users.

Note: The Guest account is also assigned this user right by default. Although this account is disabled by default, it's recommended that you configure this setting through Group Policy. However, this user right should generally be restricted to the Administrators and Users groups. 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, set the following UI path to
Administrators, Users:

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

Default Value:

Administrators, Backup Operators, Guest, Users.

References:

1. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/allow-log-on-locally>

2.2.6 (L1) Ensure 'Allow log on through Remote Desktop Services' is set to 'Administrators, Remote Desktop Users' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 is: Administrators, Remote Desktop Users.

Note: The above list is to be treated as a whitelist, which implies that the above principals need not be present for assessment of this recommendation to pass.

Note #2: In all versions of Windows prior to Windows 7, **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, set 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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/allow-log-on-through-remote-desktop-services>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
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.	●	●	●

2.2.7 (L1) Ensure 'Back up files and directories' is set to 'Administrators' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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: 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:

Administrators, Backup Operators.

References:

1. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/back-up-files-and-directories>

2.2.8 (L1) Ensure 'Change the system time' is set to 'Administrators, LOCAL SERVICE' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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: 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, an attacker 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 an attacker 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:

Administrators, LOCAL SERVICE.

References:

1. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/change-the-system-time>

2.2.9 (L1) Ensure 'Change the time zone' is set to 'Administrators, LOCAL SERVICE, Users' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting determines which users can change the time zone of the computer. This ability holds no great danger for the computer and may be useful for mobile workers.

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

Rationale:

Changing the time zone represents little vulnerability because the system time is not affected. This setting merely enables users to display their preferred time zone while being synchronized with Domain Controllers in different time zones.

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, Users:

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

Default Value:

Administrators, LOCAL SERVICE, Users.

References:

1. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/change-the-time-zone>

2.2.10 (L1) Ensure 'Create a pagefile' is set to 'Administrators' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting allows users to change the size of the pagefile. By making the pagefile extremely large or extremely small, an attacker could easily affect the performance of a compromised computer.

The recommended state for this setting is: Administrators.

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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/create-a-pagefile>

2.2.11 (L1) Ensure 'Create a token object' is set to 'No One' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/create-a-token-object>

2.2.12 (L1) Ensure 'Create global objects' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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.

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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/create-global-objects>

2.2.13 (L1) Ensure 'Create permanent shared objects' is set to 'No One' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/create-permanent-shared-objects>

2.2.14 (L1) Configure 'Create symbolic links' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 is: `Administrators` and (when the *Hyper-V* feature 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 Workstations with the Hyper-V feature installed, this user right should also be granted to the special group `NT VIRTUAL MACHINE\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:

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

Default Value:

Administrators.

References:

1. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/create-symbolic-links>

2.2.15 (L1) Ensure 'Debug programs' is set to 'Administrators' *(Automated)*

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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: 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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/debug-programs>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p><u>18.2 Ensure Explicit Error Checking is Performed for All In-house Developed Software</u></p> <p>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.</p>			

2.2.16 (L1) Ensure 'Deny access to this computer from the network' to include 'Guests, Local account' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 is to include: Guests, Local account.

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

Note: The security identifier Local account is not available in Windows 7 and Windows 8.0 unless [MSKB 2871997](#) has been installed.

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, set the following UI path to include Guests, Local account:

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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/deny-access-to-this-computer-from-the-network>

2.2.17 (L1) Ensure 'Deny log on as a batch job' to include 'Guests' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/deny-log-on-as-a-batch-job>

2.2.18 (L1) Ensure 'Deny log on as a service' to include 'Guests' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 an attacker 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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/deny-log-on-as-a-service>

2.2.19 (L1) Ensure 'Deny log on locally' to include 'Guests' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

Guest.

References:

1. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/deny-log-on-locally>

2.2.20 (L1) Ensure 'Deny log on through Remote Desktop Services' to include 'Guests, Local account' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines whether users can log on as Remote Desktop clients. After the baseline workstation is joined to a domain environment, there is no need to use local accounts to access the workstation from the network. Domain accounts can access the workstation 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, Local account.

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

Note: The security identifier Local account is not available in Windows 7 and Windows 8.0 unless [MSKB 2871997](#) has been installed.

Note #2: In all versions of Windows prior to Windows 7, **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, set the following UI path to include 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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/deny-log-on-through-remote-desktop-services>

2.2.21 (L1) Ensure 'Enable computer and user accounts to be trusted for delegation' is set to 'No One' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting allows users to change the Trusted for Delegation setting on a computer object in Active Directory. Abuse of this privilege could allow unauthorized users to impersonate other users on the network.

The recommended state for this setting is: No One.

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

Rationale:

Misuse of the **Enable computer and user accounts to be trusted for delegation** user right could allow unauthorized users to impersonate other users on the network. An attacker 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, set 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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/enable-computer-and-user-accounts-to-be-trusted-for-delegation>

2.2.22 (L1) Ensure 'Force shutdown from a remote system' is set to 'Administrators' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting allows users to shut down Windows Vista-based and 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.

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:

None - this is the default behavior.

References:

1. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/force-shutdown-from-a-remote-system>

2.2.23 (L1) Ensure 'Generate security audits' is set to 'LOCAL SERVICE, NETWORK SERVICE' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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.

Rationale:

An attacker 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 by a large number of unrelated events.

Impact:

On most computers, this is the default configuration and there will be no negative impact. However, if you have installed *Web Server (IIS)*, you will need to allow the IIS application pool(s) to 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. <https://docs.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	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

2.2.24 (L1) Ensure 'Impersonate a client after authentication' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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.

An attacker 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 attacker's level of access to that of the client.

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

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

Rationale:

An attacker 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 attacker's level of access to that of the client.

Impact:

In most cases this configuration will have no impact. If you have installed *Web Server (IIS)*, 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, set 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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/impersonate-a-client-after-authentication>

2.2.25 (L1) Ensure 'Increase scheduling priority' is set to 'Administrators, Window Manager\Window Manager Group' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 10 R1607 or older: Administrators.

On Windows 10 R1703 or newer: Administrators, Window Manager\Window Manager Group.

References:

1. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/increase-scheduling-priority>

2.2.26 (L1) Ensure 'Load and unload device drivers' is set to 'Administrators' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting allows users to dynamically load a new device driver on a system. An attacker could potentially use this capability to install malicious code that appears to be a device driver. This user right is required for users to add local printers or printer drivers in Windows Vista.

The recommended state for this setting is: Administrators.

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

Rationale:

Device drivers run as highly privileged code. A user 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 you remove the **Load and unload device drivers** user right from the Print Operators group or other accounts you could limit the abilities of users who are assigned to specific administrative roles in your environment. You should ensure 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, 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:

Administrators.

References:

1. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/load-and-unload-device-drivers>

2.2.27 (L1) Ensure 'Lock pages in memory' is set to 'No One' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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.

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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/lock-pages-in-memory>

2.2.28 (L2) Ensure 'Log on as a batch job' is set to 'Administrators' **(Automated)**

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

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 attackers from using the right to launch malicious code after gaining user level access to a computer.

The recommended state for this setting is: Administrators.

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, Performance Log Users.

References:

1. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/log-on-as-a-batch-job>

2.2.29 (L2) Configure 'Log on as a service' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This policy setting allows accounts to launch network services or to register a process as a service running on the system. This user right should be restricted on any computer in a high security environment, but because many applications may require this privilege, it should be carefully evaluated and tested before configuring it in an enterprise environment. On Windows Vista-based (and newer) computers, no users or groups have this privilege by default.

The recommended state for this setting is: No One or (when the *Hyper-V* feature is installed) NT VIRTUAL MACHINE\Virtual Machines.

Note: The *Hyper-V* feature was first introduced on Windows workstations with the 64-bit version of Windows 8.0, so the NT VIRTUAL MACHINE\Virtual Machines option does not apply to Windows 7 (or older) versions of Windows. Older OSes should only be configured for No One.

Rationale:

Log on as a service is a powerful user right because it allows accounts to launch network services or services that run continuously on a computer, even when no one is logged on to the console. The risk is reduced by the fact that only users with administrative privileges can install and configure services. An attacker who has already attained that level of access could configure the service to run with the Local System account.

Impact:

If you have installed optional components such as ASP.NET or IIS, you may need to assign the **Log on as a service** user right to additional accounts that are required by those components. IIS requires that this user right be explicitly granted to the ASPNET user account. On Windows Workstations with the Hyper-V feature installed, this user right should also be granted to the special group NT VIRTUAL MACHINE\Virtual Machines.

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:

Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Log on as a service

Default Value:

NT SERVICE\ALL SERVICES

References:

1. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/log-on-as-a-service>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

2.2.30 (L1) Ensure 'Manage auditing and security log' is set to 'Administrators' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 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, set 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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/manage-auditing-and-security-log>

2.2.31 (L1) Ensure 'Modify an object label' is set to 'No One' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 malicious user 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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/modify-an-object-label>

2.2.32 (L1) Ensure 'Modify firmware environment values' is set to 'Administrators' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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: 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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/modify-firmware-environment-values>

2.2.33 (L1) Ensure 'Perform volume maintenance tasks' is set to 'Administrators' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 workstation 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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/perform-volume-maintenance-tasks>

2.2.34 (L1) Ensure 'Profile single process' is set to 'Administrators' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines which users can use tools to monitor the performance of non-system processes. Typically, you do not need to configure this user right to use the Microsoft Management Console (MMC) Performance snap-in. However, you do need this user right if System Monitor is configured to collect data using Windows Management Instrumentation (WMI). Restricting the **Profile single process** user right prevents intruders from gaining additional information that could be used to mount an attack on the system.

The recommended state for this setting is: Administrators.

Rationale:

The **Profile single process** user right presents a moderate vulnerability. An attacker with this user right could monitor a computer's performance to help identify critical processes that they might wish to attack directly. The attacker may also be able to determine what processes run on the computer so that they could 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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/profile-single-process>

2.2.35 (L1) Ensure 'Profile system performance' is set to 'Administrators, NT SERVICE\WdiServiceHost' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting allows users to use tools to view the performance of different system processes, which could be abused to allow attackers to determine a system's active processes and provide insight into the potential attack surface of the computer.

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

Rationale:

The **Profile system performance** user right poses a moderate vulnerability. Attackers with this user right could monitor a computer's performance to help identify critical processes that they might wish to attack directly. Attackers 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 Vista: Administrators.

Windows 7 and newer: Administrators, NT SERVICE\WdiServiceHost.

References:

1. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/profile-system-performance>

2.2.36 (L1) Ensure 'Replace a process level token' is set to 'LOCAL SERVICE, NETWORK SERVICE' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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

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 *Web Server (IIS)*, 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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/replace-a-process-level-token>

2.2.37 (L1) Ensure 'Restore files and directories' is set to 'Administrators' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 computers that run Windows Vista (or newer) in your environment. 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: This user right is considered a "sensitive privilege" for the purposes of auditing.

Rationale:

An attacker 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. Attackers 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, an attacker could still restore data to a computer in a domain that is controlled by the attacker. Therefore, it is critical that organizations carefully protect the media that is used to back up data.

Impact:

If you remove the **Restore files and directories** user right from the **Backup Operators** group and other accounts you could make it impossible for users who have been delegated specific tasks to perform those tasks. You should verify that this change won't negatively affect the ability of your organization's personnel to do their jobs.

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:

Administrators, Backup Operators.

References:

1. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/restore-files-and-directories>

2.2.38 (L1) Ensure 'Shut down the system' is set to 'Administrators, Users' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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, Users.

Rationale:

The ability to shut down a workstation should be available generally to Administrators and authorized users of that workstation, but not permitted for guests or unauthorized users - in order to prevent a Denial of Service attack.

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, Users:

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

Default Value:

Administrators, Backup Operators, Users.

References:

1. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/shut-down-the-system>

2.2.39 (L1) Ensure 'Take ownership of files or other objects' is set to 'Administrators' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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: 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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/take-ownership-of-files-or-other-objects>

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 (L1) Ensure 'Accounts: Administrator account status' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting enables or disables the Administrator account during normal operation. When a computer is booted into safe mode, the Administrator account is always enabled, regardless of how this setting is configured. Note that 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.

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

Rationale:

In some organizations, it can be a daunting management challenge to maintain a regular schedule for periodic password changes for local accounts. Therefore, you may want to disable the built-in Administrator account instead of relying on regular password changes to protect it from attack. Another reason to disable this built-in account is that it cannot be locked out no matter how many failed logons it accrues, which makes it a prime target for brute force attacks that attempt to guess passwords. Also, this account has a well-known security identifier (SID) and there are third-party tools that allow authentication by using the SID rather than the account name. This capability means that even if you rename the Administrator account, an attacker could launch a brute force attack by using the SID to log on.

Impact:

Maintenance issues can arise under certain circumstances if you disable the Administrator account. For example, if the secure channel between a member computer and the Domain Controller fails in a domain environment for any reason and there is no other local Administrator account, you must restart in safe mode to fix the problem that broke the secure channel.

If the current Administrator password does not meet the password requirements, you will not be able to re-enable the Administrator account after it is disabled. If this situation occurs, another member of the Administrators group must set the password on the Administrator account with the Local Users and Groups tool.

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: Administrator account status

Default Value:

Disabled.

References:

1. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/accounts-administrator-account-status>

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 (L1) Ensure 'Accounts: Block Microsoft accounts' is set to 'Users can't add or log on with Microsoft accounts' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting prevents users from adding new Microsoft accounts on this computer.

The recommended state for this setting is: Users can't add or log on with Microsoft accounts.

Rationale:

Organizations that want to effectively implement identity management policies and maintain firm control of what accounts are used to log onto 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:

Users will not be able to log onto the computer with their Microsoft 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:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:
NoConnectedUser

Remediation:

To establish the recommended configuration via GP, set the following UI path to Users can't add or log on with Microsoft accounts:

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Block Microsoft accounts

Default Value:

Users are able to use Microsoft accounts with Windows.

References:

1. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/accounts-block-microsoft-accounts>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
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.			

2.3.1.3 (L1) Ensure 'Accounts: Guest account status' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/accounts-guest-account-status>

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.	●	●	●

2.3.1.4 (L1) Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

HKEY_LOCAL_MACHINE\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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/accounts-limit-local-account-use-of-blank-passwords-to-console-logon-only>

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.	●	●	●

2.3.1.5 (L1) Configure 'Accounts: Rename administrator account' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

The built-in local administrator account is a well-known account name that attackers will target. 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 Administrator account exists on all computers that run the Windows 2000 or newer operating systems. If you rename this account, it is slightly more difficult for unauthorized persons to guess this privileged user name and password combination.

The built-in Administrator account cannot be locked out, regardless of how many times an attacker 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 you rename the Administrator account, an attacker could launch a brute force attack by using the SID to log on.

Impact:

You will have to inform users who are authorized to use this account 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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/accounts-rename-administrator-account>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>4.7 Manage Default Accounts on Enterprise Assets and Software</p> <p>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.</p>			

2.3.1.6 (L1) Configure 'Accounts: Rename guest account' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

The built-in local guest account is another well-known name to attackers. It is recommended to rename this account to something that does not indicate its purpose. Even if you disable this account, which is recommended, ensure that you rename it for added security.

Rationale:

The Guest account exists on all computers that run the Windows 2000 or newer operating systems. If you rename this account, it is slightly more difficult for unauthorized persons to guess this privileged user name 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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/accounts-rename-guest-account>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><u>4.7 Manage Default Accounts on Enterprise Assets and Software</u></p> <p>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.</p>			

2.3.2 Audit

This section contains recommendations related to auditing controls.

2.3.2.1 (L1) 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 (L1) - Corporate/Enterprise Environment (general use)

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:

HKEY_LOCAL_MACHINE\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/security/threat-protection/security-policy-settings/audit-force-audit-policy-subcategory-settings-to-override>

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 (L1) Ensure 'Audit: Shut down system immediately if unable to log security audits' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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.

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 you also configure the Retention method for the Security log to Do not overwrite events (clear log manually). 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.

The recommended state for this setting is: Disabled.

Rationale:

If the computer 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, an attacker 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:

HKEY_LOCAL_MACHINE\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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/audit-shut-down-system-immediately-if-unable-to-log-security-audits>

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 (L1) Ensure 'Devices: Allowed to format and eject removable media' is set to 'Administrators and Interactive Users' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines who is allowed to format and eject removable NTFS media. You can use this policy setting to prevent unauthorized users from removing data on one computer to access it on another computer on which they have local administrator privileges.

The recommended state for this setting is: Administrators and Interactive Users.

Rationale:

Users may be able to move data on removable disks to a different computer where they have administrative privileges. The user could then take ownership of any file, grant themselves full control, and view or modify any file. The fact that most removable storage devices will eject media by pressing a mechanical button diminishes the advantage of this policy setting.

Impact:

None - the default value is Administrators only. Administrators and Interactive Users will be able to format and eject removable NTFS 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:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon:AllocateDASD
--

Remediation:

To establish the recommended configuration via GP, set the following UI path to Administrators and Interactive Users:

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Devices: Allowed to format and eject removable media

Default Value:

Administrators. (Only Administrators will be able to format and eject removable NTFS media.)

References:

1. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/devices-allowed-to-format-and-eject-removable-media>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	13.7 Manage USB Devices If USB storage devices are required, enterprise software should be used that can configure systems to allow the use of specific devices. An inventory of such devices should be maintained.		●	●

2.3.4.2 (L2) Ensure 'Devices: Prevent users from installing printer drivers' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

For a computer to print to a shared printer, the driver for that shared printer must be installed on the local computer. This security setting determines who is allowed to install a printer driver as part of connecting to a shared printer.

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, you should allow only Administrators, not users, to do this, because printer driver installation may unintentionally cause the computer to become less stable. A malicious user 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 an attacker 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 your computer network.

Impact:

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.

Audit:

Navigate to the UI 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\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:

Disabled. (Any user can install a printer driver as part of connecting to a shared printer.)

References:

1. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/devices-prevent-users-from-installing-printer-drivers>

2.3.5 Domain controller

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

2.3.6 Domain member

This section contains recommendations related to domain membership.

2.3.6.1 (L1) Ensure 'Domain member: Digitally encrypt or sign secure channel data (always)' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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.

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:

HKEY_LOCAL_MACHINE\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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/domain-member-digitaly-encrypt-or-sign-secure-channel-data-always>

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 (L1) Ensure 'Domain member: Digitally encrypt secure channel data (when possible)' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters:Seal SecureChannel

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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/domain-member-digitaly-encrypt-secure-channel-data-when-possible>

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 (L1) Ensure 'Domain member: Digitally sign secure channel data (when possible)' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters:Sign  
SecureChannel
```

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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/domain-member-digitally-sign-secure-channel-data-when-possible>

2.3.6.4 (L1) Ensure 'Domain member: Disable machine account password changes' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines whether a domain member can periodically change its computer account password. Computers that cannot automatically change their account passwords are potentially vulnerable, because an attacker might be able to determine the password for the system's domain account.

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:

The default configuration for Windows Server 2003-based computers that belong to a domain is that they are automatically required to change the passwords for their accounts every 30 days. If you disable this policy setting, computers that run Windows Server 2003 will retain the same passwords as their computer accounts. Computers that are no longer able to automatically change their account password are at risk from an attacker who could determine the password for the computer's domain 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:

HKEY_LOCAL_MACHINE\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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/domain-member-disable-machine-account-password-changes>

2.3.6.5 (L1) Ensure 'Domain member: Maximum machine account password age' is set to '30 or fewer days, but not 0' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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, an attacker 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.

Note #2: 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:

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 you increase this interval significantly, or set it to 0 so that the computers no longer change their passwords, an attacker 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.

Audit:

Navigate to the UI 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\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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/domain-member-maximum-machine-account-password-age>

2.3.6.6 (L1) Ensure 'Domain member: Require strong (Windows 2000 or later) session key' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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.

To enable this policy setting, all Domain Controllers in the domain must be able to encrypt secure channel data with a strong key, which means all Domain Controllers must be running Microsoft Windows 2000 or newer.

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, you should take advantage of these stronger session keys 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.

Audit:

Navigate to the UI 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\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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/domain-member-require-strong-windows-2000-or-later-session-key>

2.3.7 Interactive logon

This section contains recommendations related to interactive logons.

2.3.7.1 (L1) Ensure 'Interactive logon: Do not require CTRL+ALT+DEL' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

Microsoft developed this feature to make it easier for users with certain types of physical impairments to log on to computers that run Windows. 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.

An attacker could install a Trojan horse program that looks like the standard Windows logon dialog box and capture the user's password. The attacker 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:

HKEY_LOCAL_MACHINE\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 7 or older: Disabled.

On Windows 8.0 or newer: Enabled.

References:

1. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/interactive-logon-do-not-require-ctrl-alt-del>

2.3.7.2 (L1) Ensure 'Interactive logon: Don't display last signed-in' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 in each computer's respective Windows logon screen. Enable this policy setting to prevent intruders from collecting account names visually from the screens of desktop or laptop computers in your organization.

The recommended state for this setting is: Enabled.

Rationale:

An attacker 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 attacker 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:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System: DontDisplayLastUserName
--

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 10 Release 1703.

Default Value:

Disabled. (The name of the last user to log on is displayed in the Windows logon screen.)

References:

1. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/interactive-logon-do-not-display-last-user-name>

2.3.7.3 (BL) Ensure 'Interactive logon: Machine account lockout threshold' is set to '10 or fewer invalid logon attempts, but not 0' (Automated)

Profile Applicability:

- Level 1 (L1) + BitLocker (BL)
- Level 2 (L2) + BitLocker (BL)
- BitLocker (BL) - optional add-on for when BitLocker is deployed

Description:

This security setting determines the number of failed logon attempts that causes the machine to be locked out.

Failed password attempts against workstations or member servers that have been locked using either CTRL+ALT+DELETE or password protected screen savers counts as failed logon attempts.

The machine lockout policy is enforced only on those machines that have BitLocker enabled for protecting OS volumes. Please ensure that appropriate recovery password backup policies are enabled.

The recommended state for this setting is: 10 or fewer invalid logon attempts, but not 0.

Note: A value of 0 does not conform to the benchmark as it disables the machine account lockout threshold. Values from 1 to 3 will be interpreted as 4.

Rationale:

If a machine is lost or stolen, or if an insider threat attempts a brute force password attack against the computer, it is important to ensure that BitLocker will lock the computer and therefore prevent a successful attack.

Impact:

Users will be able to mistype their password several times, but the machine account will be locked out if a brute force password attack occurs. A locked out machine can only be recovered by providing the BitLocker recovery key at the console.

Audit:

Navigate to the UI 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\CurrentVersion\Policies\System:
MaxDevicePasswordFailedAttempts

Remediation:

To establish the recommended configuration via GP, set the following UI path to 10 or fewer invalid logon attempts, but not 0:

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Machine account lockout threshold

Default Value:

0 invalid logon attempts. (The machine will never lock out.)

References:

1. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/interactive-logon-machine-account-lockout-threshold>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>4.10 Enforce Automatic Device Lockout on Portable End-User Devices</p> <p>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.</p>		●	●

2.3.7.4 (L1) Ensure 'Interactive logon: Machine inactivity limit' is set to '900 or fewer second(s), but not 0' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

```
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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/interactive-logon-machine-inactivity-limit>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>4.3 Configure Automatic Session Locking on Enterprise Assets</p> <p>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.</p>	●	●	●
v7	<p>16.11 Lock Workstation Sessions After Inactivity</p> <p>Automatically lock workstation sessions after a standard period of inactivity.</p>	●	●	●

2.3.7.5 (L1) Configure 'Interactive logon: Message text for users attempting to log on' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting specifies a text message that displays to users when they log on. Set the following group policy to a value that is consistent with the security and operational requirements of your organization.

Rationale:

Displaying a warning message before logon may help prevent an attack by warning the attacker about the consequences of their misconduct before it happens. It may also help 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 you display should first be approved by your organization's legal and human resources representatives.

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:

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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/interactive-logon-message-text-for-users-attempting-to-log-on>

2.3.7.6 (L1) Configure 'Interactive logon: Message title for users attempting to log on' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting specifies the text displayed in the title bar of the window that users see when they log on to the system. Configure this setting in a manner that is consistent with the security and operational requirements of your organization.

Rationale:

Displaying a warning message before logon may help prevent an attack by warning the attacker about the consequences of their misconduct before it happens. It may also help to reinforce corporate policy by notifying employees of the appropriate policy during the logon process.

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:

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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/interactive-logon-message-title-for-users-attempting-to-log-on>

2.3.7.7 (L2) Ensure 'Interactive logon: Number of previous logons to cache (in case domain controller is not available)' is set to '4 or fewer logon(s)' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

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. This policy setting determines the number of unique users for whom logon information is cached locally. If this value is set to 0, the logon cache feature is disabled. An attacker who is able to access the file system of the server could locate this cached information and use a brute force attack to determine user passwords.

The recommended state for this setting is: 4 or fewer logon(s).

Rationale:

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.

Users who access the computer console will have their logon credentials cached on that computer. An attacker 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:

10 logons.

References:

1. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/interactive-logon-number-of-previous-logons-to-cache-in-case-domain-controller-is-not-available>

2.3.7.8 (L1) Ensure 'Interactive logon: Prompt user to change password before expiration' is set to 'between 5 and 14 days' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

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:

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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/interactive-logon-prompt-user-to-change-password-before-expiration>

2.3.7.9 (L1) Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or higher (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 malicious users 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, noting that values of **Force Logoff** or **Disconnect if a Remote Desktop Services session** are also acceptable settings. This group policy setting is backed by the following registry location:

```
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** (or, if applicable for your environment, **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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/interactive-logon-smart-card-removal-behavior>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.3 Configure Automatic Session Locking on Enterprise Assets</u> 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	<u>16.11 Lock Workstation Sessions After Inactivity</u> 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 (L1) Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines whether packet signing is required by the SMB client component.

Note: When Windows Vista-based computers have this policy setting enabled and they connect to file or print shares on remote servers, it is important that the setting is synchronized with its companion setting, **Microsoft network server: Digitally sign communications (always)**, on those servers. For more information about these settings, see the "Microsoft network client and server: Digitally sign communications (four related settings)" section in Chapter 5 of the Threats and Countermeasures guide.

The recommended state for this setting is: Enabled.

Rationale:

Session hijacking uses tools that allow attackers who have access to the same network as the client or server to interrupt, end, or steal a session in progress. Attackers 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 attacker 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.

The Windows 2000 Server, Windows 2000 Professional, Windows Server 2003, Windows XP Professional and Windows Vista implementations of the SMB file and print sharing protocol support mutual authentication, which prevents session hijacking attacks and supports message authentication to prevent man-in-the-middle attacks. SMB signing provides this authentication by placing a digital signature into each SMB, which is then verified by both the client and the server.

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 you configure computers to ignore all unsigned SMB communications, older applications and operating systems will not be able to connect. However, if you completely disable all SMB signing, computers will be vulnerable to session hijacking attacks.

When SMB signing policies are enabled on Domain Controllers running Windows Server 2003 and member computers running Windows Vista SP1 or Windows Server 2008 group policy processing will fail. A hotfix is available from Microsoft that resolves this issue; see Microsoft Knowledge Base article 950876 for more details: [Group Policy settings are not applied on member computers that are running Windows Server 2008 or Windows Vista SP1 when certain SMB signing policies are 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:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters:RequireSecuritySignature

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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/microsoft-network-client-digital-sign-communications-always>

2.3.8.2 (L1) Ensure 'Microsoft network client: Digitally sign communications (if server agrees)' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines whether the SMB client will attempt to negotiate SMB packet signing.

Note: Enabling this policy setting on SMB clients on your network makes them fully effective for packet signing with all clients and servers in your environment.

The recommended state for this setting is: Enabled.

Rationale:

Session hijacking uses tools that allow attackers who have access to the same network as the client or server to interrupt, end, or steal a session in progress. Attackers 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 attacker 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:

None - this is the default behavior.

The Windows 2000 Server, Windows 2000 Professional, Windows Server 2003, Windows XP Professional and Windows Vista implementations of the SMB file and print sharing protocol support mutual authentication, which prevents session hijacking attacks and supports message authentication to prevent man-in-the-middle attacks. SMB signing provides this authentication by placing a digital signature into each SMB, which is then verified by both the client and the server.

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 you configure computers to ignore all unsigned SMB communications, older applications and operating systems will not be able to connect. However, if you completely disable all SMB signing, computers will be vulnerable to session hijacking attacks.

When SMB signing policies are enabled on Domain Controllers running Windows Server 2003 and member computers running Windows Vista SP1 or Windows Server 2008 group policy processing will fail. A hotfix is available from Microsoft that resolves this issue; see Microsoft Knowledge Base article 950876 for more details: [Group Policy settings are not applied on member computers that are running Windows Server 2008 or Windows Vista SP1 when certain SMB signing policies are 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:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters:EnableSecuritySignature

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 (if server agrees)

Default Value:

Enabled. (The Microsoft network client will ask the server to perform SMB packet signing upon session setup. If packet signing has been enabled on the server, packet signing will be negotiated.)

References:

1. [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/jj852251\(v=ws.11\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/jj852251(v=ws.11))

2.3.8.3 (L1) Ensure 'Microsoft network client: Send unencrypted password to third-party SMB servers' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

```
HKEY_LOCAL_MACHINE\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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/microsoft-network-client-send-unencrypted-password-to-third-party-smb-servers>

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 (L1) 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 (L1) - Corporate/Enterprise Environment (general use)

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. An attacker 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:

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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/microsoft-network-server-amount-of-idle-time-required-before-suspending-session>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.3 Configure Automatic Session Locking on Enterprise Assets</u> 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	<u>16.11 Lock Workstation Sessions After Inactivity</u> Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

2.3.9.2 (L1) Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines whether packet signing is required by the SMB server component. Enable this policy setting in a mixed environment to prevent downstream clients from using the workstation as a network server.

The recommended state for this setting is: Enabled.

Rationale:

Session hijacking uses tools that allow attackers who have access to the same network as the client or server to interrupt, end, or steal a session in progress. Attackers 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 attacker 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 server will not communicate with a Microsoft network client unless that client agrees to perform SMB packet signing.

The Windows 2000 Server, Windows 2000 Professional, Windows Server 2003, Windows XP Professional and Windows Vista implementations of the SMB file and print sharing protocol support mutual authentication, which prevents session hijacking attacks and supports message authentication to prevent man-in-the-middle attacks. SMB signing provides this authentication by placing a digital signature into each SMB, which is then verified by both the client and the server.

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 you configure computers to ignore all unsigned SMB communications, older applications and operating systems will not be able to connect. However, if you completely disable all SMB signing, computers will be vulnerable to session hijacking attacks.

When SMB signing policies are enabled on Domain Controllers running Windows Server 2003 and member computers running Windows Vista SP1 or Windows Server 2008 group policy processing will fail. A hotfix is available from Microsoft that resolves this issue; see Microsoft Knowledge Base article 950876 for more details: [Group Policy settings are not applied on member computers that are running Windows Server 2008 or Windows Vista SP1 when certain SMB signing policies are 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:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters:
RequireSecuritySignature

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:

Disabled. (SMB packet signing is negotiated between the client and server.)

References:

1. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/microsoft-network-server-digital-sign-communications-always>

2.3.9.3 (L1) Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines whether the SMB server will negotiate SMB packet signing with clients that request it. If no signing request comes from the client, a connection will be allowed without a signature if the **Microsoft network server: Digitally sign communications (always)** setting is not enabled.

Note: Enable this policy setting on SMB clients on your network to make them fully effective for packet signing with all clients and servers in your environment.

The recommended state for this setting is: Enabled.

Rationale:

Session hijacking uses tools that allow attackers who have access to the same network as the client or server to interrupt, end, or steal a session in progress. Attackers 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 attacker 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 server will negotiate SMB packet signing as requested by the client. That is, if packet signing has been enabled on the client, packet signing will be negotiated.

The Windows 2000 Server, Windows 2000 Professional, Windows Server 2003, Windows XP Professional and Windows Vista implementations of the SMB file and print sharing protocol support mutual authentication, which prevents session hijacking attacks and supports message authentication to prevent man-in-the-middle attacks. SMB signing provides this authentication by placing a digital signature into each SMB, which is then verified by both the client and the server.

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 you configure computers to ignore all unsigned SMB communications, older applications and operating systems will not be able to connect. However, if you completely disable all SMB signing, computers will be vulnerable to session hijacking attacks.

When SMB signing policies are enabled on Domain Controllers running Windows Server 2003 and member computers running Windows Vista SP1 or Windows Server 2008 group policy processing will fail. A hotfix is available from Microsoft that resolves this issue; see Microsoft Knowledge Base article 950876 for more details: [Group Policy settings are not applied on member computers that are running Windows Server 2008 or Windows Vista SP1 when certain SMB signing policies are 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:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters:
EnableSecuritySignature

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 (if client agrees)

Default Value:

Disabled. (The SMB client will never negotiate SMB packet signing.)

References:

1. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/smbv1-microsoft-network-server-digital-sign-communications-if-client-agrees>

2.3.9.4 (L1) Ensure 'Microsoft network server: Disconnect clients when logon hours expire' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

HKEY_LOCAL_MACHINE\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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/microsoft-network-server-disconnect-clients-when-logon-hours-expire>

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	16.13 Alert on Account Login Behavior Deviation Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			●

2.3.9.5 (L1) Ensure 'Microsoft network server: Server SPN target name validation level' is set to 'Accept if provided by client' or higher (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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.

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:

```
HKEY_LOCAL_MACHINE\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` (configuring to `Required from client` also conforms to the benchmark):

```
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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/microsoft-network-server-server-spn-target-name-validation-level>

2.3.10 Network access

This section contains recommendations related to network access.

2.3.10.1 (L1) Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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.

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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-allow-anonymous-sidname-translation>

2.3.10.2 (L1) Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

HKEY_LOCAL_MACHINE\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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-do-not-allow-anonymous-enumeration-of-sam-accounts>

2.3.10.3 (L1) Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

HKEY_LOCAL_MACHINE\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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-do-not-allow-anonymous-enumeration-of-sam-accounts-and-shares>

2.3.10.4 (L1) Ensure 'Network access: Do not allow storage of passwords and credentials for network authentication' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

HKEY_LOCAL_MACHINE\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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-do-not-allow-storage-of-passwords-and-credentials-for-network-authentication>

2.3.10.5 (L1) Ensure 'Network access: Let Everyone permissions apply to anonymous users' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

HKEY_LOCAL_MACHINE\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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-let-everyone-permissions-apply-to-anonymous-users>

2.3.10.6 (L1) Ensure 'Network access: Named Pipes that can be accessed anonymously' is set to 'None' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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).

Rationale:

Limiting named pipes that can be accessed anonymously will reduce the attack surface of the system.

Impact:

This configuration will disable null session access over named pipes, and applications that rely on this feature or on unauthenticated access to named pipes will no longer 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:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters:
NullSessionPipes

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: Named Pipes that can be accessed anonymously

Default Value:

None.

References:

1. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-named-pipes-that-can-be-accessed-anonymously>

2.3.10.7 (L1) Ensure 'Network access: Remotely accessible registry paths' is configured (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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.

Note: This setting does not exist in Windows XP. There was a setting with that name in Windows XP, but it is called "Network access: Remotely accessible registry paths and sub-paths" in Windows Server 2003, Windows Vista, and Windows Server 2008 (non-R2).

Note #2: When you configure this setting you specify a list of one or more objects. 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.

The recommended state for this setting is:

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

Rationale:

The registry is a database that contains computer configuration information, and much of the information is sensitive. An attacker 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 you remove the default registry paths from the list of accessible ones, 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 you want to allow remote access, you 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:

```
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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-remotely-accessible-registry-paths>

2.3.10.8 (L1) Ensure 'Network access: Remotely accessible registry paths and sub-paths' is configured (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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.

Note: In Windows XP this setting is called "Network access: Remotely accessible registry paths," the setting with that same name in Windows Vista, Windows Server 2008 (non-R2), and Windows Server 2003 does not exist in Windows XP.

Note #2: When you configure this setting you specify a list of one or more objects. 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.

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
```

Rationale:

The registry contains sensitive computer configuration information that could be used by an attacker 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 you remove the default registry paths from the list of accessible ones, 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 you want to allow remote access, you 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:

```
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
```

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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-remotely-accessible-registry-paths-and-subpaths>

2.3.10.9 (L1) Ensure 'Network access: Restrict anonymous access to Named Pipes and Shares' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters:  
RestrictNullSessAccess
```

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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-restrict-anonymous-access-to-named-pipes-and-shares>

2.3.10.10 (L1) Ensure 'Network access: Restrict clients allowed to make remote calls to SAM' is set to 'Administrators: Remote Access: Allow' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 R1607, Server 2016 or newer OS is required to access and set this value in Group Policy.

Note #2: If your organization is using Azure Advanced Threat Protection (APT), the service account, "AATP Service" will need to be added to the recommendation configuration. For more information on adding the "AATP 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:

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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-restrict-clients-allowed-to-make-remote-sam-calls>

2.3.10.11 (L1) Ensure 'Network access: Shares that can be accessed anonymously' is set to 'None' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

```
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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-shares-that-can-be-accessed-anonymously>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
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.	●	●	●

2.3.10.12 (L1) Ensure 'Network access: Sharing and security model for local accounts' is set to 'Classic - local users authenticate as themselves' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

HKEY_LOCAL_MACHINE\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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-sharing-and-security-model-for-local-accounts>

2.3.11 Network security

This section contains recommendations related to network security.

2.3.11.1 (L1) Ensure 'Network security: Allow Local System to use computer identity for NTLM' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

HKEY_LOCAL_MACHINE\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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-allow-local-system-to-use-computer-identity-for-ntlm>

2.3.11.2 (L1) Ensure 'Network security: Allow LocalSystem NULL session fallback' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

None - this is the default behavior. 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:

```
HKEY_LOCAL_MACHINE\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:

Disabled. (NTLM will not be permitted to fall back to a NULL session when used with LocalSystem.)

References:

1. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-allow-localsystem-null-session-fallback>

2.3.11.3 (L1) Ensure 'Network Security: Allow PKU2U authentication requests to this computer to use online identities' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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.

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:

HKEY_LOCAL_MACHINE\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 be allowed to authenticate to a domain-joined machine.)

References:

1. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-allow-pku2u-authentication-requests-to-this-computer-to-use-online-identities>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

2.3.11.4 (L1) 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 (L1) - Corporate/Enterprise Environment (general use)

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 Vista 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:

[Azure Files on-premises AD DS Authentication support for AES 256 Kerberos encryption | 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:

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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-configure-encryption-types-allowed-for-kerberos>

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 (L1) Ensure 'Network security: Do not store LAN Manager hash value on next password change' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines whether the LAN Manager (LM) hash value for the new password is stored when the password is changed. 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.

Note: 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 you enable this setting to gain the proper benefit.

The recommended state for this setting is: Enabled.

Rationale:

The SAM file can be targeted by attackers 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.

Impact:

None - this is the default behavior. Earlier operating systems such as Windows 95, Windows 98, and Windows ME as well as some third-party applications 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:

HKEY_LOCAL_MACHINE\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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-do-not-store-lan-manager-hash-value-on-next-password-change>

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 (L1) Ensure 'Network security: Force logoff when logon hours expire' is set to 'Enabled' (Manual)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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.

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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-force-logoff-when-logon-hours-expire>

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	16.13 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 (L1) Ensure 'Network security: LAN Manager authentication level' is set to 'Send NTLMv2 response only. Refuse LM & NTLM' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

LAN Manager (LM) was 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 Network security: LAN Manager authentication level setting determines which challenge/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.

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 attackers 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. You can enforce a more secure authentication protocol 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 you use NTLMv2 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:

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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-lan-manager-authentication-level>

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	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.	●	●	●

2.3.11.8 (L1) Ensure 'Network security: LDAP client signing requirements' is set to 'Negotiate signing' or higher (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines the level of data signing that is requested on behalf of clients that issue LDAP BIND requests.

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.

The recommended state for this setting is: `Negotiate signing`. Configuring this setting to `Require signing` also conforms to the benchmark.

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 an attacker could cause a server to make decisions that are based on false or altered data from the LDAP queries. To lower this risk in your network, you can implement strong physical security measures to protect the network infrastructure. Also, you can make all types of man-in-the-middle attacks extremely difficult if you require digital signatures on all network packets by means of IPsec authentication headers.

Impact:

None - this is the default behavior. However, if you choose instead to configure the server to *require* LDAP signatures then you must also configure the client. If you do not configure the client 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:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LDAP:LDAPClientIntegrity

Remediation:

To establish the recommended configuration via GP, set the following UI path to Negotiate signing (configuring to Require signing also conforms to the benchmark):

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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-ldap-client-signing-requirements>

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	12.5 Configure Monitoring Systems to Record Network Packets Configure monitoring systems to record network packets passing through the boundary at each of the organization's network boundaries.		●	●

2.3.11.9 (L1) 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 (L1) - Corporate/Enterprise Environment (general use)

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:

You can 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 an attacker who has gained access to the same network. In other words, 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:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0:NTLMMinClients
ec

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:

Require 128-bit encryption. (NTLM connections will fail if strong encryption (128-bit) is not negotiated.)

References:

1. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-minimum-session-security-for-ntlm-ssp-based-including-secure-rpc-clients>

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	12.5 Configure Monitoring Systems to Record Network Packets Configure monitoring systems to record network packets passing through the boundary at each of the organization's network boundaries.	●	●	●

2.3.11.10 (L1) 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 (L1) - Corporate/Enterprise Environment (general use)

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:

You can 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 an attacker who has gained access to the same network. That is, 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:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0:NTLMMinServers
ec

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:

Require 128-bit encryption. (NTLM connections will fail if strong encryption (128-bit) is not negotiated.)

References:

1. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-minimum-session-security-for-ntlm-ssp-based-including-secure-rpc-servers>

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	12.5 Configure Monitoring Systems to Record Network Packets Configure monitoring systems to record network packets passing through the boundary at each of the organization's network boundaries.			

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

2.3.14 System cryptography

This section contains recommendations related to system cryptography.

2.3.14.1 (L2) Ensure 'System cryptography: Force strong key protection for user keys stored on the computer' is set to 'User is prompted when the key is first used' or higher (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This policy setting determines whether users' private keys (such as their S-MIME keys) require a password to be used.

The recommended state for this setting is: User is prompted when the key is first used. Configuring this setting to User must enter a password each time they use a key also conforms to the benchmark.

Rationale:

If a user's account is compromised or their computer is inadvertently left unsecured the malicious user can use the keys stored for the user to access protected resources. You can configure this policy setting so that users must provide a password that is distinct from their domain password every time they use a key. This configuration makes it more difficult for an attacker to access locally stored user keys, even if the attacker takes control of the user's computer and determines their logon password.

Impact:

Users will have to enter their password the first time they access a key that is stored on their computer. For example, if users use an S-MIME certificate to digitally sign their e-mail they will be forced to enter the password for that certificate the first time that they send a signed e-mail message. For even stronger security, the value User must enter a password each time they use a key can be set, but the overhead that is involved using this configuration may be too high for some organizations.

Microsoft does not recommend enforcing this setting on servers due to the significant impact on manageability. For example, you may not be able to configure Remote Desktop Services to use SSL certificates. More information is available in the Windows PKI TechNet Blog here: [What is a strong key protection in 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:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Cryptography:ForceKeyProtection

Remediation:

To establish the recommended configuration via GP, set the following UI path to User is prompted when the key is first used (configuring to User must enter a password each time they use a key also conforms to the benchmark):

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\System cryptography: Force strong key protection for user keys stored on the computer

Default Value:

User input is not required when new keys are stored and used.

References:

1. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/system-cryptography-force-strong-key-protection-for-user-keys-stored-on-the-computer>

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.			

2.3.15 System objects

This section contains recommendations related to system objects.

2.3.15.1 (L1) Ensure 'System objects: Require case insensitivity for non-Windows subsystems' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

HKEY_LOCAL_MACHINE\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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/system-objects-require-case-insensitivity-for-non-windows-subsystems>

2.3.15.2 (L1) Ensure 'System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

HKEY_LOCAL_MACHINE\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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/system-objects-strengthen-default-permissions-of-internal-system-objects>

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 (L1) Ensure 'User Account Control: Admin Approval Mode for the Built-in Administrator account' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 and 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:

HKEY_LOCAL_MACHINE\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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/user-account-control-admin-approval-mode-for-the-built-in-administrator-account>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
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.		●	●

2.3.17.2 (L1) 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' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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.

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:

HKEY_LOCAL_MACHINE\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:

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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/user-account-control-behavior-of-the-elevation-prompt-for-administrators-in-admin-approval-mode>

2.3.17.3 (L1) Ensure 'User Account Control: Behavior of the elevation prompt for standard users' is set to 'Automatically deny elevation requests' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

HKEY_LOCAL_MACHINE\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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/user-account-control-behavior-of-the-elevation-prompt-for-standard-users>

2.3.17.4 (L1) Ensure 'User Account Control: Detect application installations and prompt for elevation' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:
EnableInstallerDetection

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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/user-account-control-detect-application-installations-and-prompt-for-elevation>

2.3.17.5 (L1) Ensure 'User Account Control: Only elevate UIAccess applications that are installed in secure locations' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

```
HKEY_LOCAL_MACHINE\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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/user-account-control-only-elevate-uiaccess-applications-that-are-installed-in-secure-locations>

2.3.17.6 (L1) Ensure 'User Account Control: Run all administrators in Admin Approval Mode' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

```
HKEY_LOCAL_MACHINE\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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/user-account-control-run-all-administrators-in-admin-approval-mode>

2.3.17.7 (L1) Ensure 'User Account Control: Switch to the secure desktop when prompting for elevation' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:
PromptOnSecureDesktop

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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/user-account-control-switch-to-the-secure-desktop-when-prompts-for-elevation>

2.3.17.8 (L1) Ensure 'User Account Control: Virtualize file and registry write failures to per-user locations' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

HKEY_LOCAL_MACHINE\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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/user-account-control-virtualize-file-and-registry-write-failures-to-per-user-locations>

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 (L2) Ensure 'Bluetooth Audio Gateway Service (BTAGService)' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

Service supporting the audio gateway role of the Bluetooth Handsfree Profile.

The recommended state for this setting is: Disabled.

Rationale:

Bluetooth technology has inherent security risks - especially prior to the v2.1 standard. Wireless Bluetooth traffic is not well encrypted (if at all), so in a high-security environment, it should not be permitted, in spite of the added inconvenience of not being able to use Bluetooth devices.

Impact:

Bluetooth hands-free devices will not function properly with 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:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\BTAGService: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\Bluetooth Audio Gateway Service

Note: This service was first introduced in Windows 10 Release 1803. It appears to have replaced the older *Bluetooth Handsfree Service (BthHFSrv)*, which was removed from Windows in that release (it is not simply a rename, but a different service).

Default Value:

Manual (Trigger Start)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></p> <p>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.</p>			
v7	<p>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>			

5.2 (L2) Ensure 'Bluetooth Support Service (bthserv)' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

The Bluetooth service supports discovery and association of remote Bluetooth devices.

The recommended state for this setting is: Disabled.

Rationale:

Bluetooth technology has inherent security risks - especially prior to the v2.1 standard. Wireless Bluetooth traffic is not well encrypted (if at all), so in a high-security environment, it should not be permitted, in spite of the added inconvenience of not being able to use Bluetooth devices.

Impact:

Already installed Bluetooth devices may fail to operate properly and new devices may be prevented from being discovered or associated. If Bluetooth devices were installed, then some Windows components, such as Devices and Printers, may fail to operate correctly - including hanging/freezing when opened. The solution, besides re-enabling this service, is to disable or delete the offending Bluetooth device(s) in Device Manager, or disable the device altogether via the system BIOS (if it is an on-board Bluetooth 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:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\bthserv: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\Bluetooth Support Service

Default Value:

Windows 7: Manual

Windows 8.0 and newer: Manual (Trigger Start)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></p> <p>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.</p>		●	●
v7	<p><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>		●	●

5.3 (L1) Ensure 'Computer Browser (Browser)' is set to 'Disabled' or 'Not Installed' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Maintains an updated list of computers on the network and supplies this list to computers designated as browsers.

The recommended state for this setting is: Disabled or Not Installed.

Note: In Windows 8.1 and Windows 10, this service is bundled with the *SMB 1.0/CIFS File Sharing Support* optional feature. As a result, removing that feature (highly recommended unless backward compatibility is needed to XP/2003 and older Windows OSes - see [Stop using SMB1 | Storage at Microsoft](#)) will also remediate this recommendation. The feature is not installed by default starting with Windows 10 R1709.

Rationale:

This is a legacy service - its sole purpose is to maintain a list of computers and their network shares in the environment (i.e. "Network Neighborhood"). If enabled, it generates a lot of unnecessary traffic, including "elections" to see who gets to be the "master browser". This noisy traffic could also aid malicious attackers in discovering online machines, because the service also allows anyone to "browse" for shared resources without any authentication. This service used to be running by default in older Windows versions (e.g. Windows XP), but today it only remains for backward compatibility for very old software that requires it.

Impact:

The list of computers and their shares on the network will not be updated or maintained.

Audit:

Navigate to the UI 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\SYSTEM\CurrentControlSet\Services\Browser:Start

Remediation:

To establish the recommended configuration via GP, set the following UI path to: Disabled or ensure the service is not installed.

Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Computer Browser

Default Value:

Windows 7: Manual

Windows 8.0 through Windows 10 R1703: Manual (Trigger Start)

Windows 10 R1709 and newer: Not Installed (Manual (Trigger Start) when installed)

References:

1. <https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/>

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.		●	●

5.4 (L2) Ensure 'Downloaded Maps Manager (MapsBroker)' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

Windows service for application access to downloaded maps. This service is started on-demand by application accessing downloaded maps.

Rationale:

Mapping technologies can unwillingly reveal your location to attackers and other software that picks up the information. In addition, automatic downloads of data from 3rd-party sources should be minimized when not needed. Therefore this service should not be needed in high security environments.

Impact:

Applications will be prevented from accessing maps data.

Audit:

Navigate to the UI 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\SYSTEM\CurrentControlSet\Services\MapsBroker: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\Downloaded Maps Manager

Default Value:

Automatic (Delayed Start)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> 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 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

5.5 (L2) Ensure 'Geolocation Service (lfsvc)' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This service monitors the current location of the system and manages geofences (a geographical location with associated events).

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

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:

Applications will be unable to use or receive notifications for geolocation or geofences.

Audit:

Navigate to the UI 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\SYSTEM\CurrentControlSet\Services\lfsvc: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\Geolocation Service`

Default Value:

Manual (Trigger Start)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> 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 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

5.6 (L1) Ensure 'IIS Admin Service (IISADMIN)' is set to 'Disabled' or 'Not Installed' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Enables the server to administer the IIS metabase. The IIS metabase stores configuration for the SMTP and FTP services.

The recommended state for this setting is: Disabled or Not Installed.

Note: This service is not installed by default. It is supplied with Windows, but is installed by enabling an optional Windows feature (*Internet Information Services*).

Note #2: An organization may choose to selectively grant exceptions to web developers to allow IIS (or another web server) on their workstation, in order for them to locally test & develop web pages. However, the organization should track those machines and ensure the security controls and mitigations are kept up to date, to reduce risk of compromise.

Rationale:

Hosting a website from a workstation is an increased security risk, as the attack surface of that workstation is then greatly increased. If proper security mitigations are not followed, the chance of successful attack increases significantly.

Note: This security concern applies to *any* web server application installed on a workstation, not just IIS.

Impact:

IIS will not function, including Web, SMTP or FTP 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:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\IISADMIN:Start

Remediation:

To establish the recommended configuration via GP, set the following UI path to: Disabled or ensure the service is not installed.

Computer Configuration\Policies\Windows Settings\Security Settings\System Services\IIS Admin Service

Default Value:

Not Installed (Automatic when installed)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</p> <p>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.</p>		●	●
v7	<p>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>		●	●

5.7 (L1) Ensure 'Infrared monitor service (irmon)' is set to 'Disabled' or 'Not Installed' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Detects other Infrared devices that are in range and launches the file transfer application.

The recommended state for this setting is: Disabled or Not Installed.

Rationale:

Infrared connections can potentially be a source of data compromise - especially via the automatic "file transfer application" functionality. Enterprise-managed systems should utilize a more secure method of connection than infrared.

Impact:

Infrared file transfers will be prevented from 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:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\irmon:Start

Remediation:

To establish the recommended configuration via GP, set the following UI path to: Disabled or ensure the service is not installed.

Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Infrared monitor service

Default Value:

Windows 10 R1607 through Windows 10 R1809: Manual

Windows 10 R1903 and newer: Not Installed (Manual when installed)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> 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 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

5.8 (L1) Ensure 'Internet Connection Sharing (ICS) (SharedAccess)' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Provides network access translation, addressing, name resolution and/or intrusion prevention services for a home or small office network.

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

Rationale:

Internet Connection Sharing (ICS) is a feature that allows someone to "share" their Internet connection with other machines on the network - it was designed for home or small office environments where only one machine has Internet access - it effectively turns that machine into an Internet router. This feature causes the bridging of networks and likely bypassing other, more secure pathways. It should not be used on any enterprise-managed system.

Impact:

Internet Connection Sharing (ICS) will not be available. Wireless connections using Miracast will also be prevented.

Note: This service is a prerequisite for the *Microsoft Defender Application Guard* feature in Windows 10, so an exception should be made to this recommendation if intending to use Microsoft Defender Application Guard.

Note #2: If your organization is using Windows Subsystem for Linux (WSL) this service is needed for WSL to function, so an exception should be made to this recommendation. For more information, please visit the following Microsoft Blog: [Troubleshooting Windows Subsystem for Linux | 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:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess: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\Internet Connection Sharing (ICS)

Default Value:

Windows 7 through Windows 8.1: Disabled

Windows 10 R1507 and R1511: Manual

Windows 10 R1607 and newer: Manual (Trigger Start)

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.		●	●

5.9 (L2) Ensure 'Link-Layer Topology Discovery Mapper (lltdsvc)' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

Creates a Network Map, consisting of PC and device topology (connectivity) information, and metadata describing each PC and device.

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

Rationale:

The feature that this service enables could potentially be used for unauthorized discovery and connection to network devices. Disabling the service helps to prevent responses to requests for network topology discovery in high security environments.

Impact:

The Network Map will not function properly.

Audit:

Navigate to the UI 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\SYSTEM\CurrentControlSet\Services\lltdsvc: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\Link-Layer Topology Mapper

Default Value:

Manual

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> 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 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

5.10 (L1) Ensure 'LxssManager (LxssManager)' is set to 'Disabled' or 'Not Installed' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

The LXSS Manager service supports running native ELF binaries. The service provides the infrastructure necessary for ELF binaries to run on Windows.

The recommended state for this setting is: `Disabled` or `Not Installed`.

Note: This service is not installed by default. It is supplied with Windows, but is installed by enabling an optional Windows feature (*Windows Subsystem for Linux*).

Rationale:

The Linux Subsystem (LXSS) Manager allows full system access to Linux applications on Windows, including the file system. While this can certainly have some functionality and performance benefits for running those applications, it also creates new security risks in the event that a hacker injects malicious code into a Linux application. For best security, it is preferred to run Linux applications on Linux, and Windows applications on Windows.

Impact:

The Linux Subsystem will not be available, and native ELF binaries will no longer run.

Note: If your organization has made an exception to this recommendation and is using Windows Subsystem for Linux (WSL), the Internet Connection Sharing (ICS) (SharedAccess) service will need to be `Enabled` for WSL to function. For more information, please visit the following Microsoft Blog: [Troubleshooting Windows Subsystem for Linux | 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:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LxssManager:Start`

Remediation:

To establish the recommended configuration via GP, set the following UI path to: Disabled or ensure the service is not installed.

Computer Configuration\Policies\Windows Settings\Security Settings\System Services\LxssManager

Default Value:

Not Installed (Manual when installed)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</p> <p>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.</p>		●	●
v7	<p>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>		●	●

5.11 (L1) Ensure 'Microsoft FTP Service (FTPSVC)' is set to 'Disabled' or 'Not Installed' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Enables the server to be a File Transfer Protocol (FTP) server.

The recommended state for this setting is: `Disabled` or `Not Installed`.

Note: This service is not installed by default. It is supplied with Windows, but is installed by enabling an optional Windows feature (*Internet Information Services - FTP Server*).

Rationale:

Hosting an FTP server (especially a non-secure FTP server) from a workstation is an increased security risk, as the attack surface of that workstation is then greatly increased.

Note: This security concern applies to *any* FTP server application installed on a workstation, not just IIS.

Impact:

The computer will not function as an FTP 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:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\FTPSVC:Start`

Remediation:

To establish the recommended configuration via GP, set the following UI path to: `Disabled` or ensure the service is not installed.

`Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Microsoft FTP Service`

Default Value:

Not Installed (Automatic when installed)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></p> <p>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.</p>			
v7	<p>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>			

5.12 (L2) Ensure 'Microsoft iSCSI Initiator Service (MSiSCSI)' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

Manages Internet SCSI (iSCSI) sessions from this computer to remote target devices.

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

Rationale:

This service is critically necessary in order to directly attach to an iSCSI device. However, iSCSI itself uses a very weak authentication protocol (CHAP), which means that the passwords for iSCSI communication are easily exposed, unless all of the traffic is isolated and/or encrypted using another technology like IPsec. This service is generally more appropriate for servers in a controlled environment than on workstations requiring high security.

Impact:

The computer will not be able to directly login to or access iSCSI targets.

Audit:

Navigate to the UI 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\SYSTEM\CurrentControlSet\Services\MSiSCSI: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\Microsoft iSCSI Initiator Service`

Default Value:

Manual

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> 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 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

5.13 (L1) Ensure 'OpenSSH SSH Server (sshd)' is set to 'Disabled' or 'Not Installed' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

SSH protocol based service to provide secure encrypted communications between two untrusted hosts over an insecure network.

The recommended state for this setting is: Disabled or Not Installed.

Note: This service is not installed by default. It is supplied with Windows, but it is installed by enabling an optional Windows feature (*OpenSSH Server*).

Rationale:

Hosting an SSH server from a workstation is an increased security risk, as the attack surface of that workstation is then greatly increased.

Note: This security concern applies to *any* SSH server application installed on a workstation, not just the one supplied with Windows.

Impact:

The workstation will not be permitted to be a SSH host 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:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\sshd:Start

Remediation:

To establish the recommended configuration via GP, set the following UI path to: Disabled or ensure the service is not installed.

Computer Configuration\Policies\Windows Settings\Security Settings\System Services\OpenSSH SSH Server

Default Value:

Not Installed (Manual when installed)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></p> <p>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.</p>			
v7	<p>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>			

5.14 (L2) Ensure 'Peer Name Resolution Protocol (PNRPsrv)' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

Enables serverless peer name resolution over the Internet using the Peer Name Resolution Protocol (PNRP).

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

Rationale:

Peer Name Resolution Protocol is a distributed and (mostly) serverless way to handle name resolution of clients with each other. In a high security environment, it is more secure to rely on centralized name resolution methods maintained by authorized staff.

Impact:

Some peer-to-peer and collaborative applications, such as Remote Assistance, 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:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PNRPsrv: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\Peer Name Resolution Protocol`

Default Value:

Manual

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> 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 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

5.15 (L2) Ensure 'Peer Networking Grouping (p2psvc)' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

Enables multi-party communication using Peer-to-Peer Grouping.

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

Rationale:

Peer Name Resolution Protocol is a distributed and (mostly) serverless way to handle name resolution of clients with each other. In a high security environment, it is more secure to rely on centralized name resolution methods maintained by authorized staff.

Impact:

Some applications, such as HomeGroup, 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:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\p2psvc: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\Peer Networking Grouping

Default Value:

Manual

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> 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 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

5.16 (L2) Ensure 'Peer Networking Identity Manager (p2pimsvc)' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

Provides identity services for the Peer Name Resolution Protocol (PNRP) and Peer-to-Peer Grouping services.

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

Rationale:

Peer Name Resolution Protocol is a distributed and (mostly) serverless way to handle name resolution of clients with each other. In a high security environment, it is more secure to rely on centralized name resolution methods maintained by authorized staff.

Impact:

The Peer Name Resolution Protocol (PNRP) and Peer-to-Peer Grouping services may not function, and some applications, such as HomeGroup and Remote Assistance, may not function 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:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\p2pimsvc: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\Peer Networking Identity Manager`

Default Value:

Manual

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> 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 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

5.17 (L2) Ensure 'PNRP Machine Name Publication Service (PNRPAutoReg)' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This service publishes a machine name using the Peer Name Resolution Protocol. Configuration is managed via the netsh context 'p2p pnrp peer'.

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

Rationale:

Peer Name Resolution Protocol is a distributed and (mostly) serverless way to handle name resolution of clients with each other. In a high security environment, it is more secure to rely on centralized name resolution methods maintained by authorized staff.

Impact:

Some peer-to-peer and collaborative applications, such as Remote Assistance, 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:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PNRPAutoReg: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\PNRP Machine Name Publication Service`

Default Value:

Manual

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> 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 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

5.18 (L2) Ensure 'Print Spooler (Spooler)' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This service spools print jobs and handles interaction with printers.

The recommended state for this setting is: Disabled.

Rationale:

In a high security environment, unnecessary services especially those with known vulnerabilities should be disabled.

Disabling the Print Spooler (Spooler) service mitigates the PrintNightmare vulnerability ([CVE-2021-34527](#)) and other attacks against the service.

Impact:

Users 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:

`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>

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.			

5.19 (L2) Ensure 'Problem Reports and Solutions Control Panel Support (wercplsupport)' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This service provides support for viewing, sending and deletion of system-level problem reports for the Problem Reports and Solutions control panel.

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

Rationale:

This service is involved in the process of displaying/reporting issues & solutions to/from Microsoft. In a high security environment, preventing this information from being sent can help reduce privacy concerns for sensitive corporate information.

Impact:

Sending and viewing system-level problem reports and solutions to and from Microsoft may no longer 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:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\wercplsupport: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\Problem Reports and Solutions Control Panel Support`

Default Value:

Manual

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> 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 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

5.20 (L2) Ensure 'Remote Access Auto Connection Manager (RasAuto)' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

Creates a connection to a remote network whenever a program references a remote DNS or NetBIOS name or address.

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

Rationale:

The function of this service is to provide a "demand dial" type of functionality. In a high security environment, it is preferred that any remote "dial" connections (whether they be legacy dial-in POTS or VPN) are initiated by the **user**, *not* automatically by the system.

Impact:

"Dial on demand" functionality will no longer operate - remote dial-in (POTS) and VPN connections must be initiated manually by 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:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasAuto: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\Remote Access Auto Connection Manager

Default Value:

Manual

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> 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 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

5.21 (L2) Ensure 'Remote Desktop Configuration (SessionEnv)' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

Remote Desktop Configuration service (RDCS) is responsible for all Remote Desktop related configuration and session maintenance activities that require SYSTEM context. These include per-session temporary folders, RD themes, and RD certificates.

The recommended state for this setting is: Disabled.

Rationale:

In a high security environment, Remote Desktop access is an increased security risk. For these environments, only local console access should be permitted.

Impact:

Users will be unable to use Remote Assistance.

Audit:

Navigate to the UI 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\SYSTEM\CurrentControlSet\Services\SessionEnv: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\Remote Desktop Configuration`

Default Value:

Manual

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> 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 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

5.22 (L2) Ensure 'Remote Desktop Services (TermService)' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

Allows users to connect interactively to a remote computer. Remote Desktop and Remote Desktop Session Host Server depend on this service.

The recommended state for this setting is: Disabled.

Rationale:

In a high security environment, Remote Desktop access is an increased security risk. For these environments, only local console access should be permitted.

Impact:

Remote Desktop Services will not be available 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:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TermService: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\Remote Desktop Services

Default Value:

Manual

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> 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 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

5.23 (L2) Ensure 'Remote Desktop Services UserMode Port Redirector (UmRdpService)' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

Allows the redirection of Printers/Drives/Ports for RDP connections.

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

Rationale:

In a security-sensitive environment, it is desirable to reduce the possible attack surface - preventing the redirection of COM, LPT and PnP ports will reduce the number of unexpected avenues for data exfiltration and/or malicious code transfer within an RDP session.

Impact:

Printers, drives and ports (COM, LPT, PnP, etc.) will not be allowed to be redirected inside RDP sessions.

Audit:

Navigate to the UI 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\SYSTEM\CurrentControlSet\Services\UmRdpService: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\Remote Desktop Services UserMode Port Redirector

Default Value:

Manual

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> 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 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

5.24 (L1) Ensure 'Remote Procedure Call (RPC) Locator (RpcLocator)' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

In Windows 2003 and older versions of Windows, the Remote Procedure Call (RPC) Locator service manages the RPC name service database. In Windows Vista and newer versions of Windows, this service does not provide any functionality and is present for application compatibility.

The recommended state for this setting is: Disabled.

Rationale:

This is a legacy service that has no value or purpose other than application compatibility for very old software. It should be disabled unless there is a specific old application still in use on the system that requires it.

Impact:

No impact, unless an old, legacy application requires 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:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RpcLocator: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\Remote Procedure Call (RPC) Locator

Default Value:

Manual

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> 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 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

5.25 (L2) Ensure 'Remote Registry (RemoteRegistry)' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

Enables remote users to view and modify registry settings on this computer.

The recommended state for this setting is: Disabled.

Rationale:

In a high security environment, exposing the registry to remote access is an increased security risk.

Impact:

The registry can be viewed and modified only by users on the computer.

Note: Many remote administration tools, such as System Center Configuration Manager (SCCM), require the Remote Registry service to be operational for remote management. In addition, many vulnerability scanners use this service to access the registry remotely.

Audit:

Navigate to the UI 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\SYSTEM\CurrentControlSet\Services\RemoteRegistry: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\Remote Registry

Default Value:

Windows 7: Manual

Windows 8.0 and newer: Disabled

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> 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 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

5.26 (L1) Ensure 'Routing and Remote Access (RemoteAccess)' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Offers routing services to businesses in local area and wide area network environments.

The recommended state for this setting is: Disabled.

Rationale:

This service's main purpose is to provide Windows router functionality - this is not an appropriate use of workstations in an enterprise managed environment.

Impact:

The computer will not be able to be configured as a Windows router between different 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:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RemoteAccess: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\Routing and Remote Access

Default Value:

Disabled

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> 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 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

5.27 (L2) Ensure 'Server (LanmanServer)' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

Supports file, print, and named-pipe sharing over the network for this computer. If this service is stopped, these functions will be unavailable.

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

Rationale:

In a high security environment, a secure workstation should only be a *client*, not a server. Sharing workstation resources for remote access increases security risk as the attack surface is notably higher.

Impact:

File, print and named-pipe sharing functions will be unavailable from this machine over the network.

Note: Many remote administration tools, such as System Center Configuration Manager (SCCM), require the Server service to be operational for remote management. In addition, many vulnerability scanners use this service to scan the file system remotely.

Audit:

Navigate to the UI 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\SYSTEM\CurrentControlSet\Services\LanmanServer: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\Server`

Default Value:

Windows 7 through Windows 10 R1703: Automatic

Windows 10 R1709 and newer: Automatic (Trigger Start)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></p> <p>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.</p>		●	●
v7	<p><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>		●	●

5.28 (L1) Ensure 'Simple TCP/IP Services (simptcp)' is set to 'Disabled' or 'Not Installed' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Supports the following TCP/IP services: Character Generator, Daytime, Discard, Echo, and Quote of the Day.

The recommended state for this setting is: Disabled or Not Installed.

Note: This service is not installed by default. It is supplied with Windows, but is installed by enabling an optional Windows feature (*Simple TCPIP services (i.e. echo, daytime etc)*).

Rationale:

The Simple TCP/IP Services have very little purpose in a modern enterprise environment - allowing them might increase exposure and risk for attack.

Impact:

The Simple TCP/IP services (Character Generator, Daytime, Discard, Echo and Quote of the Day) 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:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\simptcp:Start

Remediation:

To establish the recommended configuration via GP, set the following UI path to: Disabled or ensure the service is not installed.

Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Simple TCP/IP Services

Default Value:

Not Installed (Automatic when installed)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> 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 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

5.29 (L2) Ensure 'SNMP Service (SNMP)' is set to 'Disabled' or 'Not Installed' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

Enables Simple Network Management Protocol (SNMP) requests to be processed by this computer.

The recommended state for this setting is: Disabled or Not Installed.

Note: This service is not installed by default. It is supplied with Windows, but is installed by enabling an optional Windows feature (*Simple Network Management Protocol (SNMP)*).

Rationale:

Features that enable inbound network connections increase the attack surface. In a high security environment, management of secure workstations should be handled locally.

Impact:

The computer will be unable to process SNMP requests.

Audit:

Navigate to the UI 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\SYSTEM\CurrentControlSet\Services\SNMP:Start

Remediation:

To establish the recommended configuration via GP, set the following UI path to: Disabled or ensure the service is not installed.

Computer Configuration\Policies\Windows Settings\Security Settings\System Services\SNMP Service

Default Value:

Not Installed (Automatic when installed)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> 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 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

5.30 (L1) Ensure 'Special Administration Console Helper (sacsrv)' is set to 'Disabled' or 'Not Installed' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This service allows administrators to remotely access a command prompt using Emergency Management Services.

The recommended state for this setting is: `Disabled` or `Not Installed`.

Note: This service is not installed by default. It is supplied with Windows, but it is installed by enabling an optional Windows capability (*Windows Emergency Management Services and Serial Console*).

Rationale:

Allowing the use of a remotely accessible command prompt that provides the ability to perform remote management tasks on a computer is a security risk.

Impact:

Users will not have access to a remote command prompt using Emergency Management 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:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\sacsrv:Start`

Remediation:

To establish the recommended configuration via GP, set the following UI path to: `Disabled` or ensure the service is not installed.

`Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Special Administration Console Helper`

Default Value:

Not Installed (Manual when installed)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></p> <p>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.</p>			
v7	<p>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>			

5.31 (L1) Ensure 'SSDP Discovery (SSDPSRV)' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Discovers networked devices and services that use the SSDP discovery protocol, such as UPnP devices. Also announces SSDP devices and services running on the local computer.

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

Rationale:

Universal Plug n Play (UPnP) is a real security risk - it allows automatic discovery and attachment to network devices. Note that UPnP is different than regular Plug n Play (PnP). Workstations should not be advertising their services (or automatically discovering and connecting to networked services) in a security-conscious enterprise managed environment.

Impact:

SSDP-based devices will not be discovered.

Audit:

Navigate to the UI 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\SYSTEM\CurrentControlSet\Services\SSDPSRV: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\SSDP Discovery`

Default Value:

Manual

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> 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 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

5.32 (L1) Ensure 'UPnP Device Host (upnphost)' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Allows UPnP devices to be hosted on this computer.

The recommended state for this setting is: Disabled.

Rationale:

Universal Plug n Play (UPnP) is a real security risk - it allows automatic discovery and attachment to network devices. Notes that UPnP is different than regular Plug n Play (PnP). Workstations should not be advertising their services (or automatically discovering and connecting to networked services) in a security-conscious enterprise managed environment.

Impact:

Any hosted UPnP devices will stop functioning and no additional hosted devices can be added.

Audit:

Navigate to the UI 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\SYSTEM\CurrentControlSet\Services\upnphost: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\UPnP Device Host

Default Value:

Manual

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> 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 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

5.33 (L1) Ensure 'Web Management Service (WMSvc)' is set to 'Disabled' or 'Not Installed' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

The Web Management Service enables remote and delegated management capabilities for administrators to manage for the Web server, sites and applications present on the machine.

The recommended state for this setting is: `Disabled` or `Not Installed`.

Note: This service is not installed by default. It is supplied with Windows, but is installed by enabling an optional Windows feature (*Internet Information Services - Web Management Tools - IIS Management Service*).

Rationale:

Remote web administration of IIS on a workstation is an increased security risk, as the attack surface of that workstation is then greatly increased. If proper security mitigations are not followed, the chance of successful attack increases significantly.

Impact:

Remote web-based management of IIS 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:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WMSvc:Start`

Remediation:

To establish the recommended configuration via GP, set the following UI path to: `Disabled` or ensure the service is not installed.

`Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Web Management Service`

Default Value:

Not Installed (Manual when installed)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></p> <p>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.</p>			
v7	<p>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>			

5.34 (L2) Ensure 'Windows Error Reporting Service (WerSvc)' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

Allows errors to be reported when programs stop working or responding and allows existing solutions to be delivered. Also allows logs to be generated for diagnostic and repair services.

The recommended state for this setting is: Disabled.

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:

If this service is stopped, error reporting might not work correctly and results of diagnostic services and repairs might not be 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:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WerSvc: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\Windows Error Reporting Service

Default Value:

Windows 7: Manual

Windows 8.0 and newer: Manual (Trigger Start)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></p> <p>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.</p>		●	●
v7	<p><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>		●	●

5.35 (L2) Ensure 'Windows Event Collector (Wecsvc)' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This service manages persistent subscriptions to events from remote sources that support WS-Management protocol. This includes Windows Vista event logs, hardware and IPMI-enabled event sources. The service stores forwarded events in a local Event Log.

The recommended state for this setting is: Disabled.

Rationale:

In a high security environment, remote connections to secure workstations should be minimized, and management functions should be done locally.

Impact:

If this service is stopped or disabled event subscriptions cannot be created and forwarded events cannot be accepted.

Note: Many remote management tools and third-party security audit tools depend on this 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:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Wecsvc: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\Windows Event Collector

Default Value:

Manual

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> 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 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

5.36 (L1) Ensure 'Windows Media Player Network Sharing Service (WMPNetworkSvc)' is set to 'Disabled' or 'Not Installed' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Shares Windows Media Player libraries to other networked players and media devices using Universal Plug and Play.

The recommended state for this setting is: Disabled or Not Installed.

Rationale:

Network sharing of media from Media Player has no place in an enterprise managed environment.

Impact:

Windows Media Player libraries will not be shared over the network to other devices and systems.

Audit:

Navigate to the UI 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\SYSTEM\CurrentControlSet\Services\WMPNetworkSvc:Start

Remediation:

To establish the recommended configuration via GP, set the following UI path to: Disabled or ensure the service is not installed.

Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Windows Media Player Network Sharing Service

Default Value:

Manual

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> 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 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

5.37 (L1) Ensure 'Windows Mobile Hotspot Service (icssvc)' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Provides the ability to share a cellular data connection with another device.

The recommended state for this setting is: Disabled.

Rationale:

The capability to run a mobile hotspot from a domain-connected computer could easily expose the internal network to wardrivers or other hackers.

Impact:

The Windows Mobile Hotspot feature 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:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\icssvc: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\Windows Mobile Hotspot Service

Default Value:

Manual (Trigger Start)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> 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 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

5.38 (L2) Ensure 'Windows Push Notifications System Service (WpnService)' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This service runs in session 0 and hosts the notification platform and connection provider which handles the connection between the device and WNS server.

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

Note: In the first two releases of Windows 10 (R1507 & R1511), the display name of this service was initially named *Windows Push Notifications Service* - but it was renamed to *Windows Push Notifications System Service* starting with Windows 10 R1607.

Rationale:

Windows Push Notification Services (WNS) is a mechanism to receive 3rd-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:

Live Tiles and other features will not get live updates.

Audit:

Navigate to the UI 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\SYSTEM\CurrentControlSet\Services\WpnService: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\Windows Push Notifications System Service`

Default Value:

Automatic

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></p> <p>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.</p>			
v7	<p>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>			

5.39 (L2) Ensure 'Windows PushToInstall Service (PushToInstall)' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This service manages Apps that are pushed to the device from the Microsoft Store App running on other devices or the web.

The recommended state for this setting is: Disabled.

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:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PushToInstall: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\Windows PushToInstall Service (PushToInstall)`

Default Value:

Manual (Trigger Start)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> 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 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

5.40 (L2) Ensure 'Windows Remote Management (WS-Management) (WinRM)' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

Windows Remote Management (WinRM) service implements the WS-Management protocol for remote management. WS-Management is a standard web services protocol used for remote software and hardware management. The WinRM service listens on the network for WS-Management requests and processes them.

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

Rationale:

Features that enable inbound network connections increase the attack surface. In a high security environment, management of secure workstations should be handled locally.

Impact:

The ability to remotely manage the system with WinRM will be lost.

Note: Many remote administration tools, such as System Center Configuration Manager (SCCM), may require the WinRM service to be operational for remote management.

Audit:

Navigate to the UI 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\SYSTEM\CurrentControlSet\Services\WinRM: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\Windows Remote Management (WS-Management)`

Default Value:

Manual

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> 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 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

5.41 (L1) Ensure 'World Wide Web Publishing Service (W3SVC)' is set to 'Disabled' or 'Not Installed' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Provides Web connectivity and administration through the Internet Information Services Manager.

The recommended state for this setting is: Disabled or Not Installed.

Note: This service is not installed by default. It is supplied with Windows, but is installed by enabling an optional Windows feature (*Internet Information Services - World Wide Web Services*).

Note #2: An organization may choose to selectively grant exceptions to web developers to allow IIS (or another web server) on their workstation, in order for them to locally test & develop web pages. However, the organization should track those machines and ensure the security controls and mitigations are kept up to date, to reduce risk of compromise.

Rationale:

Hosting a website from a workstation is an increased security risk, as the attack surface of that workstation is then greatly increased. If proper security mitigations are not followed, the chance of successful attack increases significantly.

Note: This security concern applies to *any* web server application installed on a workstation, not just IIS.

Impact:

IIS Web Services will 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:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC:Start
--

Remediation:

To establish the recommended configuration via GP, set the following UI path to: Disabled or ensure the service is not installed.

Computer Configuration\Policies\Windows Settings\Security Settings\System Services\World Wide Web Publishing Service

Default Value:

Not Installed (Automatic when installed)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</p> <p>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.</p>		●	●
v7	<p>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>		●	●

5.42 (L1) Ensure 'Xbox Accessory Management Service (XboxGipSvc)' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This service manages connected Xbox Accessories.

The recommended state for this setting is: Disabled.

Rationale:

Xbox Live is a gaming service and has no place in an enterprise managed environment (perhaps unless it is a gaming company).

Impact:

Connected Xbox accessories 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:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\XboxGipSvc: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\Xbox Accessory Management Service

Default Value:

Windows 10 R1703: Manual

Windows 10 R1709 and newer: Manual (Trigger Start)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> 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 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

5.43 (L1) Ensure 'Xbox Live Auth Manager (XblAuthManager)' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Provides authentication and authorization services for interacting with Xbox Live.

The recommended state for this setting is: Disabled.

Rationale:

Xbox Live is a gaming service and has no place in an enterprise managed environment (perhaps unless it is a gaming company).

Impact:

Connections to Xbox Live may fail and applications that interact with that service may also 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:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\XblAuthManager: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\Xbox Live Auth Manager

Default Value:

Manual

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> 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 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

5.44 (L1) Ensure 'Xbox Live Game Save (XblGameSave)' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This service syncs save data for Xbox Live save enabled games.

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

Rationale:

Xbox Live is a gaming service and has no place in an enterprise managed environment (perhaps unless it is a gaming company).

Impact:

Game save data will not upload to or download from Xbox Live.

Audit:

Navigate to the UI 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\SYSTEM\CurrentControlSet\Services\XblGameSave: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\Xbox Live Game Save`

Default Value:

Windows 10 R1507 and R1511: Manual

Windows 10 R1607 and newer: Manual (Trigger Start)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> 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 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

5.45 (L1) Ensure 'Xbox Live Networking Service (XboxNetApiSvc)' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This service supports the Windows.Networking.XboxLive application programming interface.

The recommended state for this setting is: Disabled.

Rationale:

Xbox Live is a gaming service and has no place in an enterprise managed environment (perhaps unless it is a gaming company).

Impact:

Connections to Xbox Live may fail and applications that interact with that service may also 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:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\XboxNetApiSvc: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\Xbox Live Networking Service`

Default Value:

Manual

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 Windows 10 Release 1709.

9.1 Domain Profile

This section contains recommendations for the Domain Profile of the Windows Firewall.

9.1.1 (L1) Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Select On (recommended) to have Windows Firewall with Advanced Security use the settings for this profile to filter network traffic. If you select Off, Windows Firewall with Advanced Security will not use any of the firewall rules or connection security rules for this profile.

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 an attacker 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:

HKEY_LOCAL_MACHINE\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 Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Firewall state

Default Value:

On (recommended). (The Windows Firewall with Advanced Security will be active in this profile.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
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.	●	●	●
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 (L1) Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 an attacker 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:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile:  
DefaultInboundAction
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to Block (default):

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows  
Firewall with Advanced Security\Windows Firewall with Advanced  
Security\Windows 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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>4.5 Implement and Manage a Firewall on End-User Devices</p> <p>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.</p>			
v7	<p>9.4 Apply Host-based Firewalls or Port Filtering</p> <p>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.</p>			
v7	<p>11.2 Document Traffic Configuration Rules</p> <p>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.</p>			

9.1.3 (L1) Ensure 'Windows Firewall: Domain: Outbound connections' is set to 'Allow (default)' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting determines the behavior for outbound connections that do not match an outbound firewall rule.

The recommended state for this setting is: Allow (default).

Rationale:

Some people believe that it is prudent to block all outbound connections except those specifically approved by the user or administrator. Microsoft disagrees with this opinion, blocking outbound connections by default will force users to deal with a large number of dialog boxes prompting them to authorize or block applications such as their web browser or instant messaging software. Additionally, blocking outbound traffic has little value because if an attacker has compromised the system they can reconfigure the firewall anyway.

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:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile:  
DefaultOutboundAction
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to Allow (default):

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows  
Firewall with Advanced Security\Windows Firewall with Advanced  
Security\Windows Firewall Properties\Domain Profile\Outbound connections
```

Default Value:

Allow (default). (The Windows Firewall with Advanced Security will allow all outbound connections in this profile unless there is a firewall rule explicitly blocking it.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
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.	●	●	●
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 (L1) Ensure 'Windows Firewall: Domain: Settings: Display a notification' is set to 'No' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

HKEY_LOCAL_MACHINE\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 Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows 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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
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.	●	●	●
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 (L1) Ensure 'Windows Firewall: Domain: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\domainfw.log' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Use this option 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:

%SystemRoot%\System32\logfiles\firewall\domainfw.log.

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 malicious users.

Impact:

The log file will be stored in the specified 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:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\Logging:LogFilepath

Remediation:

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

%SystemRoot%\System32\logfiles\firewall\domainfw.log:

Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Logging Customize\Name

Default Value:

%SystemRoot%\System32\logfiles\firewall\pfirewall.log

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>4.5 Implement and Manage a Firewall on End-User Devices</p> <p>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.</p>	●	●	●
v8	<p>8.5 Collect Detailed Audit Logs</p> <p>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.</p>		●	●
v7	<p>6.3 Enable Detailed Logging</p> <p>Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.</p>		●	●
v7	<p>9.4 Apply Host-based Firewalls or Port Filtering</p> <p>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.</p>	●	●	●

9.1.6 (L1) Ensure 'Windows Firewall: Domain: Logging: Size limit (KB)' is set to '16,384 KB or greater' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 malicious users.

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:

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 Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Logging Customize\Size limit (KB)

Default Value:

4,096 KB.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
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	6.4 Ensure adequate storage for logs Ensure that all systems that store logs have adequate storage space for the logs generated.		●	●
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.	●	●	●

9.1.7 (L1) Ensure 'Windows Firewall: Domain: Logging: Log dropped packets' is set to 'Yes' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 malicious users.

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:

`HKEY_LOCAL_MACHINE\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 Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows 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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>4.5 Implement and Manage a Firewall on End-User Devices</p> <p>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.</p>	●	●	●
v8	<p>8.5 Collect Detailed Audit Logs</p> <p>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.</p>		●	●
v7	<p>6.3 Enable Detailed Logging</p> <p>Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.</p>		●	●
v7	<p>9.4 Apply Host-based Firewalls or Port Filtering</p> <p>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.</p>	●	●	●

9.1.8 (L1) Ensure 'Windows Firewall: Domain: Logging: Log successful connections' is set to 'Yes' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 malicious users.

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:

`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\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 Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows 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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>4.5 Implement and Manage a Firewall on End-User Devices</p> <p>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.</p>	●	●	●
v8	<p>8.5 Collect Detailed Audit Logs</p> <p>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.</p>		●	●
v7	<p>6.3 Enable Detailed Logging</p> <p>Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.</p>		●	●
v7	<p>9.4 Apply Host-based Firewalls or Port Filtering</p> <p>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.</p>	●	●	●

9.2 Private Profile

This section contains recommendations for the Private Profile of the Windows Firewall.

9.2.1 (L1) Ensure 'Windows Firewall: Private: Firewall state' is set to 'On (recommended)' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Select On (recommended) to have Windows Firewall with Advanced Security use the settings for this profile to filter network traffic. If you select Off, Windows Firewall with Advanced Security will not use any of the firewall rules or connection security rules for this profile.

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 an attacker 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:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PrivateProfile  
: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  
Firewall with Advanced Security\Windows Firewall with Advanced  
Security\Windows Firewall Properties\Private Profile\Firewall state
```

Default Value:

On (recommended). (The Windows Firewall with Advanced Security will be active in this profile.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
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.	●	●	●
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 (L1) Ensure 'Windows Firewall: Private: Inbound connections' is set to 'Block (default)' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 an attacker 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:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PrivateProfile  
:DefaultInboundAction
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Block (default)`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows  
Firewall with Advanced Security\Windows Firewall with Advanced  
Security\Windows 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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>4.5 Implement and Manage a Firewall on End-User Devices</p> <p>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.</p>			
v7	<p>9.4 Apply Host-based Firewalls or Port Filtering</p> <p>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.</p>			
v7	<p>11.2 Document Traffic Configuration Rules</p> <p>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.</p>			

9.2.3 (L1) Ensure 'Windows Firewall: Private: Outbound connections' is set to 'Allow (default)' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting determines the behavior for outbound connections that do not match an outbound firewall rule.

The recommended state for this setting is: Allow (default).

Note: If you set Outbound connections to Block and then deploy the firewall policy by using a GPO, computers that receive the GPO settings cannot receive subsequent Group Policy updates unless you create and deploy an outbound rule that enables Group Policy to work. Predefined rules for Core Networking include outbound rules that enable Group Policy to work. Ensure that these outbound rules are active, and thoroughly test firewall profiles before deploying.

Rationale:

Some people believe that it is prudent to block all outbound connections except those specifically approved by the user or administrator. Microsoft disagrees with this opinion, blocking outbound connections by default will force users to deal with a large number of dialog boxes prompting them to authorize or block applications such as their web browser or instant messaging software. Additionally, blocking outbound traffic has little value because if an attacker has compromised the system they can reconfigure the firewall anyway.

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:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PrivateProfile :DefaultOutboundAction

Remediation:

To establish the recommended configuration via GP, set the following UI path to Allow (default):

Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Outbound connections

Default Value:

Allow (default). (The Windows Firewall with Advanced Security will allow all outbound connections in this profile unless there is a firewall rule explicitly blocking it.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
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.	●	●	●
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 (L1) Ensure 'Windows Firewall: Private: Settings: Display a notification' is set to 'No' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PrivateProfile  
:DisableNotifications
```

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows  
Firewall with Advanced Security\Windows Firewall with Advanced  
Security\Windows 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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
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.	●	●	●
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 (L1) Ensure 'Windows Firewall: Private: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\privatefw.log' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Use this option 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:

%SystemRoot%\System32\logfiles\firewall\privatefw.log.

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 malicious users.

Impact:

The log file will be stored in the specified 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:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PrivateProfile
\Logging:LogFilePath

Remediation:

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

%SystemRoot%\System32\logfiles\firewall\privatefw.log:

Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Logging Customize\Name

Default Value:

%SystemRoot%\System32\logfiles\firewall\pfirewall.log

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>4.5 Implement and Manage a Firewall on End-User Devices</p> <p>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.</p>	●	●	●
v8	<p>8.5 Collect Detailed Audit Logs</p> <p>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.</p>		●	●
v7	<p>6.3 Enable Detailed Logging</p> <p>Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.</p>		●	●
v7	<p>9.4 Apply Host-based Firewalls or Port Filtering</p> <p>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.</p>	●	●	●

9.2.6 (L1) Ensure 'Windows Firewall: Private: Logging: Size limit (KB)' is set to '16,384 KB or greater' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 malicious users.

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:

```
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
Firewall with Advanced Security\Windows Firewall with Advanced
Security\Windows Firewall Properties\Private Profile\Logging Customize\Size
limit (KB)
```

Default Value:

4,096 KB.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>4.5 Implement and Manage a Firewall on End-User Devices</p> <p>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.</p>	●	●	●
v8	<p>8.5 Collect Detailed Audit Logs</p> <p>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.</p>		●	●
v7	<p>6.4 Ensure adequate storage for logs</p> <p>Ensure that all systems that store logs have adequate storage space for the logs generated.</p>		●	●
v7	<p>9.4 Apply Host-based Firewalls or Port Filtering</p> <p>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.</p>	●	●	●

9.2.7 (L1) Ensure 'Windows Firewall: Private: Logging: Log dropped packets' is set to 'Yes' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 malicious users.

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:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PrivateProfile  
\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 Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows 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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>4.5 Implement and Manage a Firewall on End-User Devices</p> <p>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.</p>	●	●	●
v8	<p>8.5 Collect Detailed Audit Logs</p> <p>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.</p>		●	●
v7	<p>6.3 Enable Detailed Logging</p> <p>Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.</p>		●	●
v7	<p>9.4 Apply Host-based Firewalls or Port Filtering</p> <p>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.</p>	●	●	●

9.2.8 (L1) Ensure 'Windows Firewall: Private: Logging: Log successful connections' is set to 'Yes' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 malicious users.

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:

HKEY_LOCAL_MACHINE\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 Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows 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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>4.5 Implement and Manage a Firewall on End-User Devices</p> <p>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.</p>	●	●	●
v8	<p>8.5 Collect Detailed Audit Logs</p> <p>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.</p>		●	●
v7	<p>6.3 Enable Detailed Logging</p> <p>Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.</p>		●	●
v7	<p>9.4 Apply Host-based Firewalls or Port Filtering</p> <p>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.</p>	●	●	●

9.3 Public Profile

This section contains recommendations for the Public Profile of the Windows Firewall.

9.3.1 (L1) Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Select On (recommended) to have Windows Firewall with Advanced Security use the settings for this profile to filter network traffic. If you select Off, Windows Firewall with Advanced Security will not use any of the firewall rules or connection security rules for this profile.

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 an attacker 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:

```
HKEY_LOCAL_MACHINE\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  
Firewall with Advanced Security\Windows Firewall with Advanced  
Security\Windows Firewall Properties\Public Profile\Firewall state
```

Default Value:

On (recommended). (The Windows Firewall with Advanced Security will be active in this profile.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
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.	●	●	●
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 (L1) Ensure 'Windows Firewall: Public: Inbound connections' is set to 'Block (default)' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 an attacker 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:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile:
DefaultInboundAction

Remediation:

To establish the recommended configuration via GP, set the following UI path to Block (default):

Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows 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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>4.5 Implement and Manage a Firewall on End-User Devices</p> <p>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.</p>			
v7	<p>9.4 Apply Host-based Firewalls or Port Filtering</p> <p>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.</p>			
v7	<p>11.2 Document Traffic Configuration Rules</p> <p>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.</p>			

9.3.3 (L1) Ensure 'Windows Firewall: Public: Outbound connections' is set to 'Allow (default)' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting determines the behavior for outbound connections that do not match an outbound firewall rule.

The recommended state for this setting is: Allow (default).

Note: If you set Outbound connections to Block and then deploy the firewall policy by using a GPO, computers that receive the GPO settings cannot receive subsequent Group Policy updates unless you create and deploy an outbound rule that enables Group Policy to work. Predefined rules for Core Networking include outbound rules that enable Group Policy to work. Ensure that these outbound rules are active, and thoroughly test firewall profiles before deploying.

Rationale:

Some people believe that it is prudent to block all outbound connections except those specifically approved by the user or administrator. Microsoft disagrees with this opinion, blocking outbound connections by default will force users to deal with a large number of dialog boxes prompting them to authorize or block applications such as their web browser or instant messaging software. Additionally, blocking outbound traffic has little value because if an attacker has compromised the system they can reconfigure the firewall anyway.

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:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile: DefaultOutboundAction
--

Remediation:

To establish the recommended configuration via GP, set the following UI path to Allow (default):

Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Outbound connections

Default Value:

Allow (default). (The Windows Firewall with Advanced Security will allow all outbound connections in this profile unless there is a firewall rule explicitly blocking it.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
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.	●	●	●
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 (L1) Ensure 'Windows Firewall: Public: Settings: Display a notification' is set to 'No' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile:
DisableNotifications

Remediation:

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

Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows 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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>4.5 Implement and Manage a Firewall on End-User Devices</p> <p>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.</p>			
v7	<p>9.4 Apply Host-based Firewalls or Port Filtering</p> <p>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.</p>			
v7	<p>11.2 Document Traffic Configuration Rules</p> <p>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.</p>			

9.3.5 (L1) Ensure 'Windows Firewall: Public: Settings: Apply local firewall rules' is set to 'No' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile:  
AllowLocalPolicyMerge
```

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows  
Firewall with Advanced Security\Windows Firewall with Advanced  
Security\Windows Firewall Properties\Public Profile\Settings Customize\Apply  
local firewall rules
```

Default Value:

Yes (default). (Firewall rules created by administrators will be applied.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
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.	●	●	●
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	11.3 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.		●	●

9.3.6 (L1) Ensure 'Windows Firewall: Public: Settings: Apply local connection security rules' is set to 'No' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile:
AllowLocalIPsecPolicyMerge

Remediation:

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

Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows 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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>4.5 Implement and Manage a Firewall on End-User Devices</p> <p>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.</p>			
v7	<p>9.4 Apply Host-based Firewalls or Port Filtering</p> <p>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.</p>			
v7	<p>11.2 Document Traffic Configuration Rules</p> <p>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.</p>			

9.3.7 (L1) Ensure 'Windows Firewall: Public: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\publicfw.log' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Use this option 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:

%SystemRoot%\System32\logfiles\firewall\publicfw.log.

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 malicious users.

Impact:

The log file will be stored in the specified 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:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile\Logging:LogFilepath

Remediation:

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

%SystemRoot%\System32\logfiles\firewall\publicfw.log:

Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Logging Customize\Name

Default Value:

%SystemRoot%\System32\logfiles\firewall\pfirewall.log

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>4.5 Implement and Manage a Firewall on End-User Devices</p> <p>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.</p>	●	●	●
v8	<p>8.5 Collect Detailed Audit Logs</p> <p>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.</p>		●	●
v7	<p>6.3 Enable Detailed Logging</p> <p>Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.</p>		●	●
v7	<p>9.4 Apply Host-based Firewalls or Port Filtering</p> <p>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.</p>	●	●	●

9.3.8 (L1) Ensure 'Windows Firewall: Public: Logging: Size limit (KB)' is set to '16,384 KB or greater' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 malicious users.

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:

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 Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Logging Customize\Size limit (KB)

Default Value:

4,096 KB.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>4.5 Implement and Manage a Firewall on End-User Devices</p> <p>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.</p>	●	●	●
v8	<p>8.5 Collect Detailed Audit Logs</p> <p>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.</p>		●	●
v7	<p>6.4 Ensure adequate storage for logs</p> <p>Ensure that all systems that store logs have adequate storage space for the logs generated.</p>		●	●
v7	<p>9.4 Apply Host-based Firewalls or Port Filtering</p> <p>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.</p>	●	●	●

9.3.9 (L1) Ensure 'Windows Firewall: Public: Logging: Log dropped packets' is set to 'Yes' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 malicious users.

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:

`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile\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 Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows 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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>4.5 Implement and Manage a Firewall on End-User Devices</p> <p>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.</p>	●	●	●
v8	<p>8.5 Collect Detailed Audit Logs</p> <p>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.</p>		●	●
v7	<p>6.3 Enable Detailed Logging</p> <p>Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.</p>		●	●
v7	<p>9.4 Apply Host-based Firewalls or Port Filtering</p> <p>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.</p>	●	●	●

9.3.10 (L1) Ensure 'Windows Firewall: Public: Logging: Log successful connections' is set to 'Yes' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 malicious users.

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:

HKEY_LOCAL_MACHINE\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 Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows 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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>4.5 Implement and Manage a Firewall on End-User Devices</p> <p>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.</p>	●	●	●
v8	<p>8.5 Collect Detailed Audit Logs</p> <p>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.</p>		●	●
v7	<p>6.3 Enable Detailed Logging</p> <p>Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.</p>		●	●
v7	<p>9.4 Apply Host-based Firewalls or Port Filtering</p> <p>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.</p>	●	●	●

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 (L1) Ensure 'Audit Credential Validation' is set to 'Success and Failure' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

Auditing these events may be useful when investigating a security incident.

Impact:

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.

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 Success and Failure:

Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Logon\Audit Credential Validation

Default Value:

No Auditing.

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 (L1) Ensure 'Audit Application Group Management' is set to 'Success and Failure' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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.

Rationale:

Auditing events in this category may be useful when investigating an incident.

Impact:

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.

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 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. <https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-application-group-management>

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 (L1) Ensure 'Audit Security Group Management' is set to include 'Success' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

Auditing these events may be useful when investigating a security incident.

Impact:

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.

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 Success:

Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Security Group Management

Default Value:

Success.

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.		●	●

17.2.3 (L1) Ensure 'Audit User Account Management' is set to 'Success and Failure' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

Auditing these events may be useful when investigating a security incident.

Impact:

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.

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 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.

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 (L1) Ensure 'Audit PNP Activity' is set to include 'Success' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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.

Impact:

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.

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 Success:

Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Detailed Tracking\Audit PNP Activity

Default Value:

No Auditing.

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 (L1) Ensure 'Audit Process Creation' is set to include 'Success' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

Auditing these events may be useful when investigating a security incident.

Impact:

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.

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 Success:

Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Detailed Tracking\Audit Process Creation

Default Value:

No Auditing.

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

17.5 Logon/Logoff

This section contains recommendations for configuring the Logon/Logoff audit policy.

17.5.1 (L1) Ensure 'Audit Account Lockout' is set to include 'Failure' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

Auditing these events may be useful when investigating a security incident.

Impact:

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.

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 Failure:

Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Account Lockout

Default Value:

Success.

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 (L1) Ensure 'Audit Group Membership' is set to include 'Success' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

Auditing these events may be useful when investigating a security incident.

Impact:

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.

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 Success:

Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Group Membership

Default Value:

No Auditing.

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	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.		●	●
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.		●	●

17.5.3 (L1) Ensure 'Audit Logoff' is set to include 'Success' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

Auditing these events may be useful when investigating a security incident.

Impact:

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.

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 Success:

Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Logoff

Default Value:

Success.

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 (L1) Ensure 'Audit Logon' is set to 'Success and Failure' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

Auditing these events may be useful when investigating a security incident.

Impact:

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.

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 Success and Failure:

Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Logon

Default Value:

Success.

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 (L1) Ensure 'Audit Other Logon/Logoff Events' is set to 'Success and Failure' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

Auditing these events may be useful when investigating a security incident.

Impact:

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.

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 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.

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 (L1) Ensure 'Audit Special Logon' is set to include 'Success' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

Auditing these events may be useful when investigating a security incident.

Impact:

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.

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 Success:

Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Special Logon

Default Value:

Success.

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 (L1) Ensure 'Audit Detailed File Share' is set to include 'Failure' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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.

Impact:

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.

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 Failure:

Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Object Access\Audit Detailed File Share

Default Value:

No Auditing.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
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 (L1) Ensure 'Audit File Share' is set to 'Success and Failure' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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, workstations should have limited file sharing activity, as file servers would normally handle the overall burden of file sharing activities. Any unusual file sharing activity on workstations may therefore be useful in an investigation of potentially malicious activity.

Impact:

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.

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 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.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
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 (L1) Ensure 'Audit Other Object Access Events' is set to 'Success and Failure' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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.

Impact:

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.

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 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.

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 (L1) Ensure 'Audit Removable Storage' is set to 'Success and Failure' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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.

Impact:

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.

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 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.

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 (L1) Ensure 'Audit Audit Policy Change' is set to include 'Success' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 to include: Success.

Rationale:

Auditing these events may be useful when investigating a security incident.

Impact:

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.

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

Success:

Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Policy Change\Audit Audit Policy Change

Default Value:

Success.

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 (L1) Ensure 'Audit Authentication Policy Change' is set to include 'Success' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

Auditing these events may be useful when investigating a security incident.

Impact:

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.

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

Success:

Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Policy Change\Audit Authentication Policy Change

Default Value:

Success.

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 (L1) Ensure 'Audit Authorization Policy Change' is set to include 'Success' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This subcategory reports changes in authorization policy. Events for this subcategory include:

- 4704: A user right was assigned.
- 4705: A user right was removed.
- 4706: A new trust was created to a domain.
- 4707: A trust to a domain was removed.
- 4714: Encrypted data recovery policy was changed.

The recommended state for this setting is to include: Success.

Rationale:

Auditing these events may be useful when investigating a security incident.

Impact:

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.

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 Success:

Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Policy Change\Audit Authorization Policy Change

Default Value:

Success.

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 (L1) Ensure 'Audit MPSSVC Rule-Level Policy Change' is set to 'Success and Failure' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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.

Impact:

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.

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 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.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>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.</p>		●	●
v7	<p>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.</p>		●	●
v7	<p>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.</p>		●	●

17.7.5 (L1) Ensure 'Audit Other Policy Change Events' is set to include 'Failure' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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.

Impact:

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.

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 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.

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.		●	●

17.8 Privilege Use

This section contains recommendations for configuring the Privilege Use audit policy.

17.8.1 (L1) Ensure 'Audit Sensitive Privilege Use' is set to 'Success and Failure' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 and Failure.

Rationale:

Auditing these events may be useful when investigating a security incident.

Impact:

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.

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 Success and Failure:

Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Privilege Use\Audit Sensitive Privilege Use

Default Value:

No Auditing.

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 (L1) Ensure 'Audit IPsec Driver' is set to 'Success and Failure' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

Auditing these events may be useful when investigating a security incident.

Impact:

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.

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 Success and Failure:

Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\System\Audit IPsec Driver

Default Value:

No Auditing.

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 (L1) Ensure 'Audit Other System Events' is set to 'Success and Failure' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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.

Impact:

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.

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 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.

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 (L1) Ensure 'Audit Security State Change' is set to include 'Success' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 audit-able activity might not have been recorded.

The recommended state for this setting is to include: Success.

Rationale:

Auditing these events may be useful when investigating a security incident.

Impact:

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.

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

Success:

Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\System\Audit Security State Change

Default Value:

Success.

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 (L1) Ensure 'Audit Security System Extension' is set to include 'Success' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

Auditing these events may be useful when investigating a security incident.

Impact:

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.

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 Success:

Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\System\Audit Security System Extension

Default Value:

No Auditing.

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 (L1) Ensure 'Audit System Integrity' is set to 'Success and Failure' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

Auditing these events may be useful when investigating a security incident.

Impact:

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.

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 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.

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 (L1) Ensure 'Prevent enabling lock screen camera' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

HKEY_LOCAL_MACHINE\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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p>16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.</p>			

18.1.1.2 (L1) Ensure 'Prevent enabling lock screen slide show' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Personalization>NoLockScreenSlideshow

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 & 2012 R2 Administrative Templates (or newer).

Default Value:

Disabled. (Users can enable a slide show that will run after they lock the machine.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p>16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.</p>			

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 (L1) Ensure 'Allow users to enable online speech recognition services' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\InputPersonalization:AllowInputPersonalization

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 (Release 1507) Administrative Templates (or newer).

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Allow input personalization*, but it was renamed to *Allow users to enable online speech recognition services* starting with the Windows 10 R1809 & 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.)

18.1.3 (L2) Ensure 'Allow Online Tips' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

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:

Due to privacy concerns, data should never be sent to any 3rd party since this data could 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:

HKEY_LOCAL_MACHINE\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 Release 1709 Administrative Templates (or newer).

Default Value:

Enabled. (Settings will contact Microsoft content services to retrieve tips and help content.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>			

18.2 LAPS

This section contains recommendations for configuring Microsoft Local Administrator Password Solution (LAPS).

This Group Policy section is provided by the Group Policy template `AdmPwd.admx/adml` that is included with LAPS.

18.2.1 (L1) Ensure LAPS AdmPwd GPO Extension / CSE is installed (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

In May 2015, Microsoft released the Local Administrator Password Solution (LAPS) tool, which is free and supported software that allows an organization to automatically set randomized and unique local Administrator account passwords on domain-attached workstations and Member Servers. The passwords are stored in a confidential attribute of the domain computer account and can be retrieved from Active Directory by approved Sysadmins when needed.

The LAPS tool requires a small Active Directory Schema update in order to implement, as well as installation of a Group Policy Client Side Extension (CSE) on targeted computers. Please see the LAPS documentation for details.

LAPS supports Windows Vista or newer workstation OSes, and Server 2003 or newer server OSes. LAPS does not support standalone computers - they must be joined to a domain.

Note: Organizations that utilize 3rd-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations.

Note #2: LAPS is only designed to manage *local* Administrator passwords, and is therefore not recommended (or supported) for use directly on Domain Controllers, which do not have a traditional local Administrator account. We strongly encourage you to only deploy the LAPS CSE and LAPS GPO settings to member servers and workstations.

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 an attacker 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:

No impact. When installed and registered properly, `AdmPwd.dll` takes no action unless given appropriate GPO commands during Group Policy refresh. It is not a memory-resident agent or service.

In a disaster recovery scenario where Active Directory is not available, the local Administrator password will not be retrievable and a local password reset using a tool (such as Microsoft's Disaster and Recovery Toolset (DaRT) Recovery Image) may be necessary.

Audit:

The LAPS AdmPwd GPO Extension / CSE can be verified to be installed by the presence of the following registry value:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows  
NT\CurrentVersion\Winlogon\GPExtensions\{D76B9641-3288-4f75-942D-  
087DE603E3EA}:DllName
```

Remediation:

In order to utilize LAPS, a minor Active Directory Schema update is required, and a Group Policy Client Side Extension (CSE) must be installed on each managed computer. When LAPS is installed, the file `AdmPwd.dll` must be present in the following location and registered in Windows (the LAPS AdmPwd GPO Extension / CSE installation does this for you):

```
C:\Program Files\LAPS\CSE\AdmPwd.dll
```

Default Value:

Not Installed.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>5.2 Use Unique Passwords</p> <p>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.</p>	●	●	●
v8	<p>5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts</p> <p>Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.</p>	●	●	●
v7	<p>4.4 Use Unique Passwords</p> <p>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.</p>	●	●	●
v7	<p>16.2 Configure Centralized Point of Authentication</p> <p>Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.</p>	●	●	●

18.2.2 (L1) Ensure 'Do not allow password expiration time longer than required by policy' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

In May 2015, Microsoft released the Local Administrator Password Solution (LAPS) tool, which is free and supported software that allows an organization to automatically set randomized and unique local Administrator account passwords on domain-attached workstations and Member Servers. The passwords are stored in a confidential attribute of the domain computer account and can be retrieved from Active Directory by approved Sysadmins when needed.

The LAPS tool requires a small Active Directory Schema update in order to implement, as well as installation of a Group Policy Client Side Extension (CSE) on targeted computers. Please see the LAPS documentation for details.

LAPS supports Windows Vista or newer workstation OSes, and Server 2003 or newer server OSes. LAPS does not support standalone computers - they must be joined to a domain.

The recommended state for this setting is: Enabled.

Note: Organizations that utilize 3rd-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations.

Note #2: LAPS is only designed to manage *local* Administrator passwords, and is therefore not recommended (or supported) for use directly on Domain Controllers, which do not have a traditional local Administrator account. We strongly encourage you to only deploy the LAPS CSE and LAPS GPO settings to member servers and workstations.

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 an attacker 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:

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:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft  
Services\AdmPwd:PwdExpirationProtectionEnabled
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\LAPS\Do not allow  
password expiration time longer than required by policy
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (AdmPwd.admx/adml) is required - it is included with Microsoft Local Administrator Password Solution (LAPS).

Default Value:

Disabled. (Password expiration time may be longer than required by the "Password Settings" policy.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	16.10 Ensure All Accounts Have An Expiration Date Ensure that all accounts have an expiration date that is monitored and enforced.		●	●

18.2.3 (L1) Ensure 'Enable Local Admin Password Management' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

In May 2015, Microsoft released the Local Administrator Password Solution (LAPS) tool, which is free and supported software that allows an organization to automatically set randomized and unique local Administrator account passwords on domain-attached workstations and Member Servers. The passwords are stored in a confidential attribute of the domain computer account and can be retrieved from Active Directory by approved Sysadmins when needed.

The LAPS tool requires a small Active Directory Schema update in order to implement, as well as installation of a Group Policy Client Side Extension (CSE) on targeted computers. Please see the LAPS documentation for details.

LAPS supports Windows Vista or newer workstation OSes, and Server 2003 or newer server OSes. LAPS does not support standalone computers - they must be joined to a domain.

The recommended state for this setting is: Enabled.

Note: Organizations that utilize 3rd-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations.

Note #2: LAPS is only designed to manage *local* Administrator passwords, and is therefore not recommended (or supported) for use directly on Domain Controllers, which do not have a traditional local Administrator account. We strongly encourage you to only deploy the LAPS CSE and LAPS GPO settings to member servers and workstations.

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 an attacker 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 local administrator password is managed (provided that the LAPS AdmPwd GPO Extension / CSE is installed on the target computer (see recommendation *Ensure LAPS AdmPwd GPO Extension / CSE is installed*), the Active Directory domain schema and account permissions have been properly configured on the domain).

In a disaster recovery scenario where Active Directory is not available, the local Administrator password will not be retrievable and a local password reset using a tool (such as Microsoft's Disaster and Recovery Toolset (DaRT) Recovery Image) may be 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:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft Services\AdmPwd:AdmPwdEnabled

Remediation:

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

Computer Configuration\Policies\Administrative Templates\LAPS\Enable Local Admin Password Management

Note: This Group Policy path does not exist by default. An additional Group Policy template (AdmPwd.admx/adm1) is required - it is included with Microsoft Local Administrator Password Solution (LAPS).

Default Value:

Disabled. (Local Administrator password is NOT managed.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>5.2 Use Unique Passwords</p> <p>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.</p>	●	●	●
v8	<p>5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts</p> <p>Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.</p>	●	●	●
v7	<p>4.4 Use Unique Passwords</p> <p>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.</p>	●	●	●
v7	<p>16.2 Configure Centralized Point of Authentication</p> <p>Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.</p>	●	●	●

18.2.4 (L1) Ensure 'Password Settings: Password Complexity' is set to 'Enabled: Large letters + small letters + numbers + special characters' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

In May 2015, Microsoft released the Local Administrator Password Solution (LAPS) tool, which is free and supported software that allows an organization to automatically set randomized and unique local Administrator account passwords on domain-attached workstations and Member Servers. The passwords are stored in a confidential attribute of the domain computer account and can be retrieved from Active Directory by approved Sysadmins when needed.

The LAPS tool requires a small Active Directory Schema update in order to implement, as well as installation of a Group Policy Client Side Extension (CSE) on targeted computers. Please see the LAPS documentation for details.

LAPS supports Windows Vista or newer workstation OSes, and Server 2003 or newer server OSes. LAPS does not support standalone computers - they must be joined to a domain.

The recommended state for this setting is: Enabled: Large letters + small letters + numbers + special characters.

Note: Organizations that utilize 3rd-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations.

Note #2: LAPS is only designed to manage *local* Administrator passwords, and is therefore not recommended (or supported) for use directly on Domain Controllers, which do not have a traditional local Administrator account. We strongly encourage you to only deploy the LAPS CSE and LAPS GPO settings to member servers and workstations.

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 an attacker 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:

LAPS-generated passwords will be required to contain large letters + small letters + numbers + special characters.

Audit:

Navigate to the UI 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\Policies\Microsoft  
Services\AdmPwd:PasswordComplexity
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to Enabled, and configure the Password Complexity option to Large letters + small letters + numbers + special characters:

```
Computer Configuration\Policies\Administrative Templates\LAPS\Password  
Settings
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (AdmPwd.admx/adml) is required - it is included with Microsoft Local Administrator Password Solution (LAPS).

Default Value:

Large letters + small letters + numbers + special characters.

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.			

18.2.5 (L1) Ensure 'Password Settings: Password Length' is set to 'Enabled: 15 or more' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

In May 2015, Microsoft released the Local Administrator Password Solution (LAPS) tool, which is free and supported software that allows an organization to automatically set randomized and unique local Administrator account passwords on domain-attached workstations and Member Servers. The passwords are stored in a confidential attribute of the domain computer account and can be retrieved from Active Directory by approved Sysadmins when needed.

The LAPS tool requires a small Active Directory Schema update in order to implement, as well as installation of a Group Policy Client Side Extension (CSE) on targeted computers. Please see the LAPS documentation for details.

LAPS supports Windows Vista or newer workstation OSes, and Server 2003 or newer server OSes. LAPS does not support standalone computers - they must be joined to a domain.

The recommended state for this setting is: Enabled: 15 or more.

Note: Organizations that utilize 3rd-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations.

Note #2: LAPS is only designed to manage *local* Administrator passwords, and is therefore not recommended (or supported) for use directly on Domain Controllers, which do not have a traditional local Administrator account. We strongly encourage you to only deploy the LAPS CSE and LAPS GPO settings to member servers and workstations.

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 an attacker 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:

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:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft Services\AdmPwd>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\LAPS\Password Settings

Note: This Group Policy path does not exist by default. An additional Group Policy template (AdmPwd.admx/adml) is required - it is included with Microsoft Local Administrator Password Solution (LAPS).

Default Value:

14 characters.

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.	●	●	●

18.2.6 (L1) Ensure 'Password Settings: Password Age (Days)' is set to 'Enabled: 30 or fewer' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

In May 2015, Microsoft released the Local Administrator Password Solution (LAPS) tool, which is free and supported software that allows an organization to automatically set randomized and unique local Administrator account passwords on domain-attached workstations and Member Servers. The passwords are stored in a confidential attribute of the domain computer account and can be retrieved from Active Directory by approved Sysadmins when needed.

The LAPS tool requires a small Active Directory Schema update in order to implement, as well as installation of a Group Policy Client Side Extension (CSE) on targeted computers. Please see the LAPS documentation for details.

LAPS supports Windows Vista or newer workstation OSes, and Server 2003 or newer server OSes. LAPS does not support standalone computers - they must be joined to a domain.

The recommended state for this setting is: Enabled: 30 or fewer.

Note: Organizations that utilize 3rd-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations.

Note #2: LAPS is only designed to manage *local* Administrator passwords, and is therefore not recommended (or supported) for use directly on Domain Controllers, which do not have a traditional local Administrator account. We strongly encourage you to only deploy the LAPS CSE and LAPS GPO settings to member servers and workstations.

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 an attacker 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:

LAPS-generated passwords will be required to have a maximum age of 30 days (or fewer, 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:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft
Services\AdmPwd>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\LAPS\Password Settings

Note: This Group Policy path does not exist by default. An additional Group Policy template (AdmPwd.admx/adml) is required - it is included with Microsoft Local Administrator Password Solution (LAPS).

Default Value:

30 days.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	16.10 Ensure All Accounts Have An Expiration Date Ensure that all accounts have an expiration date that is monitored and enforced.	●	●	●

18.3 MS Security Guide

This section contains settings 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 from Microsoft at [this link](#).

18.3.1 (L1) Ensure 'Apply UAC restrictions to local accounts on network logons' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:
LocalAccountTokenFilterPolicy

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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.4 <u>Restrict Administrator Privileges to Dedicated Administrator Accounts</u> Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	●	●	●
v7	4.3 <u>Ensure the Use of Dedicated Administrative Accounts</u> 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.	●	●	●

18.3.2 (L1) Ensure 'Configure SMB v1 client driver' is set to 'Enabled: Disable driver (recommended)' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 than 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:

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:

Windows 7 and Windows 8.0: Enabled: Manual start.

Windows 8.1 and Windows 10 (up to R1703): Enabled: Automatic start.

Windows 10 R1709 and newer: Enabled: Disable driver.

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.		●	●

18.3.3 (L1) Ensure 'Configure SMB v1 server' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 than 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:

HKEY_LOCAL_MACHINE\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:

Windows 10 R1703 and older: Enabled.

Windows 10 R1709 and newer: Disabled.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●
v7	<u>14.3 Disable Workstation to Workstation Communication</u> 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.		●	●

18.3.4 (L1) Ensure 'Enable Structured Exception Handling Overwrite Protection (SEHOP)' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

```
HKEY_LOCAL_MACHINE\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.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>10.5 Enable Anti-Exploitation Features</p> <p>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™.</p>			
v7	<p>8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies</p> <p>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.</p>			

18.3.5 (L1) Ensure 'Limits print driver installation to Administrators' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether users that 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:

```
HKEY_LOCAL_MACHINE\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\MS Security  
Guide\Limits print driver installation to Administrators
```

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. (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>

18.3.6 (L1) Ensure 'NetBT NodeType configuration' is set to 'Enabled: P-node (recommended)' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

HKEY_LOCAL_MACHINE\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:

B-node (broadcast only) if a WINS server is not configured in NIC properties.

H-node (hybrid - point-to-point first, then broadcast) if a WINS server is configured in NIC properties.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.3.7 (L1) Ensure 'WDigest Authentication' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

When WDigest authentication is enabled, Lsass.exe retains a copy of the user's plaintext password in memory, where it can be at risk of theft. If this setting is not configured, WDigest authentication is disabled in Windows 8.1 and in Windows Server 2012 R2; it is enabled by default in earlier versions of Windows and Windows Server.

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 `UseLogonCredential`, see Microsoft Knowledge Base article 2871997: [Microsoft Security Advisory Update to improve credentials protection and management May 13, 2014](#).

The recommended state for this setting is: Disabled.

Rationale:

Preventing the plaintext storage of credentials in memory may reduce opportunity for credential theft.

Impact:

None - this is also the default configuration for Windows 8.1 and newer.

Audit:

Navigate to the UI 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\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest  
:UseLogonCredential
```

Remediation:

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

Computer Configuration\Policies\Administrative Templates\MS Security Guide\WDigest Authentication (disabling may require KB2871997)

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 8.0 and older: Enabled. (Lsass.exe retains a copy of the user's plaintext password in memory, where it is at risk of theft.)

On Windows 8.1 and newer: Disabled. (Lsass.exe does not retain a copy of the user's plaintext password in memory.)

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.			

18.4 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 from this TechNet blog post: [The MSS settings – Microsoft Security Guidance blog](#)

18.4.1 (L1) Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

HKEY_LOCAL_MACHINE\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 (not recommended)

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.

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.	●	●	

18.4.2 (L1) Ensure 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

An attacker 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:

```
HKEY_LOCAL_MACHINE\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 (protects against packet spoofing)
```

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.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></p> <p>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.</p>			
v7	<p>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>			

18.4.3 (L1) Ensure 'MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

An attacker 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:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters:Disable  
IPSourceRouting
```

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 (protects against packet spoofing)

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.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.	●		●
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.	●		●

18.4.4 (L2) Ensure 'MSS: (DisableSavePassword) Prevent the dial-up password from being saved' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

When you dial a phonebook or VPN entry in Dial-Up Networking, you can use the "Save Password" option so that your Dial-Up Networking password is cached and you will not need to enter it on successive dial attempts. For security, administrators may want to prevent users from caching passwords.

The recommended state for this setting is: Enabled.

Rationale:

An attacker who steals a mobile user's computer could automatically connect to the organization's network if the **Save This Password** check box is selected for the dial-up or VPN networking entry used to connect to your organization's network.

Impact:

Users will not be able to automatically store their logon credentials for dial-up and VPN 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:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\Parameters:DisableSavePassword

Remediation:

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

Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS:(DisableSavePassword) Prevent the dial-up password from being saved

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. (Saving of dial-up and VPN passwords is allowed.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</p> <p>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.</p>			
v7	<p>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>			

18.4.5 (L1) Ensure 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 for your organization. This group policy object is backed by the following registry location:

HKEY_LOCAL_MACHINE\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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.4.6 (L2) Ensure 'MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds' is set to 'Enabled: 300,000 or 5 minutes (recommended)' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

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 (recommended).

Rationale:

An attacker 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:

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 (recommended):

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.

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.	●	●	●

18.4.7 (L1) 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 (L1) - Corporate/Enterprise Environment (general use)

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 malicious user 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.

An attacker 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:

HKEY_LOCAL_MACHINE\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.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</p> <p>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.</p>		●	●
v7	<p>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>		●	●

18.4.8 (L2) Ensure 'MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

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:

An attacker 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:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters:Perform RouterDiscovery

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 (could lead to DoS)

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.

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.			

18.4.9 (L1) Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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](https://docs.microsoft.com/en-us/windows/desktop/applications/dynamic-link-library-search-order)

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:

HKEY_LOCAL_MACHINE\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 (recommended)

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.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.6 Allowlist Authorized Libraries Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, .so, etc., files, are allowed to load into a system process. Block unauthorized libraries from loading into a system process. Reassess bi-annually, or more frequently.		●	●
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.		●	●

18.4.10 (L1) Ensure 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)' is set to 'Enabled: 5 or fewer seconds' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Windows includes a grace period between when the screen saver is launched and when the console is actually locked automatically when screen saver locking is enabled.

The recommended state for this setting is: Enabled: 5 or fewer seconds.

Rationale:

The default grace period that is allowed for user movement before the screen saver lock takes effect is five seconds. If you leave the default grace period configuration, your computer is vulnerable to a potential attack from someone who could approach the console and attempt to log on to the computer before the lock takes effect. An entry to the registry can be made to adjust the length of the grace period.

Impact:

Users will have to enter their passwords to resume their console sessions as soon as the grace period ends after screen saver activation.

Audit:

Navigate to the UI 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:ScreenSaverGracePeriod
--

Remediation:

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

5 or fewer seconds:

```
Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS:  
(ScreenSaverGracePeriod) The time in seconds before the screen saver grace  
period expires (0 recommended)
```

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 seconds.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.3 Configure Automatic Session Locking on Enterprise Assets</u> 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	<u>16.11 Lock Workstation Sessions After Inactivity</u> Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

18.4.11 (L2) Ensure 'MSS: (TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted' is set to 'Enabled: 3' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

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 malicious user 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:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TCPIP6\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 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.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>			

18.4.12 (L2) Ensure 'MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted' is set to 'Enabled: 3' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

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 malicious user 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:

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.

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.	●	●	

18.4.13 (L1) 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 (L1) - Corporate/Enterprise Environment (general use)

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:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Security:WarningLevel

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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
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.	●	●	●

18.5 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.

18.5.1 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.

18.5.2 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).

18.5.3 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).

18.5.4 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.

18.5.4.1 (L1) Ensure 'Configure DNS over HTTPS (DoH) name resolution' is set to 'Enabled: Allow DoH' or higher (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting determines if DNS over HTTPS (DoH) is used by the system. DNS over HTTPS (DoH) is a protocol for performing remote Domain Name System (DNS) resolution over the Hypertext Transfer Protocol Secure (HTTPS). For additional information on DNS over HTTPS (DoH), visit: [Secure DNS Client over HTTPS \(DoH\) on Windows Server 2022 | Microsoft Docs](#).

The recommended state for this setting is: `Enabled: Allow DoH`. Configuring this setting to `Enabled: Require DoH` also conforms to the benchmark.

Rationale:

DNS over HTTPS (DoH) helps protect against DNS spoofing. Spoofing makes a transmission appear to come from a user other than the user who performed the action. It can also help prevent man-in-the-middle (MitM) attacks because the session in-between is encrypted.

Impact:

If the option `Enabled: Require DoH` is chosen, this could limit 3rd party products from logging DNS traffic (in transit) as the traffic would be encrypted while in transit. The `Require DoH` option could also lead to domain-joined systems not functioning properly within the environment.

The option `Enabled: Allow DoH` will perform DoH queries if the configured DNS servers support it. If they don't support it, classic name resolution will be used. This is the safest option.

Note: Per Microsoft, don't enable the `Enabled: Require DoH` option for domain-joined computers as Active Directory Domain Services is heavily reliant on DNS because the Windows Server DNS Server service does not support DoH queries.

Audit:

Navigate to the UI 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\Policies\Microsoft\Windows NT\DNSClient:DoHPolicy`

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Allow DoH` (configuring to `Enabled: Require DoH` also conforms to the benchmark):

`Computer Configuration\Policies\Administrative Templates\Network\DNS Client\Configure DNS over HTTPS (DoH) 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 10 Release 21H2 Administrative Templates (or newer).

Default Value:

Disabled. (The computer will use locally configured settings.)

References:

1. <https://docs.microsoft.com/en-us/windows-server/networking/dns/doh-client-support>

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.		●	●

18.5.4.2 (L1) Ensure 'Turn off multicast name resolution' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

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:

An attacker 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:

```
HKEY_LOCAL_MACHINE\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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</p> <p>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.</p>		●	●
v7	<p>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>		●	●

18.5.5 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 Release 1607 & Server 2016 Administrative Templates (or newer).

18.5.5.1 (L2) Ensure 'Enable Font Providers' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

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:

`HKEY_LOCAL_MACHINE\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 Release 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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	16.5 Use Up-to-Date and Trusted Third-Party Software Components Use up-to-date and trusted third-party software components. When possible, choose established and proven frameworks and libraries that provide adequate security. Acquire these components from trusted sources or evaluate the software for vulnerabilities before use.			
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.			

18.5.6 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).

18.5.7 Lanman Server

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 `LanmanServer.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.5.8 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 (Release 1507) Administrative Templates (or newer).

18.5.8.1 (L1) Ensure 'Enable insecure guest logons' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 10 R1709: [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:

```
HKEY_LOCAL_MACHINE\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 Release 1511 Administrative Templates (or newer).

Default Value:

Windows 10 R1703 and older: Enabled. (The SMB client will allow insecure guest logons.)

Windows 10 R1709 and newer: Disabled. (The SMB client will reject insecure guest logons.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.5.9 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.

18.5.9.1 (L2) Ensure 'Turn on Mapper I/O (LLTDIO) driver' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

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:

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 locations:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\LLTD:AllowLLTDIOOnDomain  
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\LLTD:AllowLLTDIOOnPublicNet  
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\LLTD:EnableLLTDIO  
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\LLTD:ProhibitLLTDIOOnPrivateNet
```

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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>		●	●

18.5.9.2 (L2) Ensure 'Turn on Responder (RSPNDR) driver' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

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:

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 locations:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\LLTD:AllowRspndrOnDomain  
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\LLTD:AllowRspndrOnPublicNet  
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\LLTD:EnableRspndr  
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\LLTD:ProhibitRspndrOnPrivateNet
```

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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.5.10 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.

18.5.10.1 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.

18.5.10.2 (L2) Ensure 'Turn off Microsoft Peer-to-Peer Networking Services' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

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:

HKEY_LOCAL_MACHINE\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-pnrv.admx/adml that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Peer-to-peer protocols are turned on.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.5.11 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.

18.5.11.1 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 Release 1709 Administrative Templates.

18.5.11.2 (L1) Ensure 'Prohibit installation and configuration of Network Bridge on your DNS domain network' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

HKEY_LOCAL_MACHINE\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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.2 Establish and Maintain a Secure Network Architecture Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.		●	●
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.		●	●

18.5.11.3 (L1) Ensure 'Prohibit use of Internet Connection Sharing on your DNS domain network' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

HKEY_LOCAL_MACHINE\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.)

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.			
v8	12.2 Establish and Maintain a Secure Network Architecture Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.			
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.			

18.5.11.4 (L1) Ensure 'Require domain users to elevate when setting a network's location' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

HKEY_LOCAL_MACHINE\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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.4 <u>Restrict Administrator Privileges to Dedicated Administrator Accounts</u> Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	●	●	●
v7	4.3 <u>Ensure the Use of Dedicated Administrative Accounts</u> 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.	●	●	●

18.5.12 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.

18.5.13 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).

18.5.14 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 (Release 1507) Administrative Templates (or newer).

18.5.14.1 (L1) Ensure 'Hardened UNC Paths' is set to 'Enabled, with "Require Mutual Authentication" and "Require Integrity" set for all NETLOGON and SYSVOL shares' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting configures secure access to UNC paths.

The recommended state for this setting is: Enabled, with "Require Mutual Authentication" and "Require Integrity" set for all NETLOGON and SYSVOL shares.

Note: If the environment exclusively contains Windows 8.0 / Server 2012 (non-R2) or newer systems, then the "Privacy" setting may (optionally) also be set to enable SMB encryption. However, using SMB encryption will render the targeted share paths completely inaccessible by older OSes, so only use this additional option with caution and thorough testing.

Rationale:

In February 2015, Microsoft released a new control mechanism to mitigate a security risk in Group Policy as part of the [MS15-011](#) / [MSKB 3000483](#) security update. This mechanism 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  
\*\*\*\SYSVOL RequireMutualAuthentication=1, RequireIntegrity=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:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\Harden edPaths:*\NETLOGON
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\Harden edPaths:*\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  
\*\*\*\SYSVOL RequireMutualAuthentication=1, RequireIntegrity=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 (Release 1507) Administrative Templates (or newer).

Default Value:

Disabled. (No UNC paths are hardened.)

18.5.15 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.

18.5.16 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.

18.5.17 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.

18.5.18 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.

18.5.19 TCP/IP 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).

18.5.19.1 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).

18.5.19.2 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).

18.5.19.2.1 (L2) Disable IPv6 (Ensure TCPIP6 Parameter 'DisabledComponents' is set to '0xff (255)' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

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.

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 Registry path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration, set the following Registry value to 0xff (255) (DWORD):

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TCPIP6\Parameters:DisabledComponents
```

Note: This change does not take effect until the computer has been restarted.

Note #2: Although Microsoft does not provide an ADMX template to configure this registry value, a custom .ADM template ([Disable-IPv6-Components-KB929852.adm](#)) is provided in the CIS Benchmark Remediation Kit to facilitate its configuration. Be aware though that simply turning off the group policy setting in the .ADM 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.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.5.20 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.

18.5.20.1 (L2) Ensure 'Configuration of wireless settings using Windows Connect Now' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

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.

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:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WCN\Registrars:EnableRegistrars  
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WCN\Registrars:DisableUPnPRegistrar  
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WCN\Registrars:DisableInBand802DOT11Registrar  
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WCN\Registrars:DisableFlashConfigRegistrar  
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WCN\Registrars:DisableWPDRegistrar
```

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.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
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.			●

18.5.20.2 (L2) Ensure 'Prohibit access of the Windows Connect Now wizards' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

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.

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:

HKEY_LOCAL_MACHINE\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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>			

18.5.21 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).

18.5.21.1 (L1) 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 (L1) - Corporate/Enterprise Environment (general use)

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:

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 Release 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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
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.			●

18.5.21.2 (L1) Ensure 'Prohibit connection to non-domain networks when connected to domain authenticated network' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

HKEY_LOCAL_MACHINE\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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
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.	●	●	●

18.5.22 Wireless 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 `wlansvc.admx/adml` that is included with the Microsoft Windows 10 Release 1511 Administrative Templates (or newer).

18.5.23 WLAN Service

This section contains recommendations for WLAN Service settings.

This Group Policy section is provided by the Group Policy template `wlansvc.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.5.23.1 WLAN Media Cost

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 `wlansvc.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.5.23.2 WLAN Settings

This setting contains recommendations for WLAN Settings.

This Group Policy section is provided by the Group Policy template `wlansvc.admx/adml` that is included with the Microsoft Windows 10 Release 1511 Administrative Templates (or newer).

18.5.23.2.1 (L1) Ensure 'Allow Windows to automatically connect to suggested open hotspots, to networks shared by contacts, and to hotspots offering paid services' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines whether users can enable the following WLAN settings: "Connect to suggested open hotspots," "Connect to networks shared by my contacts," and "Enable paid services".

- "Connect to suggested open hotspots" enables Windows to automatically connect users to open hotspots it knows about by crowdsourcing networks that other people using Windows have connected to.
- "Connect to networks shared by my contacts" enables Windows to automatically connect to networks that the user's contacts have shared with them, and enables users on this device to share networks with their contacts.
- "Enable paid services" enables Windows to temporarily connect to open hotspots to determine if paid services are available.

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

Note: These features are also known by the name "*Wi-Fi Sense*".

Rationale:

Automatically connecting to an open hotspot or network can introduce the system to a rogue network with malicious intent.

Impact:

Connect to suggested open hotspots, Connect to networks shared by my contacts, and Enable paid services will each be turned off and users on the device will be prevented from enabling 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:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WcmSvc\wifinetworkmanager\config:AutoConnectAllowedOEM

Remediation:

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

Computer Configuration\Policies\Administrative Templates\Network\WLAN Service\WLAN Settings\Allow Windows to automatically connect to suggested open hotspots, to networks shared by contacts, and to hotspots offering paid services

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `wlansvc.admx/adml` that is included with the Microsoft Windows 10 Release 1511 Administrative Templates (or newer).

Default Value:

Enabled. (Users can choose to enable or disable either "Connect to suggested open hotspots" or "Connect to networks shared by my contacts".)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
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 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.

18.6.1 (L1) Ensure 'Allow Print Spooler to accept client connections' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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.

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, users will continue to be able to print *from their workstation*. However, the workstation's 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.

Audit:

Navigate to the 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:

HKEY_LOCAL_MACHINE\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>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>		●	●

18.6.2 (L1) 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 (L1) - Corporate/Enterprise Environment (general use)

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:

HKEY_LOCAL_MACHINE\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>

18.6.3 (L1) 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 (L1) - Corporate/Enterprise Environment (general use)

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:

```
HKEY_LOCAL_MACHINE\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>

18.7 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).

18.7.1 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 Release 1803 Administrative Templates (or newer).

18.7.1.1 (L2) Ensure 'Turn off notifications network usage' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

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 3rd-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:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\PushNotifications:NoCloudApplicationNotification

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 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Disabled.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.8 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.

18.8.1 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).

18.8.2 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 Release 1607 & Server 2016 Administrative Templates (or newer).

18.8.3 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).

18.8.3.1 (L1) Ensure 'Include command line in process creation events' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 workstation OSes older than Windows 8.1. However, in February 2015 Microsoft added support for the feature to Windows 7 and Windows 8.0 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:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\  
Audit:ProcessCreationIncludeCmdLine_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. (Process 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

18.8.4 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.

18.8.4.1 (L1) Ensure 'Encryption Oracle Remediation' is set to 'Enabled: Force Updated Clients' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 from Windows Vista onwards are affected by this vulnerability, and will be compatible with this recommendation provided that they have been patched at least 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:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\CredSSP\Parameters: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 Release 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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>7.3 Perform Automated Operating System Patch Management</u> Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v7	<u>3.4 Deploy Automated Operating System Patch Management Tools</u> 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.	●	●	●

18.8.4.2 (L1) Ensure 'Remote host allows delegation of non-exportable credentials' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Remote host allows delegation of non-exportable credentials. 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 attackers 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:

HKEY_LOCAL_MACHINE\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 Release 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>

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	16.5 Encrypt Transmittal of Username and Authentication Credentials Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.		●	●

18.8.5 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 (Release 1507) Administrative Templates (or newer).

18.8.5.1 (NG) Ensure 'Turn On Virtualization Based Security' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) + Next Generation Windows Security (NG)
- Level 1 (L1) + BitLocker (BL) + Next Generation Windows Security (NG)
- Level 2 (L2) + Next Generation Windows Security (NG)
- Level 2 (L2) + BitLocker (BL) + Next Generation Windows Security (NG)
- Next Generation Windows Security (NG) - optional add-on for use in the newest hardware and configuration environments

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.

Audit:

Navigate to the UI 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\Policies\Microsoft\Windows\DeviceGuard:EnableVirtualizationBasedSecurity
```

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 (Release 1507) Administrative Templates (or newer).

Default Value:

Disabled.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 <u>Enable Anti-Exploitation Features</u> 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 <u>Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies</u> 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.		●	●

18.8.5.2 (NG) Ensure 'Turn On Virtualization Based Security: Select Platform Security Level' is set to 'Secure Boot and DMA Protection' (Automated)

Profile Applicability:

- Level 1 (L1) + Next Generation Windows Security (NG)
- Level 1 (L1) + BitLocker (BL) + Next Generation Windows Security (NG)
- Level 2 (L2) + Next Generation Windows Security (NG)
- Level 2 (L2) + BitLocker (BL) + Next Generation Windows Security (NG)
- Next Generation Windows Security (NG) - optional add-on for use in the newest hardware and configuration environments

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: Secure Boot and DMA Protection.

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 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:

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:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DeviceGuard:RequirePlatformSecurityFeatures

Remediation:

To establish the recommended configuration via GP, set the following UI path to 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 (Release 1507) Administrative Templates (or newer).

Default Value:

Disabled.

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.		●	●

18.8.5.3 (NG) Ensure 'Turn On Virtualization Based Security: Virtualization Based Protection of Code Integrity' is set to 'Enabled with UEFI lock' (Automated)

Profile Applicability:

- Level 1 (L1) + Next Generation Windows Security (NG)
- Level 1 (L1) + BitLocker (BL) + Next Generation Windows Security (NG)
- Level 2 (L2) + Next Generation Windows Security (NG)
- Level 2 (L2) + BitLocker (BL) + Next Generation Windows Security (NG)
- Next Generation Windows Security (NG) - optional add-on for use in the newest hardware and configuration environments

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:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DeviceGuard:Hypervisor
EnforcedCodeIntegrity

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 (Release 1507) Administrative Templates (or newer).

Default Value:

Disabled.

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.		●	●

18.8.5.4 (NG) Ensure 'Turn On Virtualization Based Security: Require UEFI Memory Attributes Table' is set to 'True (checked)' (Automated)

Profile Applicability:

- Level 1 (L1) + Next Generation Windows Security (NG)
- Level 1 (L1) + BitLocker (BL) + Next Generation Windows Security (NG)
- Level 2 (L2) + Next Generation Windows Security (NG)
- Level 2 (L2) + BitLocker (BL) + Next Generation Windows Security (NG)
- Next Generation Windows Security (NG) - optional add-on for use in the newest hardware and configuration environments

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:

HKEY_LOCAL_MACHINE\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 Release 1703 Administrative Templates (or newer).

Default Value:

Disabled.

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.	●	●	

18.8.5.5 (NG) Ensure 'Turn On Virtualization Based Security: Credential Guard Configuration' is set to 'Enabled with UEFI lock' (Automated)

Profile Applicability:

- Level 1 (L1) + Next Generation Windows Security (NG)
- Level 1 (L1) + BitLocker (BL) + Next Generation Windows Security (NG)
- Level 2 (L2) + Next Generation Windows Security (NG)
- Level 2 (L2) + BitLocker (BL) + Next Generation Windows Security (NG)
- Next Generation Windows Security (NG) - optional add-on for use in the newest hardware and configuration environments

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.

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: 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:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DeviceGuard:LsaCfgFlags

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: 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 Release 1511 Administrative Templates (or newer).

Default Value:

Disabled.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 <u>Enable Anti-Exploitation Features</u> 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 <u>Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies</u> 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.		●	●

18.8.5.6 (NG) Ensure 'Turn On Virtualization Based Security: Secure Launch Configuration' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) + Next Generation Windows Security (NG)
- Level 1 (L1) + BitLocker (BL) + Next Generation Windows Security (NG)
- Level 2 (L2) + Next Generation Windows Security (NG)
- Level 2 (L2) + BitLocker (BL) + Next Generation Windows Security (NG)
- Next Generation Windows Security (NG) - optional add-on for use in the newest hardware and configuration environments

Description:

Secure Launch protects the Virtualization Based Security environment from exploited vulnerabilities in device firmware.

The recommended state for this setting is: Enabled.

Note: 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:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DeviceGuard:ConfigureSystemGuardLaunch

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 Release 1809 & Server 2019 Administrative Templates (or newer).

Default Value:

Not Configured. (Administrative users can choose whether to enable or disable Secure Launch.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 <u>Enable Anti-Exploitation Features</u> 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 <u>Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies</u> 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.		●	●

18.8.6 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 Release 1709 Administrative Templates (or newer).

18.8.7 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.

18.8.7.1 Device Installation Restrictions

This section contains recommendations related to device installation restrictions.

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.

18.8.7.1.1 (BL) Ensure 'Prevent installation of devices that match any of these device IDs' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) + BitLocker (BL)
- Level 2 (L2) + BitLocker (BL)
- BitLocker (BL) - optional add-on for when BitLocker is deployed

Description:

This policy setting allows you to specify a list of Plug and Play hardware IDs and compatible IDs for devices that Windows is prevented from installing. This policy setting takes precedence over any other policy setting that allows Windows to install a device.

If you enable this policy setting, Windows is prevented from installing a device whose hardware ID or compatible ID appears in the list you create. If you enable this policy setting on a remote desktop server, the policy setting affects redirection of the specified devices from a remote desktop client to the remote desktop server.

If you disable or do not configure this policy setting, devices can be installed and updated as allowed or prevented by other policy settings.

The recommended state for this setting is: Enabled.

Note: In versions of Windows 10 Release 1803 (and newer), there is a new control named *Enumeration policy for external devices incompatible with Kernel DMA Protection* available that mitigates much of the risk for malicious devices that may perform Direct Memory Access (DMA) attacks. The newer control is also now part of the Windows 10 CIS benchmark, in section 18.8.26. However, if your environment still contains **any** Windows 10 Release 1709 (or older) workstations, then the newer control will not work, so this setting remains important to disable Thunderbolt devices on those systems.

Rationale:

A BitLocker-protected computer may be vulnerable to Direct Memory Access (DMA) attacks when the computer is turned on or is in the Standby power state - this includes when the workstation is locked.

BitLocker with TPM-only authentication lets a computer enter the power-on state without any pre-boot authentication. Therefore, an attacker may be able to perform DMA attacks.

This issue is documented in Microsoft Knowledge Base article 2516445: [Blocking the SBP-2 driver and Thunderbolt controllers to reduce 1394 DMA and Thunderbolt DMA threats to BitLocker](#).

Impact:

Devices matching the specified device IDs will be prevented from installation.

Audit:

Navigate to the UI 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\Policies\Microsoft\Windows\DeviceInstall\Restrictions:DenyDeviceIDs

Remediation:

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

Computer Configuration\Policies\Administrative Templates\System\Device Installation\Device Installation Restrictions\Prevent installation of devices that match any of these device IDs

Note: This Group Policy path is provided by the Group Policy template DeviceInstallation.admx/adml that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Devices can be installed and updated as allowed or prevented by other policy settings.)

18.8.7.1.2 (BL) Ensure 'Prevent installation of devices that match any of these device IDs: Prevent installation of devices that match any of these device IDs' is set to 'PCI\CC_0C0A' (Automated)

Profile Applicability:

- Level 1 (L1) + BitLocker (BL)
- Level 2 (L2) + BitLocker (BL)
- BitLocker (BL) - optional add-on for when BitLocker is deployed

Description:

This policy setting allows you to specify a list of Plug and Play hardware IDs and compatible IDs for devices that Windows is prevented from installing. This policy setting takes precedence over any other policy setting that allows Windows to install a device.

If you enable this policy setting, Windows is prevented from installing a device whose hardware ID or compatible ID appears in the list you create. If you enable this policy setting on a remote desktop server, the policy setting affects redirection of the specified devices from a remote desktop client to the remote desktop server.

If you disable or do not configure this policy setting, devices can be installed and updated as allowed or prevented by other policy settings.

The recommended state for this setting is: `PCI\CC_0C0A`

Note: This device ID is for Thunderbolt controllers. The USB Type-C (USB-C) port standard that is now common in many computers, especially laptops, utilizes Thunderbolt technology, and therefore may be affected by this restriction. If your organization needs to use USB-C extensively, you may need to decide, internally, to allow yourselves an exception to this recommendation. However, please ensure that all necessary decision-makers have accepted the increased risk of BitLocker encryption key theft (and therefore data theft) via malicious Thunderbolt devices (when left unattended), by doing so.

Note #2: In versions of Windows 10 Release 1803 (and newer), there is a new control named *Enumeration policy for external devices incompatible with Kernel DMA Protection* available that mitigates much of the risk for malicious devices that may perform Direct Memory Access (DMA) attacks. The newer control is also now part of the Windows 10 CIS benchmark, in section 18.8.26. However, if your environment still contains **any** Windows 10 Release 1709 (or older) workstations, then the newer control will not work, so this setting remains important to disable Thunderbolt devices on those systems.

Rationale:

A BitLocker-protected computer may be vulnerable to Direct Memory Access (DMA) attacks when the computer is turned on or is in the Standby power state - this includes when the workstation is locked.

BitLocker with TPM-only authentication lets a computer enter the power-on state without any pre-boot authentication. Therefore, an attacker may be able to perform DMA attacks.

This issue is documented in Microsoft Knowledge Base article 2516445: [Blocking the SBP-2 driver and Thunderbolt controllers to reduce 1394 DMA and Thunderbolt DMA threats to BitLocker](#).

Impact:

Thunderbolt controllers will be prevented from being installed in 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:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DeviceInstall\Restrictions\DenyDeviceIDs:1

Remediation:

To establish the recommended configuration via GP, set the following UI path to Enabled, and add `PCI\CC_0C0A` to the Device IDs list:

Computer Configuration\Policies\Administrative Templates\System\Device Installation\Device Installation Restrictions\Prevent installation of devices that match any of these device IDs

Note: This Group Policy path is provided by the Group Policy template `DeviceInstallation.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

None. (No device ID types are prevented from installation.)

18.8.7.1.3 (BL) Ensure 'Prevent installation of devices that match any of these device IDs: Also apply to matching devices that are already installed.' is set to 'True' (checked) (Automated)

Profile Applicability:

- Level 1 (L1) + BitLocker (BL)
- Level 2 (L2) + BitLocker (BL)
- BitLocker (BL) - optional add-on for when BitLocker is deployed

Description:

This policy setting allows you to specify a list of Plug and Play hardware IDs and compatible IDs for devices that Windows is prevented from installing. This policy setting takes precedence over any other policy setting that allows Windows to install a device.

If you enable this policy setting, Windows is prevented from installing a device whose hardware ID or compatible ID appears in the list you create. If you enable this policy setting on a remote desktop server, the policy setting affects redirection of the specified devices from a remote desktop client to the remote desktop server.

If you disable or do not configure this policy setting, devices can be installed and updated as allowed or prevented by other policy settings.

The recommended state for this setting is: **True (checked)**.

Note: In versions of Windows 10 Release 1803 (and newer), there is a new control named *Enumeration policy for external devices incompatible with Kernel DMA Protection* available that mitigates much of the risk for malicious devices that may perform Direct Memory Access (DMA) attacks. The newer control is also now part of the Windows 10 CIS benchmark, in section 18.8.26. However, if your environment still contains **any** Windows 10 Release 1709 (or older) workstations, then the newer control will not work, so this setting remains important to disable Thunderbolt devices on those systems.

Rationale:

A BitLocker-protected computer may be vulnerable to Direct Memory Access (DMA) attacks when the computer is turned on or is in the Standby power state - this includes when the workstation is locked.

BitLocker with TPM-only authentication lets a computer enter the power-on state without any pre-boot authentication. Therefore, an attacker may be able to perform DMA attacks.

This issue is documented in Microsoft Knowledge Base article 2516445: [Blocking the SBP-2 driver and Thunderbolt controllers to reduce 1394 DMA and Thunderbolt DMA threats to BitLocker](#).

Impact:

Existing devices (that match the device IDs specified) that were previously installed prior to the hardening will be disabled or removed.

Audit:

Navigate to the UI 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\Policies\Microsoft\Windows\DeviceInstall\Restrictions:DenyDeviceIDsRetroactive
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to Enabled, and check the Also apply to matching devices that are already installed. checkbox:

```
Computer Configuration\Policies\Administrative Templates\System\Device Installation\Device Installation Restrictions\Prevent installation of devices that match any of these device IDs
```

Note: This Group Policy path is provided by the Group Policy template `DeviceInstallation.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

False (unchecked). (Pre-existing devices matching the device IDs will not be disabled or removed.)

18.8.7.1.4 (BL) Ensure 'Prevent installation of devices using drivers that match these device setup classes' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) + BitLocker (BL)
- Level 2 (L2) + BitLocker (BL)
- BitLocker (BL) - optional add-on for when BitLocker is deployed

Description:

This policy setting allows you to specify a list of device setup class globally unique identifiers (GUIDs) for device drivers that Windows is prevented from installing. This policy setting takes precedence over any other policy setting that allows Windows to install a device.

If you enable this policy setting, Windows is prevented from installing or updating device drivers whose device setup class GUIDs appear in the list you create. If you enable this policy setting on a remote desktop server, the policy setting affects redirection of the specified devices from a remote desktop client to the remote desktop server.

If you disable or do not configure this policy setting, Windows can install and update devices as allowed or prevented by other policy settings.

The recommended state for this setting is: Enabled.

Rationale:

A BitLocker-protected computer may be vulnerable to Direct Memory Access (DMA) attacks when the computer is turned on or is in the Standby power state - this includes when the workstation is locked.

BitLocker with TPM-only authentication lets a computer enter the power-on state without any pre-boot authentication. Therefore, an attacker may be able to perform DMA attacks.

This issue is documented in Microsoft Knowledge Base article 2516445: [Blocking the SBP-2 driver and Thunderbolt controllers to reduce 1394 DMA and Thunderbolt DMA threats to BitLocker.](#)

Impact:

Devices matching the specified device setup classes will be prevented from installation.

Audit:

Navigate to the UI 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\Policies\Microsoft\Windows\DeviceInstall\Restrictions:DenyDeviceClasses

Remediation:

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

Computer Configuration\Policies\Administrative Templates\System\Device Installation\Device Installation Restrictions\Prevent installation of devices using drivers that match these device setup classes

Note: This Group Policy path is provided by the Group Policy template DeviceInstallation.admx/adml that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Devices can be installed and updated as allowed or prevented by other policy settings.)

18.8.7.1.5 (BL) Ensure 'Prevent installation of devices using drivers that match these device setup classes: Prevent installation of devices using drivers for these device setup' is set to 'IEEE 1394 device setup classes' (Automated)

Profile Applicability:

- Level 1 (L1) + BitLocker (BL)
- Level 2 (L2) + BitLocker (BL)
- BitLocker (BL) - optional add-on for when BitLocker is deployed

Description:

This policy setting allows you to specify a list of device setup class globally unique identifiers (GUIDs) for device drivers that Windows is prevented from installing. This policy setting takes precedence over any other policy setting that allows Windows to install a device.

If you enable this policy setting, Windows is prevented from installing or updating device drivers whose device setup class GUIDs appear in the list you create. If you enable this policy setting on a remote desktop server, the policy setting affects redirection of the specified devices from a remote desktop client to the remote desktop server.

If you disable or do not configure this policy setting, Windows can install and update devices as allowed or prevented by other policy settings.

Here are the four entries we recommend and what they translate to:

- {d48179be-ec20-11d1-b6b8-00c04fa372a7} - IEEE 1394 devices that support the SBP2 Protocol Class
- {7ebefbc0-3200-11d2-b4c2-00a0C9697d07} - IEEE 1394 devices that support the IEC-61883 Protocol Class
- {c06ff265-ae09-48f0-812c-16753d7cba83} - IEEE 1394 devices that support the AVC Protocol Class
- {6bdd1fc1-810f-11d0-bec7-08002be2092f} - IEEE 1394 Host Bus Controller Class

The full list of system-defined device setup classes available in Windows is here: [System-Defined Device Setup Classes Available to Vendors | Microsoft Docs](#)

The recommended state for this setting is: {d48179be-ec20-11d1-b6b8-00c04fa372a7}, {7ebefbc0-3200-11d2-b4c2-00a0C9697d07}, {c06ff265-ae09-48f0-812c-16753d7cba83}, and {6bdd1fc1-810f-11d0-bec7-08002be2092f}

Note: IEEE 1394 has also been known/branded as *FireWire* (by Apple), *iLINK* (by Sony) and *Lynx* (by Texas Instruments).

Rationale:

A BitLocker-protected computer may be vulnerable to Direct Memory Access (DMA) attacks when the computer is turned on or is in the Standby power state - this includes when the workstation is locked.

BitLocker with TPM-only authentication lets a computer enter the power-on state without any pre-boot authentication. Therefore, an attacker may be able to perform DMA attacks.

This issue is documented in Microsoft Knowledge Base article 2516445: [Blocking the SBP-2 driver and Thunderbolt controllers to reduce 1394 DMA and Thunderbolt DMA threats to BitLocker.](#)

Impact:

IEEE 1394 drives & devices will be prevented from being installed in 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:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DeviceInstall\Restrictions\DenyDeviceClasses:<numeric value>
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to Enabled, and add {d48179be-ec20-11d1-b6b8-00c04fa372a7}, {7ebefbc0-3200-11d2-b4c2-00a0C9697d07}, {c06ff265-ae09-48f0-812c-16753d7cba83}, and {6bdd1fc1-810f-11d0-bec7-08002be2092f} to the device setup classes list:

Computer Configuration\Policies\Administrative Templates\System\Device Installation\Device Installation Restrictions\Prevent installation of devices using drivers that match these device setup classes

Note: This Group Policy path is provided by the Group Policy template DeviceInstallation.admx/adml that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

None. (No device setup classes are prevented from installation.)

Additional Information:

Documented in [MSKB 2516445](#).

18.8.7.1.6 (BL) Ensure 'Prevent installation of devices using drivers that match these device setup classes: Also apply to matching devices that are already installed.' is set to 'True' (checked) (Automated)

Profile Applicability:

- Level 1 (L1) + BitLocker (BL)
- Level 2 (L2) + BitLocker (BL)
- BitLocker (BL) - optional add-on for when BitLocker is deployed

Description:

This policy setting allows you to specify a list of device setup class globally unique identifiers (GUIDs) for device drivers that Windows is prevented from installing. This policy setting takes precedence over any other policy setting that allows Windows to install a device.

If you enable this policy setting, Windows is prevented from installing or updating device drivers whose device setup class GUIDs appear in the list you create. If you enable this policy setting on a remote desktop server, the policy setting affects redirection of the specified devices from a remote desktop client to the remote desktop server.

If you disable or do not configure this policy setting, Windows can install and update devices as allowed or prevented by other policy settings.

The recommended state for this setting is: True (checked).

Rationale:

A BitLocker-protected computer may be vulnerable to Direct Memory Access (DMA) attacks when the computer is turned on or is in the Standby power state - this includes when the workstation is locked.

BitLocker with TPM-only authentication lets a computer enter the power-on state without any pre-boot authentication. Therefore, an attacker may be able to perform DMA attacks.

This issue is documented in Microsoft Knowledge Base article 2516445: [Blocking the SBP-2 driver and Thunderbolt controllers to reduce 1394 DMA and Thunderbolt DMA threats to BitLocker.](#)

Impact:

Existing devices (that match the device setup classes specified) that were previously installed prior to the hardening will be disabled or removed.

Audit:

Navigate to the UI 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\Policies\Microsoft\Windows\DeviceInstall\Restrictions:DenyDeviceClassesRetroactive

Remediation:

To establish the recommended configuration via GP, set the following UI path to Enabled, and check the Also apply to matching devices that are already installed. checkbox:

Computer Configuration\Policies\Administrative Templates\System\Device Installation\Device Installation Restrictions\Prevent installation of devices using drivers that match these device setup classes

Note: This Group Policy path is provided by the Group Policy template DeviceInstallation.admx/adml that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

False (unchecked). (Pre-existing devices matching the device setup classes will not be disabled or removed.)

18.8.7.2 (L1) Ensure 'Prevent device metadata retrieval from the Internet' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 3rd-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 3rd-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 3rd-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:

HKEY_LOCAL_MACHINE\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 device metadata retrieval from the Internet

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).

Default Value:

Disabled. (The setting in the Device Installation Settings dialog box controls whether Windows retrieves device metadata from the Internet.)

18.8.8 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 `DeviceRedirection.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.8.9 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.

18.8.10 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.

18.8.11 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 Release 1703 Administrative Templates (or newer).

18.8.12 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.

18.8.13 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.

18.8.14 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).

18.8.14.1 (L1) Ensure 'Boot-Start Driver Initialization Policy' is set to 'Enabled: Good, unknown and bad but critical' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

```
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.)

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.		●	●

18.8.15 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).

18.8.16 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).

18.8.17 File Share Shadow Copy Agent

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 `FileServerVSSAgent.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.8.18 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).

18.8.19 Filesystem (formerly NTFS Filesystem)

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 `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.

18.8.20 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.

18.8.21 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.

18.8.21.1 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).

18.8.21.2 (L1) Ensure 'Configure registry policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

The "Do not apply during periodic background processing" option prevents the system from updating affected policies in the background while the computer is in use. When background updates are disabled, policy changes will not take effect until the next user logon or system restart.

The recommended state for this setting is: `Enabled: FALSE` (unchecked).

Rationale:

Setting this option to false (unchecked) will ensure that domain policy changes take effect more quickly, as compared to waiting until the next user logon or system restart.

Impact:

Group Policies will be reapplied every time they are refreshed, which could 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:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ Policies\Microsoft\Windows\Group  
Policy\{35378EAC-683F-11D2-A89A-00C04FBBCFA2}: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 registry policy processing
```

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 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Disabled. (Group policies are not reapplied until the next logon or restart.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
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.		●	●

18.8.21.3 (L1) Ensure 'Configure registry policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

The "Process even if the Group Policy objects have not changed" option updates and reapplies policies even if the policies have not changed.

The recommended state for this setting is: Enabled: TRUE (checked).

Rationale:

Setting this option to true (checked) will ensure unauthorized changes that might have been configured locally are forced to match the domain-based Group Policy settings again.

Impact:

Group Policies will be reapplied even if they have not been changed, which could 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:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Group  
Policy\{35378EAC-683F-11D2-A89A-00C04FBBCFA2}: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 registry policy processing

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 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Disabled. (Group policies are not reapplied if they have not been changed.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
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.		●	●

18.8.21.4 (L1) Ensure 'Continue experiences on this device' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

`HKEY_LOCAL_MACHINE\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 Release 1607 & Server 2016 Administrative Templates (or newer).

Default Value:

The default behavior depends on the Windows edition.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>			

18.8.21.5 (L1) Ensure 'Turn off background refresh of Group Policy' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 in effect when the following registry location 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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p>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.</p>			

18.8.22 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.

18.8.22.1 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.

18.8.22.1.1 (L2) Ensure 'Turn off access to the Store' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This policy setting specifies whether to use the Store service for finding an application to open a file with an unhandled file type or protocol association. When a user opens a file type or protocol that is not associated with any applications on the computer, the user is given the choice to select a local application or use the Store service to find an application.

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

Rationale:

The Store service is a retail outlet built into Windows, primarily for consumer use. In an enterprise managed environment the IT department should be managing the installation of all applications to reduce the risk of the installation of vulnerable software.

Impact:

The "Look for an app in the Store" item in the Open With dialog is removed.

Audit:

Navigate to the UI 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\Policies\Microsoft\Windows\Explorer:NoUseStoreOpenWith

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 access to the Store

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template ICM.admx/adml that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Disabled. (Users are allowed to use the Store service and the Store item is available in the Open With dialog.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.	●	●	●

18.8.22.1.2 (L1) Ensure 'Turn off downloading of print drivers over HTTP' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

HKEY_LOCAL_MACHINE\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.)

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.			

18.8.22.1.3 (L2) Ensure 'Turn off handwriting personalization data sharing' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

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:

HKEY_LOCAL_MACHINE\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.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>			

18.8.22.1.4 (L2) Ensure 'Turn off handwriting recognition error reporting' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

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:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\HandwritingErrorReport  
s:PreventHandwritingErrorReports
```

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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>		●	●

18.8.22.1.5 (L2) Ensure 'Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

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:

```
HKEY_LOCAL_MACHINE\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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>			

18.8.22.1.6 (L1) Ensure 'Turn off Internet download for Web publishing and online ordering wizards' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explore
r: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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	7.4 Maintain and Enforce Network-Based URL Filters Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.			

18.8.22.1.7 (L2) Ensure 'Turn off printing over HTTP' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

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 malicious users. 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:

HKEY_LOCAL_MACHINE\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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
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.			●

18.8.22.1.8 (L2) Ensure 'Turn off Registration if URL connection is referring to Microsoft.com' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

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:

HKEY_LOCAL_MACHINE\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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>		●	●

18.8.22.1.9 (L2) Ensure 'Turn off Search Companion content file updates' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

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:

HKEY_LOCAL_MACHINE\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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.8.22.1.10 (L2) Ensure 'Turn off the "Order Prints" picture task' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

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:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explore  
r: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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>		●	●

18.8.22.1.11 (L2) Ensure 'Turn off the "Publish to Web" task for files and folders' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

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 Web Publishing wizard is used to download a list of providers and allow users to publish content to the Web.

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:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorerr:NoPublishingWizard

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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>			

18.8.22.1.12 (L2) Ensure 'Turn off the Windows Messenger Customer Experience Improvement Program' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

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:

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:

HKEY_LOCAL_MACHINE\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.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>			

18.8.22.1.13 (L2) Ensure 'Turn off Windows Customer Experience Improvement Program' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

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 Windows 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:

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:

`HKEY_LOCAL_MACHINE\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.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>		●	●

18.8.22.1.14 (L2) Ensure 'Turn off Windows Error Reporting' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

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:

```
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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>		●	●

18.8.23 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.

18.8.24 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).

18.8.25 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.

18.8.25.1 (L2) Ensure 'Support device authentication using certificate' is set to 'Enabled: Automatic' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

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 locations:

```
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 (Release 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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	1.6 Address Unauthorized Assets Ensure that unauthorized assets are either removed from the network, quarantined or the inventory is updated in a timely manner.	●	●	●
v7	1.8 Utilize Client Certificates to Authenticate Hardware Assets Use client certificates to authenticate hardware assets connecting to the organization's trusted network.			●

18.8.26 Kernel DMA Protection

This section contains recommendations related to Kernel DMA Protection.

This Group Policy section is provided by the Group Policy template `DmaGuard.admx/adml` that is included with the Microsoft Windows 10 Release 1809 and Server 2019 Administrative Templates (or newer).

18.8.26.1 (BL) Ensure 'Enumeration policy for external devices incompatible with Kernel DMA Protection' is set to 'Enabled: Block All' (Automated)

Profile Applicability:

- Level 1 (L1) + BitLocker (BL)
- Level 1 (L1) + BitLocker (BL) + Next Generation Windows Security (NG)
- Level 2 (L2) + BitLocker (BL)
- Level 2 (L2) + BitLocker (BL) + Next Generation Windows Security (NG)
- BitLocker (BL) - optional add-on for when BitLocker is deployed

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 R1803 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:

```
HKEY_LOCAL_MACHINE\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 Release 1809 & Server 2019 Administrative Templates (or newer).

Default Value:

Windows 10 R1803 and newer: Enabled if UEFI BIOS is present. Disabled if using legacy BIOS.

Older OSes: Not supported (i.e. Disabled).

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
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.	●	●	●

18.8.27 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.

18.8.27.1 (L2) Ensure 'Disallow copying of user input methods to the system account for sign-in' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

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:

```
HKEY_LOCAL_MACHINE\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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

18.8.28 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.

18.8.28.1 (L1) Ensure 'Block user from showing account details on sign-in' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

An attacker with access to the console (for example, someone with physical access or someone who is able to connect to the workstation through Remote Desktop Services) could view the name of the last user who logged on to the server. The attacker could then try to guess the password, use a dictionary, or use a brute-force attack to try and log on.

Impact:

Users 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:

```
HKEY_LOCAL_MACHINE\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 Release 1607 & Server 2016 Administrative Templates (or newer).

Default Value:

Disabled. (Users may choose to show account details on the sign-in screen.)

18.8.28.2 (L1) Ensure 'Do not display network selection UI' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

```
HKEY_LOCAL_MACHINE\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.)

18.8.28.3 (L1) Ensure 'Do not enumerate connected users on domain-joined computers' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting prevents connected users from being enumerated on domain-joined computers.

The recommended state for this setting is: Enabled.

Rationale:

A malicious user 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:

HKEY_LOCAL_MACHINE\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.)

18.8.28.4 (L1) Ensure 'Enumerate local users on domain-joined computers' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting allows local users to be enumerated on domain-joined computers.

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

Rationale:

A malicious user 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:

HKEY_LOCAL_MACHINE\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.)

18.8.28.5 (L1) Ensure 'Turn off app notifications on the lock screen' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System:DisableLockScreenAppNotifications

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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.			

18.8.28.6 (L1) Ensure 'Turn off picture password sign-in' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting allows you to control whether a domain user can sign in using a picture password.

The recommended state for this setting is: Enabled.

Note: If the picture password feature is permitted, the user's domain password is cached in the system vault when using it.

Rationale:

Picture passwords bypass the requirement for a typed complex password. In a shared work environment, a simple shoulder surf where someone observed the on-screen gestures would allow that person to gain access to the system without the need to know the complex password. Vertical monitor screens with an image are much more visible at a distance than horizontal key strokes, increasing the likelihood of a successful observation of the mouse gestures.

Impact:

Users will not be able to set up or sign in with a picture password.

Audit:

Navigate to the UI 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\Policies\Microsoft\Windows\System:BlockDomainPicturePassword

Remediation:

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

Computer Configuration\Policies\Administrative Templates\System\Logon\Turn off picture password 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).

Default Value:

Disabled. (Users can set up and use a picture password.)

18.8.28.7 (L1) Ensure 'Turn on convenience PIN sign-in' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

```
HKEY_LOCAL_MACHINE\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 Release 1511 Administrative Templates.

Default Value:

Disabled. (A domain user can't set up and use a convenience PIN.)

18.8.29 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 (Release 1507) Administrative Templates (or newer).

18.8.30 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.

18.8.31 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 Release 1709 Administrative Templates (or newer).

18.8.31.1 (L2) Ensure 'Allow Clipboard synchronization across devices' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This setting determines whether Clipboard contents can be synchronized across devices.

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

Rationale:

In high security environments, clipboard data should stay local to the system and not synced across devices, as it may contain very sensitive information that must be contained locally.

Impact:

Clipboard contents will not be shareable 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:

```
HKEY_LOCAL_MACHINE\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 may not exist by default. It is provided by the Group Policy template `OSPolicy.admx/adml` that is included with the Microsoft Windows 10 Release 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.)

18.8.31.2 (L2) Ensure 'Allow upload of User Activities' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This policy setting determines whether published User Activities can be uploaded to the cloud.

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

Rationale:

Due to privacy concerns, data should never be sent to any 3rd party since this data could 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:

`HKEY_LOCAL_MACHINE\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 Release 1803 Administrative Templates (or newer).

Default Value:

Enabled. (Activities of type User Activity are allowed to be uploaded to the cloud.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>			

18.8.32 Performance 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 `PerfCenterCPL.admx/adml` that is only included with the Microsoft Windows Vista through the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

18.8.33 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 Release 1703 Administrative Templates (or newer).

18.8.34 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.

18.8.34.1 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.

18.8.34.2 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 Release 1607 & Server 2016 Administrative Templates (or newer).

18.8.34.3 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.

18.8.34.4 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.

18.8.34.5 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 Release 1709 Administrative Templates (or newer).

18.8.34.6 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.

18.8.34.6.1 (L1) Ensure 'Allow network connectivity during connected-standby (on battery)' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 attackers 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:

```
HKEY_LOCAL_MACHINE\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 Release 1607 & Server 2016 Administrative Templates (or newer).

Default Value:

Enabled. (Network connectivity will be maintained in standby while on battery.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>			

18.8.34.6.2 (L1) Ensure 'Allow network connectivity during connected-standby (plugged in)' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 attackers 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:

```
HKEY_LOCAL_MACHINE\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 Release 1607 & Server 2016 Administrative Templates (or newer).

Default Value:

Enabled. (Network connectivity will be maintained in standby while plugged in.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>			

18.8.34.6.3 (BL) Ensure 'Allow standby states (S1-S3) when sleeping (on battery)' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) + BitLocker (BL)
- Level 2 (L2) + BitLocker (BL)
- BitLocker (BL) - optional add-on for when BitLocker is deployed

Description:

This policy setting manages whether or not Windows is allowed to use standby states when putting the computer in a sleep state.

The recommended state for this setting is: Disabled.

Rationale:

System sleep states (S1-S3) keep power to the RAM which may contain secrets, such as the BitLocker volume encryption key. An attacker finding a computer in sleep states (S1-S3) could directly attack the memory of the computer and gain access to the secrets through techniques such as RAM reminisce and direct memory access (DMA).

Impact:

Users will not be able to use Sleep (S3) while on battery, which resumes faster than Hibernation (S4).

Audit:

Navigate to the UI 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\Policies\Microsoft\Power\PowerSettings\abfc2519-3608-4c2a-94ea-171b0ed546ab: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 standby states (S1-S3) when sleeping (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. (Windows is allowed to use standby states when putting the computer in a sleep state.)

18.8.34.6.4 (BL) Ensure 'Allow standby states (S1-S3) when sleeping (plugged in)' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) + BitLocker (BL)
- Level 2 (L2) + BitLocker (BL)
- BitLocker (BL) - optional add-on for when BitLocker is deployed

Description:

This policy setting manages whether or not Windows is allowed to use standby states when putting the computer in a sleep state.

The recommended state for this setting is: Disabled.

Rationale:

System sleep states (S1-S3) keep power to the RAM which may contain secrets, such as the BitLocker volume encryption key. An attacker finding a computer in sleep states (S1-S3) could directly attack the memory of the computer and gain access to the secrets through techniques such as RAM reminisce and direct memory access (DMA).

Impact:

Users will not be able to use Sleep (S3) while plugged in, which resumes faster than Hibernation (S4).

Audit:

Navigate to the UI 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\Policies\Microsoft\Power\PowerSettings\abfc2519-3608-4c2a-94ea-171b0ed546ab: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 standby states (S1-S3) when sleeping (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. (Windows is allowed to use standby states when putting the computer in a sleep state.)

18.8.34.6.5 (L1) Ensure 'Require a password when a computer wakes (on battery)' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

HKEY_LOCAL_MACHINE\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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>4.3 Configure Automatic Session Locking on Enterprise Assets</p> <p>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.</p>			
v7	<p>16.11 Lock Workstation Sessions After Inactivity</p> <p>Automatically lock workstation sessions after a standard period of inactivity.</p>			

18.8.34.6.6 (L1) Ensure 'Require a password when a computer wakes (plugged in)' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

HKEY_LOCAL_MACHINE\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.)

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.	●	●	●

18.8.35 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).

18.8.36 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.

18.8.36.1 (L1) Ensure 'Configure Offer Remote Assistance' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 malicious 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:

HKEY_LOCAL_MACHINE\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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

18.8.36.2 (L1) Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

HKEY_LOCAL_MACHINE\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.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>		●	●

18.8.37 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.

18.8.37.1 (L1) Ensure 'Enable RPC Endpoint Mapper Client Authentication' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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. 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 we do not recommend applying it to Domain Controllers.

Note: This policy will not be effective until the system is rebooted.

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

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.

Audit:

Navigate to the UI 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\ 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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>		●	●

18.8.37.2 (L1) Ensure 'Restrict Unauthenticated RPC clients' is set to 'Enabled: Authenticated' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

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:

HKEY_LOCAL_MACHINE\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: Authenticated. (Only authenticated RPC clients are allowed to connect to RPC servers running on the machine. Exemptions are granted to interfaces that have requested them.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.8.38 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.

18.8.39 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.

18.8.40 Security Account 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 `SAM.admx/adml` that is included with the Microsoft Windows 11 Release 21H2 Administrative Templates (or newer).

18.8.41 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.

18.8.42 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 Release 1903 Administrative Templates (or newer).

18.8.43 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).

18.8.44 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.

18.8.45 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 Release 1709 Administrative Templates (or newer).

18.8.46 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 Release 1903 Administrative Templates (or newer).

18.8.47 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.

18.8.48 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.

18.8.48.1 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.

18.8.48.2 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.

18.8.48.3 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.

18.8.48.4 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).

18.8.48.5 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.

18.8.48.5.1 (L2) Ensure 'Microsoft Support Diagnostic Tool: Turn on MSDT interactive communication with support provider' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

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:

Due to privacy concerns, data should never be sent to any 3rd party since this data could 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:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\ScriptedDiagnosticsProvider\Policy:DisableQueryRemoteServer
```

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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>		●	●

18.8.48.6 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 `Msি-FileRecovery.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.8.48.7 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).

18.8.48.8 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).

18.8.48.9 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.

18.8.48.10 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.

18.8.48.11 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).

18.8.48.11.1 (L2) Ensure 'Enable/Disable PerfTrack' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

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:

`HKEY_LOCAL_MACHINE\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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>			

18.8.49 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.

18.8.50 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.

18.8.50.1 (L2) Ensure 'Turn off the advertising ID' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

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:

Tracking user activity for advertising purposes, even anonymously, may be a privacy concern. In an enterprise managed environment, applications should not need or require tracking for targeted advertising.

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:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\AdvertisingInfo:DisabledByGroupPolicy
```

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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.	●	●	●

18.8.51 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.

18.8.52 Windows HotStart

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 `HotStart.admx/adml` that is only included with the Microsoft Windows Vista through the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

18.8.53 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.

18.8.53.1 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.

18.8.53.1.1 (L2) Ensure 'Enable Windows NTP Client' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This policy setting specifies whether the Windows NTP Client is enabled. Enabling the Windows NTP Client allows your computer to synchronize its computer clock with other NTP servers. You might want to disable this service if you decide to use a third-party time provider.

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

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:

You can set the local computer clock to synchronize time with NTP 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:

HKEY_LOCAL_MACHINE\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.)

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.		●	●

18.8.53.1.2 (L2) Ensure 'Enable Windows NTP Server' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This policy setting allows you to specify whether the Windows NTP Server is enabled.

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

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.

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:

```
HKEY_LOCAL_MACHINE\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.)

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 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.

18.9.1 Active Directory Federation 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 `adfs.admx/adml` that is only included with the Microsoft Windows Vista through the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

18.9.2 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.

18.9.3 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.

18.9.4 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).

18.9.4.1 (L2) Ensure 'Allow a Windows app to share application data between users' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

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:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\AppMode  
1\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 (Release 1507) Administrative Templates (or newer).

Default Value:

Disabled. (Windows apps won't be able to share app data with other instances of that app.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
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.	●	●	●

18.9.4.2 (L1) Ensure 'Prevent non-admin users from installing packaged Windows apps' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting manages non-Administrator users' ability to install Windows app packages.

The recommended state for this setting is: Enabled.

Rationale:

In a corporate managed environment, application installations should be managed centrally by IT staff, not by end users.

Impact:

Non-Administrator users will not be able to install Microsoft Store app packages, unless they are explicitly permitted by other policies. If a Microsoft Store app is required for legitimate use, an Administrator will need to perform the installation from an Administrator context.

Audit:

Navigate to the UI 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\Policies\Microsoft\Windows\Appx:BlockNonAdminUser  
Install
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows  
Components\App Package Deployment\Prevent non-admin users from installing  
packaged Windows apps
```

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 Release 2004 Administrative Templates (or newer).

Default Value:

Disabled. (All users will be able to initiate installation of Microsoft Store app packages.)

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	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.	●	●	●

18.9.5 App Privacy

This section contains recommendations for App Privacy settings.

This Group Policy section is provided by the Group Policy template `AppPrivacy.admx/adml` that is included with the Microsoft Windows 10 Release 1511 Administrative Templates (or newer).

18.9.5.1 (L1) Ensure 'Let Windows apps activate with voice while the system is locked' is set to 'Enabled: Force Deny' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting specifies whether Windows apps can be activated by voice (apps and Cortana) while the system is locked.

The recommended state for this setting is: Enabled: Force Deny.

Rationale:

Access to any computer resource should not be allowed when the device is locked.

Impact:

Users will not be able to activate apps while the computer is locked.

Audit:

Navigate to the UI 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\Policies\Microsoft\Windows\AppPrivacy:LetAppsActivateWithVoiceAboveLock

Remediation:

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

Force Deny:

Computer Configuration\Policies\Administrative Templates\Windows Components\App Privacy\Let Windows apps activate with voice while the system is locked

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template AppPrivacy.admx/adml that is included with the Microsoft Windows 10 Release 1903 Administrative Templates (or newer).

Default Value:

Disabled. (The user can decide whether Windows apps can interact with applications using speech while the system is locked by using Settings > Privacy on the device.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>		●	●

18.9.6 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).

18.9.6.1 (L1) Ensure 'Allow Microsoft accounts to be optional' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

HKEY_LOCAL_MACHINE\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.)

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.	●	●	

18.9.6.2 (L2) Ensure 'Block launching Universal Windows apps with Windows Runtime API access from hosted content.' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This policy setting controls whether Microsoft Store apps with Windows Runtime API access directly from web content can be launched.

The recommended state for this setting is: Enabled.

Rationale:

Blocking apps from the web with direct access to the Windows API can prevent malicious apps from being run on a system. Only system administrators should be installing approved applications.

Impact:

Universal Windows apps which declare Windows Runtime API access in the ApplicationContentUriRules section of the manifest cannot be launched (Universal Windows apps which have not declared Windows Runtime API access in the manifest will not be affected).

Audit:

Navigate to the UI 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\CurrentVersion\Policies\System:  
BlockHostedAppAccessWinRT
```

Remediation:

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

Computer Configuration\Policies\Administrative Templates\Windows Components\App runtime\Block launching Universal Windows apps with Windows Runtime API access from hosted content.

Note: A reboot may be required after the setting is applied.

Note #2: 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 10 RTM (Release 1507) Administrative Templates (or newer).

Note #3: In older Microsoft Windows Administrative Templates, this setting was initially named *Block launching Windows Store apps with Windows Runtime API access from hosted content.*, but it was renamed starting with the Windows 10 Release 1803 Administrative Templates.

Default Value:

Disabled. (All Universal Windows apps can be launched.)

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.			

18.9.7 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.

18.9.8 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.

18.9.8.1 (L1) Ensure 'Disallow Autoplay for non-volume devices' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting disallows AutoPlay for MTP devices like cameras or phones.

The recommended state for this setting is: Enabled.

Rationale:

An attacker 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:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Explorer:NoAutoplayfor
nonVolume

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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.3 <u>Disable Autorun and Autoplay for Removable Media</u> Disable autorun and autoplay auto-execute functionality for removable media.	●	●	●
v7	8.5 <u>Configure Devices Not To Auto-run Content</u> Configure devices to not auto-run content from removable media.	●	●	●

18.9.8.2 (L1) Ensure 'Set the default behavior for AutoRun' is set to 'Enabled: Do not execute any autorun commands' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explore  
r: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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>10.3 Disable Autorun and Autoplay for Removable Media</u> Disable autorun and autoplay auto-execute functionality for removable media.	●	●	●
v7	<u>8.5 Configure Devices Not To Auto-run Content</u> Configure devices to not auto-run content from removable media.	●	●	●

18.9.8.3 (L1) Ensure 'Turn off Autoplay' is set to 'Enabled: All drives' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Autoplay starts to read from a drive as soon as you insert media in the drive, which causes the setup file for programs or audio media to start immediately. An attacker could use this feature to launch a program to damage the computer or data on the computer. Autoplay is disabled by default on some removable drive types, such as floppy disk and network drives, but not on CD-ROM drives.

Note: You cannot use this policy setting to enable Autoplay on computer drives in which it is disabled by default, such as floppy disk and network drives.

The recommended state for this setting is: Enabled: All drives.

Rationale:

An attacker 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:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorerr: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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>10.3 Disable Autorun and Autoplay for Removable Media</u> Disable autorun and autoplay auto-execute functionality for removable media.	●	●	●
v7	<u>8.5 Configure Devices Not To Auto-run Content</u> Configure devices to not auto-run content from removable media.	●	●	●

18.9.9 Backup

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 `UserdataBackup.admx/adml` that is only included with the Microsoft Windows Vista through the Windows 10 Release 1511 Administrative Templates (except for the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates).

18.9.10 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).

18.9.10.1 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 Release 1511 Administrative Templates (or newer).

18.9.10.1.1 (L1) Ensure 'Configure enhanced anti-spoofing' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

HKEY_LOCAL_MACHINE\SOFTWARE\ Policies\Microsoft\Biometrics\FacialFeatures:EnhancedAntiSpoofing

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 Release 1511 Administrative Templates (or newer).

Note #2: In the Windows 10 Release 1511 and Windows 10 Release 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 Release 1703 Administrative Templates.

Default Value:

Users are able to choose whether or not to use enhanced anti-spoofing on supported devices.

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™.		●	●

18.9.11 BitLocker Drive Encryption

This section contains recommendations for configuring BitLocker.

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.

18.9.11.1 Fixed Data Drives

This section contains recommendations for configuring Fixed Data Drives in BitLocker.

This Group Policy section is provided by the Group Policy template `VolumeEncryption.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.9.11.1.1 (BL) Ensure 'Allow access to BitLocker-protected fixed data drives from earlier versions of Windows' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) + BitLocker (BL)
- Level 2 (L2) + BitLocker (BL)
- BitLocker (BL) - optional add-on for when BitLocker is deployed

Description:

This policy setting configures whether or not fixed data drives formatted with the FAT file system can be unlocked and viewed on computers running Windows Server 2008 (non-R2), Windows Vista, Windows XP with Service Pack 3 (SP3), or Windows XP with Service Pack 2 (SP2) operating systems.

Note: This policy setting does not apply to drives that are formatted with the NTFS file system.

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

Rationale:

By default BitLocker virtualizes FAT formatted drives to permit access via the BitLocker To Go Reader on previous versions of Windows. Additionally the BitLocker To Go Reader application is applied to the unencrypted portion of the drive.

The BitLocker To Go Reader application, like any other application, is subject to spoofing and could be a mechanism to propagate malware.

Impact:

Fixed data drives formatted with the FAT file system that are BitLocker-protected cannot be unlocked on computers running Windows Server 2008 (non-R2), Windows Vista, Windows XP with SP3 or Windows XP with SP2. `BitLockerToGo.exe` will not be 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:

HKEY_LOCAL_MACHINE\SOFTWARE\ Policies\Microsoft\FVE:FDVDiscoveryVolumeType

Remediation:

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

Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Fixed Data Drives\Allow access to BitLocker-protected fixed data drives from earlier versions of Windows

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `volumeEncryption.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Default Value:

Enabled. (Fixed data drives formatted with the FAT file system can be unlocked on computers running Windows Server 2008 (non-R2), Windows Vista, Windows XP with SP3 or Windows XP with SP2, and their content can be viewed. These operating systems will only have read-only access to BitLocker-protected drives.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.6 Encrypt Data on End-User Devices Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.	●	●	●
v7	13.6 Encrypt the Hard Drive of All Mobile Devices. Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.	●	●	●

18.9.11.1.2 (BL) Ensure 'Choose how BitLocker-protected fixed drives can be recovered' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) + BitLocker (BL)
- Level 2 (L2) + BitLocker (BL)
- BitLocker (BL) - optional add-on for when BitLocker is deployed

Description:

This policy setting allows you to control how BitLocker-protected fixed data drives are recovered in the absence of the required credentials. This policy setting is applied when you turn on BitLocker.

The "Allow data recovery agent" check box is used to specify whether a Data Recovery Agent can be used with BitLocker-protected fixed data drives. Before a Data Recovery Agent can be used it must be added from the Public Key Policies item in either the Group Policy Management Console or the Local Group Policy Editor. Consult the BitLocker Drive Encryption Deployment Guide on Microsoft TechNet for more information about adding Data Recovery Agents.

In "Configure user storage of BitLocker recovery information" select whether users are allowed, required, or not allowed to generate a 48-digit recovery password or a 256-bit recovery key.

Select "Omit recovery options from the BitLocker setup wizard" to prevent users from specifying recovery options when they enable BitLocker on a drive. This means that you will not be able to specify which recovery option to use when you enable BitLocker, instead BitLocker recovery options for the drive are determined by the policy setting.

In "Save BitLocker recovery information to Active Directory Domain Services" choose which BitLocker recovery information to store in AD DS for fixed data drives. If you select "Backup recovery password and key package", both the BitLocker recovery password and key package are stored in AD DS. Storing the key package supports recovering data from a drive that has been physically corrupted. If you select "Backup recovery password only", only the recovery password is stored in AD DS.

Select the "Do not enable BitLocker until recovery information is stored in AD DS for fixed data drives" check box if you want to prevent users from enabling BitLocker unless the computer is connected to the domain and the backup of BitLocker recovery information to AD DS succeeds.

Note: If the "Do not enable BitLocker until recovery information is stored in AD DS for fixed data drives" check box is selected, a recovery password is automatically generated.

The recommended state for this setting is: Enabled.

Rationale:

Administrators should always have a safe, secure way to access encrypted data in the event users cannot access their data.

Additionally, as with any authentication method, a drive can be compromised by guessing or finding the authentication information used to access the drive.

Impact:

To use BitLocker, a Data Recovery Agent will need to be configured for fixed drives. To recover a drive will require highly-controlled access to the Data Recovery Agent private key.

Audit:

Navigate to the UI 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\Policies\Microsoft\FVE:FDVRecovery

Remediation:

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

Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Fixed Data Drives\Choose how BitLocker-protected fixed drives can be recovered

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `VolumeEncryption.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Default Value:

Disabled. (The default recovery options are supported for BitLocker recovery - a DRA is allowed, and the recovery options can be specified by the user including the recovery password and recovery key, and recovery information is not backed up to AD DS.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.6 Encrypt Data on End-User Devices Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.	●	●	●
v7	13.6 Encrypt the Hard Drive of All Mobile Devices. Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.	●	●	●

18.9.11.1.3 (BL) Ensure 'Choose how BitLocker-protected fixed drives can be recovered: Allow data recovery agent' is set to 'Enabled: True' (Automated)

Profile Applicability:

- Level 1 (L1) + BitLocker (BL)
- Level 2 (L2) + BitLocker (BL)
- BitLocker (BL) - optional add-on for when BitLocker is deployed

Description:

This policy setting allows you to control how BitLocker-protected fixed data drives are recovered in the absence of the required credentials. This policy setting is applied when you turn on BitLocker.

The "Allow data recovery agent" check box is used to specify whether a Data Recovery Agent can be used with BitLocker-protected fixed data drives. Before a Data Recovery Agent can be used it must be added from the Public Key Policies item in either the Group Policy Management Console or the Local Group Policy Editor. Consult the BitLocker Drive Encryption Deployment Guide on Microsoft TechNet for more information about adding Data Recovery Agents.

The recommended state for this setting is: `Enabled: True` (checked).

Rationale:

Administrators should always have a safe, secure way to access encrypted data in the event users cannot access their data.

Additionally, as with any authentication method, a drive can be compromised by guessing or finding the authentication information used to access the drive.

To use BitLocker, a Data Recovery Agent will need to be configured for fixed drives. To recover a drive will require highly-controlled access to the Data Recovery Agent private key.

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:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\FVE:FDVManageDRA

Remediation:

To establish the recommended configuration via GP, set the following UI path to Enabled: True (checked):

Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Fixed Data Drives\Choose how BitLocker-protected fixed drives can be recovered: Allow data recovery agent

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template VolumeEncryption.admx/adml that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Default Value:

Enabled: True. (A DRA is allowed.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.6 Encrypt Data on End-User Devices Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.	●	●	●
v7	13.6 Encrypt the Hard Drive of All Mobile Devices. Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.	●	●	●

18.9.11.1.4 (BL) Ensure 'Choose how BitLocker-protected fixed drives can be recovered: Recovery Password' is set to 'Enabled: Allow 48-digit recovery password' (Automated)

Profile Applicability:

- Level 1 (L1) + BitLocker (BL)
- Level 2 (L2) + BitLocker (BL)
- BitLocker (BL) - optional add-on for when BitLocker is deployed

Description:

This policy setting allows you to control how BitLocker-protected fixed data drives are recovered in the absence of the required credentials. This policy setting is applied when you turn on BitLocker.

In "Configure user storage of BitLocker recovery information" select whether users are allowed, required, or not allowed to generate a 48-digit recovery password or a 256-bit recovery key.

The recommended state for this setting is: Enabled: Allow 48-digit recovery password.

Rationale:

Administrators should always have a safe, secure way to access encrypted data in the event users cannot access their data.

Additionally, as with any authentication method, a drive can be compromised by guessing or finding the authentication information used to access the drive.

To use BitLocker, a Data Recovery Agent will need to be configured for fixed drives. To recover a drive will require highly-controlled access to the Data Recovery Agent private key.

Impact:

A 48-digit recovery password will be permitted for fixed drives.

Audit:

Navigate to the UI 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\Policies\Microsoft\FVE:FDVRecoveryPassword

Remediation:

To establish the recommended configuration via GP, set the following UI path to Enabled:
Allow 48-digit recovery password:

Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Fixed Data Drives\Choose how BitLocker-protected fixed drives can be recovered: Recovery Password

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template VolumeEncryption.admx/adml that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Default Value:

Recovery options are specified by the user.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.6 Encrypt Data on End-User Devices Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.	●	●	●
v7	13.6 Encrypt the Hard Drive of All Mobile Devices. Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.	●	●	●

18.9.11.1.5 (BL) Ensure 'Choose how BitLocker-protected fixed drives can be recovered: Recovery Key' is set to 'Enabled: Allow 256-bit recovery key' (Automated)

Profile Applicability:

- Level 1 (L1) + BitLocker (BL)
- Level 2 (L2) + BitLocker (BL)
- BitLocker (BL) - optional add-on for when BitLocker is deployed

Description:

This policy setting allows you to control how BitLocker-protected fixed data drives are recovered in the absence of the required credentials. This policy setting is applied when you turn on BitLocker.

In "Configure user storage of BitLocker recovery information" select whether users are allowed, required, or not allowed to generate a 48-digit recovery password or a 256-bit recovery key.

The recommended state for this setting is: Enabled: Allow 256-bit recovery key.

Rationale:

Administrators should always have a safe, secure way to access encrypted data in the event users cannot access their data.

Additionally, as with any authentication method, a drive can be compromised by guessing or finding the authentication information used to access the drive.

To use BitLocker, a Data Recovery Agent will need to be configured for fixed drives. To recover a drive will require highly-controlled access to the Data Recovery Agent private key.

Impact:

A 256-bit recovery key will be permitted for fixed drives.

Audit:

Navigate to the UI 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\ Policies\Microsoft\FVE:FDVRecoveryKey

Remediation:

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

Allow 256-bit recovery key:

Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Fixed Data Drives\Choose how BitLocker-protected fixed drives can be recovered: Recovery Key

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template VolumeEncryption.admx/adml that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Default Value:

Recovery options are specified by the user.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.6 Encrypt Data on End-User Devices Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.	●	●	●
v7	13.6 Encrypt the Hard Drive of All Mobile Devices. Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.	●	●	●

18.9.11.1.6 (BL) Ensure 'Choose how BitLocker-protected fixed drives can be recovered: Omit recovery options from the BitLocker setup wizard' is set to 'Enabled: True' (Automated)

Profile Applicability:

- Level 1 (L1) + BitLocker (BL)
- Level 2 (L2) + BitLocker (BL)
- BitLocker (BL) - optional add-on for when BitLocker is deployed

Description:

This policy setting allows you to control how BitLocker-protected fixed data drives are recovered in the absence of the required credentials. This policy setting is applied when you turn on BitLocker.

Select "Omit recovery options from the BitLocker setup wizard" to prevent users from specifying recovery options when they enable BitLocker on a drive. This means that you will not be able to specify which recovery option to use when you enable BitLocker, instead BitLocker recovery options for the drive are determined by the policy setting.

The recommended state for this setting is: Enabled: True (checked).

Rationale:

Administrators should always have a safe, secure way to access encrypted data in the event users cannot access their data.

Additionally, as with any authentication method, a drive can be compromised by guessing or finding the authentication information used to access the drive.

To use BitLocker, a Data Recovery Agent will need to be configured for fixed drives. To recover a drive will require highly-controlled access to the Data Recovery Agent private key.

Impact:

The ability to manually select recovery options for fixed drives will not be presented to the user in the BitLocker setup wizard.

Audit:

Navigate to the UI 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\ Policies\Microsoft\FVE:FDVHideRecoveryPage

Remediation:

To establish the recommended configuration via GP, set the following UI path to Enabled: True (checked):

Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Fixed Data Drives\Choose how BitLocker-protected fixed drives can be recovered: Omit recovery options from the BitLocker setup wizard

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template VolumeEncryption.admx/adml that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Default Value:

Recovery options for fixed drives are selectable by the user in the BitLocker setup wizard.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.6 Encrypt Data on End-User Devices Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.	●	●	●
v7	13.6 Encrypt the Hard Drive of All Mobile Devices. Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.	●	●	●

18.9.11.1.7 (BL) Ensure 'Choose how BitLocker-protected fixed drives can be recovered: Save BitLocker recovery information to AD DS for fixed data drives' is set to 'Enabled: False' (Automated)

Profile Applicability:

- Level 1 (L1) + BitLocker (BL)
- Level 2 (L2) + BitLocker (BL)
- BitLocker (BL) - optional add-on for when BitLocker is deployed

Description:

This policy setting allows you to control how BitLocker-protected fixed data drives are recovered in the absence of the required credentials. This policy setting is applied when you turn on BitLocker.

In "Save BitLocker recovery information to Active Directory Domain Services" choose which BitLocker recovery information to store in AD DS for fixed data drives. If you select "Backup recovery password and key package", both the BitLocker recovery password and key package are stored in AD DS. Storing the key package supports recovering data from a drive that has been physically corrupted. If you select "Backup recovery password only", only the recovery password is stored in AD DS.

The recommended state for this setting is: `Enabled: False` (unchecked).

Rationale:

Administrators should always have a safe, secure way to access encrypted data in the event users cannot access their data.

Additionally, as with any authentication method, a drive can be compromised by guessing or finding the authentication information used to access the drive.

To use BitLocker, a Data Recovery Agent will need to be configured for fixed drives. To recover a drive will require highly-controlled access to the Data Recovery Agent private key.

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:

HKEY_LOCAL_MACHINE\SOFTWARE\ Policies\Microsoft\FVE:FDVActiveDirectoryBackup

Remediation:

To establish the recommended configuration via GP, set the following UI path to Enabled: False (unchecked):

Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Fixed Data Drives\Choose how BitLocker-protected fixed drives can be recovered: Save BitLocker recovery information to AD DS for fixed data drives

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template VolumeEncryption.admx/adml that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Default Value:

BitLocker recovery information for fixed drives is not backed up to AD DS.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.6 Encrypt Data on End-User Devices Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.	●	●	●
v7	13.6 Encrypt the Hard Drive of All Mobile Devices. Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.	●	●	●

18.9.11.1.8 (BL) Ensure 'Choose how BitLocker-protected fixed drives can be recovered: Configure storage of BitLocker recovery information to AD DS' is set to 'Enabled: Backup recovery passwords and key packages' (Automated)

Profile Applicability:

- Level 1 (L1) + BitLocker (BL)
- Level 2 (L2) + BitLocker (BL)
- BitLocker (BL) - optional add-on for when BitLocker is deployed

Description:

This policy setting allows you to control how BitLocker-protected fixed data drives are recovered in the absence of the required credentials. This policy setting is applied when you turn on BitLocker.

In "Save BitLocker recovery information to Active Directory Domain Services" choose which BitLocker recovery information to store in AD DS for fixed data drives. If you select "Backup recovery password and key package", both the BitLocker recovery password and key package are stored in AD DS. Storing the key package supports recovering data from a drive that has been physically corrupted. If you select "Backup recovery password only", only the recovery password is stored in AD DS.

The recommended state for this setting is: Enabled: Backup recovery passwords and key packages.

Rationale:

Administrators should always have a safe, secure way to access encrypted data in the event users cannot access their data.

Additionally, as with any authentication method, a drive can be compromised by guessing or finding the authentication information used to access the drive.

To use BitLocker, a Data Recovery Agent will need to be configured for fixed drives. To recover a drive will require highly-controlled access to the Data Recovery Agent private key.

Impact:

None - this value is ignored when the checkbox above it (*Save BitLocker recovery information to AD DS for fixed data drives*) is False (unchecked), as is required in Rule 18.9.11.1.7. If that checkbox is set to True (checked), both recovery passwords and key packages for fixed drives will be saved to AD DS.

Audit:

Navigate to the UI 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\Policies\Microsoft\FVE:FDVActiveDirectoryInfoToStore

Remediation:

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

Backup recovery passwords and key packages:

Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Fixed Data Drives\Choose how BitLocker-protected fixed drives can be recovered: Configure storage of BitLocker recovery information to AD DS:

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template volumeEncryption.admx/adml that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Default Value:

BitLocker recovery information for fixed drives is not backed up to AD DS.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.6 Encrypt Data on End-User Devices Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.	●	●	●
v7	13.6 Encrypt the Hard Drive of All Mobile Devices. Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.	●	●	●

18.9.11.1.9 (BL) Ensure 'Choose how BitLocker-protected fixed drives can be recovered: Do not enable BitLocker until recovery information is stored to AD DS for fixed data drives' is set to 'Enabled: False'
(Automated)

Profile Applicability:

- Level 1 (L1) + BitLocker (BL)
- Level 2 (L2) + BitLocker (BL)
- BitLocker (BL) - optional add-on for when BitLocker is deployed

Description:

This policy setting allows you to control how BitLocker-protected fixed data drives are recovered in the absence of the required credentials. This policy setting is applied when you turn on BitLocker.

Select the "Do not enable BitLocker until recovery information is stored in AD DS for fixed data drives" check box if you want to prevent users from enabling BitLocker unless the computer is connected to the domain and the backup of BitLocker recovery information to AD DS succeeds.

Note: If the "Do not enable BitLocker until recovery information is stored in AD DS for fixed data drives" check box is selected, a recovery password is automatically generated.

The recommended state for this setting is: Enabled: False (unchecked).

Rationale:

Administrators should always have a safe, secure way to access encrypted data in the event users cannot access their data.

Additionally, as with any authentication method, a drive can be compromised by guessing or finding the authentication information used to access the drive.

To use BitLocker, a Data Recovery Agent will need to be configured for fixed drives. To recover a drive will require highly-controlled access to the Data Recovery Agent private key.

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:

HKEY_LOCAL_MACHINE\SOFTWARE\ Policies\Microsoft\FVE:FDVRequireActiveDirectoryBackup

Remediation:

To establish the recommended configuration via GP, set the following UI path to Enabled: False (unchecked):

Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Fixed Data Drives\Choose how BitLocker-protected fixed drives can be recovered: Do not enable BitLocker until recovery information is stored to AD DS for fixed data drives

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `volumeEncryption.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Default Value:

BitLocker can be enabled on fixed drives without the requirement of storing recovery information to Active Directory first.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.6 Encrypt Data on End-User Devices Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.	●	●	●
v7	13.6 Encrypt the Hard Drive of All Mobile Devices. Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.	●	●	●

18.9.11.1.10 (BL) Ensure 'Configure use of hardware-based encryption for fixed data drives' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) + BitLocker (BL)
- Level 2 (L2) + BitLocker (BL)
- BitLocker (BL) - optional add-on for when BitLocker is deployed

Description:

This policy setting allows you to manage BitLocker's use of hardware-based encryption on fixed data drives and specify which encryption algorithms it can use with hardware-based encryption. Using hardware-based encryption can improve performance of drive operations that involve frequent reading or writing of data to the drive.

You can specify additional options that control whether BitLocker software-based encryption is used instead of hardware-based encryption on computers that do not support hardware-based encryption and whether you want to restrict the encryption algorithms and cipher suites used with hardware-based encryption.

The recommended state for this setting is: Disabled.

Rationale:

From a security perspective hardware-based encryption may introduce vulnerabilities in the hardware encryption of certain self-encrypting drives (SEDs), if the vendor and/or user has not updated the firmware to remediate the vulnerability. For more information visit [ADV180028 - Security Update Guide - Microsoft - Guidance for configuring BitLocker to enforce software encryption.](#)

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:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\FVE:FDVHardwareEncryption

Remediation:

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

Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Fixed Data Drives\Configure use of hardware-based encryption for fixed data drives

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `VolumeEncryption.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

BitLocker will use software-based encryption irrespective of hardware-based encryption availability.

References:

1. <https://msrc.microsoft.com/update-guide/en-US/vulnerability/ADV180028>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.6 Encrypt Data on End-User Devices Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.	●	●	●
v7	13.6 Encrypt the Hard Drive of All Mobile Devices. Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.	●	●	●

18.9.11.1.11 (BL) Ensure 'Configure use of passwords for fixed data drives' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) + BitLocker (BL)
- Level 2 (L2) + BitLocker (BL)
- BitLocker (BL) - optional add-on for when BitLocker is deployed

Description:

This policy setting specifies whether a password is required to unlock BitLocker-protected fixed data drives.

Note: This setting is enforced when turning on BitLocker, not when unlocking a volume. BitLocker will allow unlocking a drive with any of the protectors available on the drive.

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

Rationale:

Using a dictionary-style attack, passwords can be guessed or discovered by repeatedly attempting to unlock a drive. Since this type of BitLocker password does include anti-dictionary attack protections provided by a TPM, for example, there is no mechanism to slow down rapid brute-force attacks against them.

Impact:

The password option will not be available when configuring BitLocker for fixed drives.

Audit:

Navigate to the UI 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\Policies\Microsoft\FVE:FDVPassphrase`

Remediation:

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

Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Fixed Data Drives\Configure use of passwords for fixed data drives

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `VolumeEncryption.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Default Value:

Passwords are supported, without complexity requirements and with an 8 character minimum.

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	13.6 Encrypt the Hard Drive of All Mobile Devices. Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.	●	●	●

18.9.11.1.12 (BL) Ensure 'Configure use of smart cards on fixed data drives' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) + BitLocker (BL)
- Level 2 (L2) + BitLocker (BL)
- BitLocker (BL) - optional add-on for when BitLocker is deployed

Description:

This policy setting allows you to specify whether smart cards can be used to authenticate user access to the BitLocker-protected fixed data drives on a computer.

Smart cards can be used to authenticate user access to the drive. You can require smart card authentication by selecting the "Require use of smart cards on fixed data drives" check box.

Note: This setting is enforced when turning on BitLocker, not when unlocking a drive. BitLocker will allow unlocking a drive with any of the protectors available on the drive.

The recommended state for this setting is: Enabled.

Rationale:

A drive can be compromised by guessing or finding the authentication information used to access the drive. For example, a password could be guessed, or a drive set to automatically unlock could be lost or stolen with the computer it automatically unlocks with.

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:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\FVE:FDVAllowUserCert

Remediation:

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

Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Fixed Data Drives\Configure use of smart cards on fixed data drives

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `VolumeEncryption.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Default Value:

Enabled. (Users are allowed to use smart cards to authenticate their access to BitLocker-protected fixed data drives.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.3 Require MFA for Externally-Exposed Applications Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.			
v7	16.3 Require Multi-factor Authentication Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.			

18.9.11.1.13 (BL) Ensure 'Configure use of smart cards on fixed data drives: Require use of smart cards on fixed data drives' is set to 'Enabled: True' (Automated)

Profile Applicability:

- Level 1 (L1) + BitLocker (BL)
- Level 2 (L2) + BitLocker (BL)
- BitLocker (BL) - optional add-on for when BitLocker is deployed

Description:

This policy setting allows you to specify whether smart cards *must* be used to authenticate user access to the BitLocker-protected fixed data drives on a computer.

Smart cards can be used to authenticate user access to the drive. You can require a smart card authentication by selecting the "Require use of smart cards on fixed data drives" check box.

Note: This setting is enforced when turning on BitLocker, not when unlocking a drive. BitLocker will allow unlocking a drive with any of the protectors available on the drive.

The recommended state for this setting is: Enabled: True (checked).

Rationale:

A drive can be compromised by guessing or finding the authentication information used to access the drive. For example, a password could be guessed, or a drive set to automatically unlock could be lost or stolen with the computer it automatically unlocks with.

Impact:

Smart cards will be required to authenticate user access to fixed data drives. Use of smart cards requires PKI infrastructure. Users will need to authenticate with the smart card to unlock the fixed data drive every time they restart 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:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\FVE:FDVEnforceUserCert

Remediation:

To establish the recommended configuration via GP, set the following UI path to Enabled: True (checked):

Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Fixed Data Drives\Configure use of smart cards on fixed data drives: Require use of smart cards on fixed data drives

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `VolumeEncryption.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Default Value:

Enabled: False (unchecked). (Users are allowed to use smart cards to authenticate their access to BitLocker-protected fixed data drives, but it is not required.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.3 <u>Require MFA for Externally-Exposed Applications</u> Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.		●	●
v7	16.3 <u>Require Multi-factor Authentication</u> Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		●	●

18.9.11.2 Operating System Drives

This section contains recommendations for configuring Operating System Drives in BitLocker.

This Group Policy section is provided by the Group Policy template `VolumeEncryption.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.9.11.2.1 (BL) Ensure 'Allow enhanced PINs for startup' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) + BitLocker (BL)
- Level 2 (L2) + BitLocker (BL)
- BitLocker (BL) - optional add-on for when BitLocker is deployed

Description:

This policy setting allows you to configure whether or not enhanced startup PINs are used with BitLocker.

Enhanced startup PINs permit the use of characters including uppercase and lowercase letters, symbols, numbers, and spaces. This policy setting is applied when you turn on BitLocker.

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

Rationale:

A numeric-only PIN provides less entropy than a PIN that is alpha-numeric. When not using enhanced PIN for startup, BitLocker requires the use of the function keys [F1-F10] for PIN entry since the PIN is entered in the pre-OS environment before localization support is available. This limits each PIN digit to one of ten possibilities. The TPM has an anti-hammering feature that includes a mechanism to exponentially increase the delay for PIN retry attempts; however, an attacker is able to more effectively mount a brute force attack using a domain of 10 digits of the function keys.

Impact:

All new BitLocker startup PINs set will be enhanced PINs.

Note: Not all computers enable full keyboard support in the Pre-OS environment. Some keys may not be available. It is recommended this functionality be tested using the computers in your environment prior to it being deployed.

Audit:

Navigate to the UI 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\Policies\Microsoft\FVE:UseEnhancedPin

Remediation:

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

Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives\Allow enhanced PINs for startup

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template VolumeEncryption.admx/adml that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Default Value:

Disabled. (Enhanced PINs will not be used.)

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	16.3 Require Multi-factor Authentication Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		●	●

18.9.11.2.2 (BL) Ensure 'Allow Secure Boot for integrity validation' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) + BitLocker (BL)
- Level 2 (L2) + BitLocker (BL)
- BitLocker (BL) - optional add-on for when BitLocker is deployed

Description:

This policy setting allows you to configure whether Secure Boot will be allowed as the platform integrity provider for BitLocker operating system drives.

Secure Boot ensures that the PC's pre-boot environment only loads firmware that is digitally signed by authorized software publishers. Secure Boot also provides more flexibility for managing pre-boot configuration than legacy BitLocker integrity checks.

Secure Boot requires a system that meets the UEFI 2.3.1 Specifications for Class 2 and Class 3 computers.

When this policy is enabled and the hardware is capable of using Secure Boot for BitLocker scenarios, the "Use enhanced Boot Configuration Data validation profile" group policy setting is ignored and Secure Boot verifies BCD settings according to the Secure Boot policy setting, which is configured separately from BitLocker.

Note: If the group policy setting "Configure TPM platform validation profile for native UEFI firmware configurations" is enabled and has PCR 7 omitted, BitLocker will be prevented from using Secure Boot for platform or Boot Configuration Data (BCD) integrity validation.

The recommended state for this setting is: Enabled.

Rationale:

Secure Boot ensures that only firmware digitally signed by authorized software publishers is loaded during computer startup, which reduces the risk of rootkits and other types of malware from gaining control of the system. It also helps provide protection against malicious users booting from an alternate operating 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:

HKEY_LOCAL_MACHINE\SOFTWARE\ Policies\Microsoft\FVE:OSAllowSecureBootForIntegrity

Remediation:

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

Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives\Allow Secure Boot for integrity validation

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `VolumeEncryption.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Enabled. (BitLocker will use Secure Boot for platform integrity if the platform is capable of Secure Boot-based integrity validation.)

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™.		●	●

18.9.11.2.3 (BL) Ensure 'Choose how BitLocker-protected operating system drives can be recovered' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) + BitLocker (BL)
- Level 2 (L2) + BitLocker (BL)
- BitLocker (BL) - optional add-on for when BitLocker is deployed

Description:

This policy setting allows you to control how BitLocker-protected operating system drives are recovered in the absence of the required startup key information. This policy setting is applied when you turn on BitLocker.

The "Allow certificate-based data recovery agent" check box is used to specify whether a Data Recovery Agent can be used with BitLocker-protected operating system drives. Before a Data Recovery Agent can be used it must be added from the Public Key Policies item in either the Group Policy Management Console or the Local Group Policy Editor. Consult the BitLocker Drive Encryption Deployment Guide on Microsoft TechNet for more information about adding Data Recovery Agents.

In "Configure user storage of BitLocker recovery information" select whether users are allowed, required, or not allowed to generate a 48-digit recovery password or a 256-bit recovery key.

Select "Omit recovery options from the BitLocker setup wizard" to prevent users from specifying recovery options when they enable BitLocker on a drive. This means that you will not be able to specify which recovery option to use when you enable BitLocker, instead BitLocker recovery options for the drive are determined by the policy setting.

In "Save BitLocker recovery information to Active Directory Domain Services", choose which BitLocker recovery information to store in AD DS for operating system drives. If you select "Backup recovery password and key package", both the BitLocker recovery password and key package are stored in AD DS. Storing the key package supports recovering data from a drive that has been physically corrupted. If you select "Backup recovery password only", only the recovery password is stored in AD DS.

Select the "Do not enable BitLocker until recovery information is stored in AD DS for operating system drives" check box if you want to prevent users from enabling BitLocker unless the computer is connected to the domain and the backup of BitLocker recovery information to AD DS succeeds.

Note: If the "Do not enable BitLocker until recovery information is stored in AD DS for operating system drives" check box is selected, a recovery password is automatically generated.

The recommended state for this setting is: Enabled.

Rationale:

Should a user lose their primary means for accessing an encrypted OS volume, or should the system not pass its boot time integrity checks, the system will go into recovery mode. If the recovery key has not been backed up to Active Directory, the user would need to have saved the recovery key to another location such as a USB flash drive, or have printed the recovery password, and now have access to one of those in order to recover the system. If the user is unable to produce the recovery key, then the user will be denied access to the encrypted volume and subsequently any data that is stored there.

Impact:

Users will need to be domain connected to turn on BitLocker. This policy is not FIPS complaint.

Audit:

Navigate to the UI 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\Policies\Microsoft\FVE:OSRecovery

Remediation:

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

Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives\Choose how BitLocker-protected operating system drives can be recovered

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `VolumeEncryption.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Default Value:

Disabled. (The default recovery options are supported for BitLocker recovery - a DRA is allowed, and the recovery options can be specified by the user including the recovery password and recovery key, and recovery information is not backed up to AD DS.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.6 Encrypt Data on End-User Devices Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.	●	●	●
v7	13.6 Encrypt the Hard Drive of All Mobile Devices. Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.	●	●	●

18.9.11.2.4 (BL) Ensure 'Choose how BitLocker-protected operating system drives can be recovered: Allow data recovery agent' is set to 'Enabled: False' (Automated)

Profile Applicability:

- Level 1 (L1) + BitLocker (BL)
- Level 2 (L2) + BitLocker (BL)
- BitLocker (BL) - optional add-on for when BitLocker is deployed

Description:

This policy setting allows you to control how BitLocker-protected operating system drives are recovered in the absence of the required startup key information. This policy setting is applied when you turn on BitLocker.

The "Allow certificate-based data recovery agent" check box is used to specify whether a Data Recovery Agent can be used with BitLocker-protected operating system drives. Before a Data Recovery Agent can be used it must be added from the Public Key Policies item in either the Group Policy Management Console or the Local Group Policy Editor. Consult the BitLocker Drive Encryption Deployment Guide on Microsoft TechNet for more information about adding Data Recovery Agents.

The recommended state for this setting is: `Enabled: False` (unchecked).

Rationale:

Should a user lose their primary means for accessing an encrypted OS volume, or should the system not pass its boot time integrity checks, the system will go into recovery mode. If the recovery key has not been backed up to Active Directory, the user would need to have saved the recovery key to another location such as a USB flash drive, or have printed the recovery password, and now have access to one of those in order to recover the system. If the user is unable to produce the recovery key, then the user will be denied access to the encrypted volume and subsequently any data that is stored there.

Impact:

A Data Recovery Agent will not be permitted for the operating system drive. Users will need to be domain connected to turn on BitLocker. This policy is not FIPS complaint.

Audit:

Navigate to the UI 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\Policies\Microsoft\FVE:OSManageDRA

Remediation:

To establish the recommended configuration via GP, set the following UI path to Enabled: False (unchecked):

Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives\Choose how BitLocker-protected operating system drives can be recovered: Allow data recovery agent

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template VolumeEncryption.admx/adml that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Default Value:

Enabled: True. (A DRA is allowed.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.6 Encrypt Data on End-User Devices Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.	●	●	●
v7	13.6 Encrypt the Hard Drive of All Mobile Devices. Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.	●	●	●

18.9.11.2.5 (BL) Ensure 'Choose how BitLocker-protected operating system drives can be recovered: Recovery Password' is set to 'Enabled: Require 48-digit recovery password' (Automated)

Profile Applicability:

- Level 1 (L1) + BitLocker (BL)
- Level 2 (L2) + BitLocker (BL)
- BitLocker (BL) - optional add-on for when BitLocker is deployed

Description:

This policy setting allows you to control how BitLocker-protected operating system drives are recovered in the absence of the required startup key information. This policy setting is applied when you turn on BitLocker.

In "Configure user storage of BitLocker recovery information" select whether users are allowed, required, or not allowed to generate a 48-digit recovery password or a 256-bit recovery key.

The recommended state for this setting is: Enabled: Require 48-digit recovery password.

Rationale:

Should a user lose their primary means for accessing an encrypted OS volume, or should the system not pass its boot time integrity checks, the system will go into recovery mode. If the recovery key has not been backed up to Active Directory, the user would need to have saved the recovery key to another location such as a USB flash drive, or have printed the recovery password, and now have access to one of those in order to recover the system. If the user is unable to produce the recovery key, then the user will be denied access to the encrypted volume and subsequently any data that is stored there.

Impact:

A 48-digit recovery password will be required for the operating system drive. Users will need to be domain connected to turn on BitLocker. This policy is not FIPS complaint.

Audit:

Navigate to the UI 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\Policies\Microsoft\FVE:OSRecoveryPassword

Remediation:

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

Require 48-digit recovery password:

Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives\Choose how BitLocker-protected operating system drives can be recovered: Recovery Password

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template VolumeEncryption.admx/adml that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Default Value:

Recovery options are specified by the user.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.6 Encrypt Data on End-User Devices Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.	●	●	●
v7	13.6 Encrypt the Hard Drive of All Mobile Devices. Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.	●	●	●

18.9.11.2.6 (BL) Ensure 'Choose how BitLocker-protected operating system drives can be recovered: Recovery Key' is set to 'Enabled: Do not allow 256-bit recovery key' (Automated)

Profile Applicability:

- Level 1 (L1) + BitLocker (BL)
- Level 2 (L2) + BitLocker (BL)
- BitLocker (BL) - optional add-on for when BitLocker is deployed

Description:

This policy setting allows you to control how BitLocker-protected operating system drives are recovered in the absence of the required startup key information. This policy setting is applied when you turn on BitLocker.

In "Configure user storage of BitLocker recovery information" select whether users are allowed, required, or not allowed to generate a 48-digit recovery password or a 256-bit recovery key.

The recommended state for this setting is: Enabled: Do not allow 256-bit recovery key.

Rationale:

Should a user lose their primary means for accessing an encrypted OS volume, or should the system not pass its boot time integrity checks, the system will go into recovery mode. If the recovery key has not been backed up to Active Directory, the user would need to have saved the recovery key to another location such as a USB flash drive, or have printed the recovery password, and now have access to one of those in order to recover the system. If the user is unable to produce the recovery key, then the user will be denied access to the encrypted volume and subsequently any data that is stored there.

Impact:

A 256-bit recovery key will not be permitted for the operating system drive. Users will need to be domain connected to turn on BitLocker. This policy is not FIPS complaint.

Audit:

Navigate to the UI 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\Policies\Microsoft\FVE:OSRecoveryKey

Remediation:

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

Do not allow 256-bit recovery key:

Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives\Choose how BitLocker-protected operating system drives can be recovered: Recovery Key

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template VolumeEncryption.admx/adml that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Default Value:

Recovery options are specified by the user.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.6 Encrypt Data on End-User Devices Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.	●	●	●
v7	13.6 Encrypt the Hard Drive of All Mobile Devices. Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.	●	●	●

18.9.11.2.7 (BL) Ensure 'Choose how BitLocker-protected operating system drives can be recovered: Omit recovery options from the BitLocker setup wizard' is set to 'Enabled: True' (Automated)

Profile Applicability:

- Level 1 (L1) + BitLocker (BL)
- Level 2 (L2) + BitLocker (BL)
- BitLocker (BL) - optional add-on for when BitLocker is deployed

Description:

This policy setting allows you to control how BitLocker-protected operating system drives are recovered in the absence of the required startup key information. This policy setting is applied when you turn on BitLocker.

Select "Omit recovery options from the BitLocker setup wizard" to prevent users from specifying recovery options when they enable BitLocker on a drive. This means that you will not be able to specify which recovery option to use when you enable BitLocker, instead BitLocker recovery options for the drive are determined by the policy setting.

The recommended state for this setting is: Enabled: True (checked).

Rationale:

Should a user lose their primary means for accessing an encrypted OS volume, or should the system not pass its boot time integrity checks, the system will go into recovery mode. If the recovery key has not been backed up to Active Directory, the user would need to have saved the recovery key to another location such as a USB flash drive, or have printed the recovery password, and now have access to one of those in order to recover the system. If the user is unable to produce the recovery key, then the user will be denied access to the encrypted volume and subsequently any data that is stored there.

Impact:

The ability to manually select recovery options for the operating drive will not be presented to the user in the BitLocker setup wizard.

Audit:

Navigate to the UI 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\ Policies\Microsoft\FVE:OSHideRecoveryPage

Remediation:

To establish the recommended configuration via GP, set the following UI path to Enabled: True (checked):

Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives\Choose how BitLocker-protected operating system drives can be recovered: Omit recovery options from the BitLocker setup wizard

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template VolumeEncryption.admx/adml that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Default Value:

Recovery options for the operating system drive are selectable by the user in the BitLocker setup wizard.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.6 Encrypt Data on End-User Devices Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.	●	●	●
v7	13.6 Encrypt the Hard Drive of All Mobile Devices. Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.	●	●	●

18.9.11.2.8 (BL) Ensure 'Choose how BitLocker-protected operating system drives can be recovered: Save BitLocker recovery information to AD DS for operating system drives' is set to 'Enabled: True' (Automated)

Profile Applicability:

- Level 1 (L1) + BitLocker (BL)
- Level 2 (L2) + BitLocker (BL)
- BitLocker (BL) - optional add-on for when BitLocker is deployed

Description:

This policy setting allows you to control how BitLocker-protected operating system drives are recovered in the absence of the required startup key information. This policy setting is applied when you turn on BitLocker.

In "Save BitLocker recovery information to Active Directory Domain Services", choose which BitLocker recovery information to store in AD DS for operating system drives. If you select "Backup recovery password and key package", both the BitLocker recovery password and key package are stored in AD DS. Storing the key package supports recovering data from a drive that has been physically corrupted. If you select "Backup recovery password only", only the recovery password is stored in AD DS.

The recommended state for this setting is: `Enabled: True` (checked).

Rationale:

Should a user lose their primary means for accessing an encrypted OS volume, or should the system not pass its boot time integrity checks, the system will go into recovery mode. If the recovery key has not been backed up to Active Directory, the user would need to have saved the recovery key to another location such as a USB flash drive, or have printed the recovery password, and now have access to one of those in order to recover the system. If the user is unable to produce the recovery key, then the user will be denied access to the encrypted volume and subsequently any data that is stored there.

Impact:

BitLocker recovery information for the operating system drive will be backed up to AD DS. Users will need to be domain connected to turn on BitLocker. This policy is not FIPS complaint.

Audit:

Navigate to the UI 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\Policies\Microsoft\FVE:OSActiveDirectoryBackup

Remediation:

To establish the recommended configuration via GP, set the following UI path to Enabled: True (checked):

Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives\Choose how BitLocker-protected operating system drives can be recovered: Save BitLocker recovery information to AD DS for operating system drives

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template VolumeEncryption.admx/adml that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Default Value:

BitLocker recovery information for the operating system drive is not backed up to AD DS.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.6 Encrypt Data on End-User Devices Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.	●	●	●
v7	13.6 Encrypt the Hard Drive of All Mobile Devices. Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.	●	●	●

18.9.11.2.9 (BL) Ensure 'Choose how BitLocker-protected operating system drives can be recovered: Configure storage of BitLocker recovery information to AD DS:' is set to 'Enabled: Store recovery passwords and key packages' (Automated)

Profile Applicability:

- Level 1 (L1) + BitLocker (BL)
- Level 2 (L2) + BitLocker (BL)
- BitLocker (BL) - optional add-on for when BitLocker is deployed

Description:

This policy setting allows you to control how BitLocker-protected operating system drives are recovered in the absence of the required startup key information. This policy setting is applied when you turn on BitLocker.

In "Save BitLocker recovery information to Active Directory Domain Services", choose which BitLocker recovery information to store in AD DS for operating system drives. If you select "Backup recovery password and key package", both the BitLocker recovery password and key package are stored in AD DS. Storing the key package supports recovering data from a drive that has been physically corrupted. If you select "Backup recovery password only", only the recovery password is stored in AD DS.

The recommended state for this setting is: Enabled: Store recovery passwords and key packages.

Rationale:

Should a user lose their primary means for accessing an encrypted OS volume, or should the system not pass its boot time integrity checks, the system will go into recovery mode. If the recovery key has not been backed up to Active Directory, the user would need to have saved the recovery key to another location such as a USB flash drive, or have printed the recovery password, and now have access to one of those in order to recover the system. If the user is unable to produce the recovery key, then the user will be denied access to the encrypted volume and subsequently any data that is stored there.

Impact:

Both the recovery password and the key package for the operating system drive will be saved to AD DS. Users will need to be domain connected to turn on BitLocker. This policy is not FIPS complaint.

Audit:

Navigate to the UI 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\Policies\Microsoft\FVE:OSActiveDirectoryInfoToStore
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to Enabled:
Store recovery passwords and key packages:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives\Choose how BitLocker-protected operating system drives can be recovered: Configure storage of BitLocker recovery information to AD DS:
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `volumeEncryption.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Default Value:

BitLocker recovery information for the operating system drive is not backed up to AD DS.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.6 Encrypt Data on End-User Devices Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.	●	●	●
v7	13.6 Encrypt the Hard Drive of All Mobile Devices. Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.	●	●	●

18.9.11.2.10 (BL) Ensure 'Choose how BitLocker-protected operating system drives can be recovered: Do not enable BitLocker until recovery information is stored to AD DS for operating system drives' is set to 'Enabled: True' (Automated)

Profile Applicability:

- Level 1 (L1) + BitLocker (BL)
- Level 2 (L2) + BitLocker (BL)
- BitLocker (BL) - optional add-on for when BitLocker is deployed

Description:

This policy setting allows you to control how BitLocker-protected operating system drives are recovered in the absence of the required startup key information. This policy setting is applied when you turn on BitLocker.

Select the "Do not enable BitLocker until recovery information is stored in AD DS for operating system drives" check box if you want to prevent users from enabling BitLocker unless the computer is connected to the domain and the backup of BitLocker recovery information to AD DS succeeds.

Note: If the "Do not enable BitLocker until recovery information is stored in AD DS for operating system drives" check box is selected, a recovery password is automatically generated.

The recommended state for this setting is: Enabled: True (checked).

Rationale:

Should a user lose their primary means for accessing an encrypted OS volume, or should the system not pass its boot time integrity checks, the system will go into recovery mode. If the recovery key has not been backed up to Active Directory, the user would need to have saved the recovery key to another location such as a USB flash drive, or have printed the recovery password, and now have access to one of those in order to recover the system. If the user is unable to produce the recovery key, then the user will be denied access to the encrypted volume and subsequently any data that is stored there.

Impact:

Users will need to be domain connected and the back up of BitLocker recovery information for the operating system drive must succeed in order to turn on BitLocker. This policy is not FIPS complaint.

Audit:

Navigate to the UI 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\Policies\Microsoft\FVE:OSRequireActiveDirectoryBackup
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives\Choose how BitLocker-protected operating system drives can be recovered: Do not enable BitLocker until recovery information is stored to AD DS for operating system drives
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `volumeEncryption.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Default Value:

BitLocker can be enabled on the operating system drive without the requirement of storing recovery information to Active Directory first.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.6 Encrypt Data on End-User Devices Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.	●	●	●
v7	13.6 Encrypt the Hard Drive of All Mobile Devices. Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.	●	●	●

18.9.11.2.11 (BL) Ensure 'Configure use of hardware-based encryption for operating system drives' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) + BitLocker (BL)
- Level 2 (L2) + BitLocker (BL)
- BitLocker (BL) - optional add-on for when BitLocker is deployed

Description:

This policy setting allows you to manage BitLocker's use of hardware-based encryption on operating system drives and specify which encryption algorithms it can use with hardware-based encryption. Using hardware-based encryption can improve performance of drive operations that involve frequent reading or writing of data to the drive.

You can specify additional options that control whether BitLocker software-based encryption is used instead of hardware-based encryption on computers that do not support hardware-based encryption and whether you want to restrict the encryption algorithms and cipher suites used with hardware-based encryption.

The recommended state for this setting is: Disabled.

Rationale:

From a security perspective hardware-based encryption may introduce vulnerabilities in the hardware encryption of certain self-encrypting drives (SEDs), if the vendor and/or user has not updated the firmware to remediate the vulnerability. For more information visit [ADV180028 - Security Update Guide - Microsoft - Guidance for configuring BitLocker to enforce software encryption.](#)

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:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\FVE:OSHardwareEncryption

Remediation:

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

Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives\Configure use of hardware-based encryption for operating system drives

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `VolumeEncryption.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

BitLocker will use software-based encryption irrespective of hardware-based encryption availability.

References:

1. <https://msrc.microsoft.com/update-guide/en-US/vulnerability/ADV180028>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.6 Encrypt Data on End-User Devices Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.	●	●	●
v7	13.6 Encrypt the Hard Drive of All Mobile Devices. Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.	●	●	●

18.9.11.2.12 (BL) Ensure 'Configure use of passwords for operating system drives' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) + BitLocker (BL)
- Level 2 (L2) + BitLocker (BL)
- BitLocker (BL) - optional add-on for when BitLocker is deployed

Description:

This policy setting specifies the constraints for passwords used to unlock BitLocker-protected operating system drives.

Note: This setting is enforced when turning on BitLocker, not when unlocking a volume. BitLocker will allow unlocking a drive with any of the protectors available on the drive.

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

Rationale:

Using a dictionary-style attack, passwords can be guessed or discovered by repeatedly attempting to unlock a drive. Since this type of BitLocker password does include anti-dictionary attack protections provided by a TPM, for example, there is no mechanism to slow down rapid brute-force attacks against them.

Impact:

The password option will not be available when configuring BitLocker for the operating system drive.

Audit:

Navigate to the UI 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\Policies\Microsoft\FVE:OSPassphrase`

Remediation:

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

Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives\Configure use of passwords for operating system drives

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `VolumeEncryption.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

Passwords are supported, without complexity requirements and with an 8 character minimum.

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	13.6 Encrypt the Hard Drive of All Mobile Devices. Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.	●	●	●

18.9.11.2.13 (BL) Ensure 'Require additional authentication at startup' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) + BitLocker (BL)
- Level 2 (L2) + BitLocker (BL)
- BitLocker (BL) - optional add-on for when BitLocker is deployed

Description:

This policy setting allows you to configure whether BitLocker requires additional authentication each time the computer starts and whether you are using BitLocker with or without a Trusted Platform Module (TPM). This policy setting is applied when you turn on BitLocker.

Note: Only one of the additional authentication options can be required at startup, otherwise a policy error occurs.

If you want to use BitLocker on a computer without a TPM, select the "Allow BitLocker without a compatible TPM" check box. In this mode a USB drive is required for start-up and the key information used to encrypt the drive is stored on the USB drive, creating a USB key. When the USB key is inserted the access to the drive is authenticated and the drive is accessible. If the USB key is lost or unavailable you will need to use one of the BitLocker recovery options to access the drive.

On a computer with a compatible TPM, four types of authentication methods can be used at startup to provide added protection for encrypted data. When the computer starts, it can use only the TPM for authentication, or it can also require insertion of a USB flash drive containing a startup key, the entry of a 4-digit to 20-digit personal identification number (PIN), or both.

Users can configure advanced startup options in the BitLocker setup wizard.

Note #2: If you want to require the use of a startup PIN and a USB flash drive, you must configure BitLocker settings using the command-line tool `manage-bde` instead of the BitLocker Drive Encryption setup wizard.

The recommended state for this setting is: Enabled.

Rationale:

TPM without use of a PIN will only validate early boot components and does not require a user to enter any additional authentication information. If a computer is lost or stolen in this configuration, BitLocker will not provide any additional measure of protection beyond what is provided by native Windows authentication unless the early boot components are tampered with or the encrypted drive is removed from the machine.

Impact:

A PIN requires physical presence to restart the computer. This functionality is not compatible with Wake on LAN solutions.

Audit:

Navigate to the UI 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\Policies\Microsoft\FVE:UseAdvancedStartup

Remediation:

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

Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives\Require additional authentication at startup

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template volumeEncryption.admx/adml that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Default Value:

Disabled. (Users can configure only basic options on computers with a TPM.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.6 Encrypt Data on End-User Devices Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.	●	●	●
v7	13.6 Encrypt the Hard Drive of All Mobile Devices. Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.	●	●	●

18.9.11.2.14 (BL) Ensure 'Require additional authentication at startup: Allow BitLocker without a compatible TPM' is set to 'Enabled: False' (Automated)

Profile Applicability:

- Level 1 (L1) + BitLocker (BL)
- Level 2 (L2) + BitLocker (BL)
- BitLocker (BL) - optional add-on for when BitLocker is deployed

Description:

This policy setting allows you to configure whether you can use BitLocker without a Trusted Platform Module (TPM), instead using a password or startup key on a USB flash drive. This policy setting is applied when you turn on BitLocker.

The recommended state for this setting is: `Enabled: False` (unchecked).

Rationale:

TPM without use of a PIN will only validate early boot components and does not require a user to enter any additional authentication information. If a computer is lost or stolen in this configuration, BitLocker will not provide any additional measure of protection beyond what is provided by native Windows authentication unless the early boot components are tampered with or the encrypted drive is removed from the machine.

Impact:

A compatible TPM will be required in order to use BitLocker.

Audit:

Navigate to the UI 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\Policies\Microsoft\FVE:EnableBDEWithNoTPM`

Remediation:

To establish the recommended configuration via GP, set the following UI path to Enabled: False (unchecked):

```
Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives\Require additional authentication at startup: Allow BitLocker without a compatible TPM
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `volumeEncryption.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Default Value:

True (checked). (Users can use BitLocker without a compatible TPM by using a password or startup key on a USB flash drive.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.6 Encrypt Data on End-User Devices Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.	●	●	●
v7	13.6 Encrypt the Hard Drive of All Mobile Devices. Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.	●	●	●

18.9.11.3 Removable Data Drives

This section contains recommendations for configuring Removable Data Drives in BitLocker.

This Group Policy section is provided by the Group Policy template `VolumeEncryption.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.9.11.3.1 (BL) Ensure 'Allow access to BitLocker-protected removable data drives from earlier versions of Windows' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) + BitLocker (BL)
- Level 2 (L2) + BitLocker (BL)
- BitLocker (BL) - optional add-on for when BitLocker is deployed

Description:

This policy setting configures whether or not removable data drives formatted with the FAT file system can be unlocked and viewed on computers running Windows Server 2008 (non-R2), Windows Vista, Windows XP with Service Pack 3 (SP3), or Windows XP with Service Pack 2 (SP2) operating systems.

Note: This policy setting does not apply to drives that are formatted with the NTFS file system.

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

Rationale:

By default BitLocker virtualizes FAT formatted drives to permit access via the BitLocker To Go Reader on previous versions of Windows. Additionally the BitLocker To Go Reader application is applied to the unencrypted portion of the drive.

The BitLocker To Go Reader application, like any other application, is subject to spoofing and could be a mechanism to propagate malware.

Impact:

Removable data drives formatted with the FAT file system that are BitLocker-protected cannot be unlocked on computers running Windows Server 2008 (non-R2), Windows Vista, Windows XP with SP3 or Windows XP with SP2. `BitLockerToGo.exe` will not be 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:

`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\FVE:RDVDDiscoveryVolumeType`

Remediation:

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

`Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Removable Data Drives\Allow access to BitLocker-protected removable data drives from earlier versions of Windows`

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `VolumeEncryption.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Default Value:

Enabled. (Removable data drives formatted with the FAT file system can be unlocked on computers running Windows Server 2008 (non-R2), Windows Vista, Windows XP with SP3 or Windows XP with SP2, and their content can be viewed. These operating systems will only have read-only access to BitLocker-protected drives.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.6 Encrypt Data on End-User Devices Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.	●	●	●
v7	13.6 Encrypt the Hard Drive of All Mobile Devices. Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.	●	●	●

18.9.11.3.2 (BL) Ensure 'Choose how BitLocker-protected removable drives can be recovered' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) + BitLocker (BL)
- Level 2 (L2) + BitLocker (BL)
- BitLocker (BL) - optional add-on for when BitLocker is deployed

Description:

This policy setting allows you to control how BitLocker-protected removable data drives are recovered in the absence of the required credentials. This policy setting is applied when you turn on BitLocker.

The "Allow data recovery agent" check box is used to specify whether a Data Recovery Agent can be used with BitLocker-protected removable data drives. Before a Data Recovery Agent can be used it must be added from the Public Key Policies item in either the Group Policy Management Console or the Local Group Policy Editor. Consult the BitLocker Drive Encryption Deployment Guide on Microsoft TechNet for more information about adding Data Recovery Agents.

In "Configure user storage of BitLocker recovery information" select whether users are allowed, required, or not allowed to generate a 48-digit recovery password or a 256-bit recovery key.

Select "Omit recovery options from the BitLocker setup wizard" to prevent users from specifying recovery options when they enable BitLocker on a drive. This means that you will not be able to specify which recovery option to use when you enable BitLocker, instead BitLocker recovery options for the drive are determined by the policy setting.

In "Save BitLocker recovery information to Active Directory Domain Services" choose which BitLocker recovery information to store in AD DS for removable data drives. If you select "Backup recovery password and key package", both the BitLocker recovery password and key package are stored in AD DS. If you select "Backup recovery password only", only the recovery password is stored in AD DS.

Select the "Do not enable BitLocker until recovery information is stored in AD DS for removable data drives" check box if you want to prevent users from enabling BitLocker unless the computer is connected to the domain and the backup of BitLocker recovery information to AD DS succeeds.

Note: If the "Do not enable BitLocker until recovery information is stored in AD DS for removable data drives" check box is selected, a recovery password is automatically generated.

The recommended state for this setting is: Enabled.

Rationale:

Administrators should always have a safe, secure way to access encrypted data in the event users cannot access their data.

Additionally, as with any authentication method, a drive can be compromised by guessing or finding the authentication information used to access the drive.

Impact:

To use BitLocker a Data Recovery Agent will need to be configured for removable drives. To recover a drive will require highly-controlled access to the Data Recovery Agent private key.

Audit:

Navigate to the UI 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\Policies\Microsoft\FVE:RDVRecovery
--

Remediation:

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

Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Removable Data Drives\Choose how BitLocker-protected removable drives can be recovered

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `VolumeEncryption.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Default Value:

Disabled. (The default recovery options are supported for BitLocker recovery - a DRA is allowed, and the recovery options can be specified by the user including the recovery password and recovery key, and recovery information is not backed up to AD DS.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.9 <u>Encrypt Data on Removable Media</u> Encrypt data on removable media.		●	●
v7	13.6 <u>Encrypt the Hard Drive of All Mobile Devices.</u> Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.	●	●	●

18.9.11.3.3 (BL) Ensure 'Choose how BitLocker-protected removable drives can be recovered: Allow data recovery agent' is set to 'Enabled: True' (Automated)

Profile Applicability:

- Level 1 (L1) + BitLocker (BL)
- Level 2 (L2) + BitLocker (BL)
- BitLocker (BL) - optional add-on for when BitLocker is deployed

Description:

This policy setting allows you to control how BitLocker-protected removable data drives are recovered in the absence of the required credentials. This policy setting is applied when you turn on BitLocker.

The "Allow data recovery agent" check box is used to specify whether a Data Recovery Agent can be used with BitLocker-protected removable data drives. Before a Data Recovery Agent can be used it must be added from the Public Key Policies item in either the Group Policy Management Console or the Local Group Policy Editor. Consult the BitLocker Drive Encryption Deployment Guide on Microsoft TechNet for more information about adding Data Recovery Agents.

The recommended state for this setting is: Enabled: True (checked).

Rationale:

Administrators should always have a safe, secure way to access encrypted data in the event users cannot access their data.

Additionally, as with any authentication method, a drive can be compromised by guessing or finding the authentication information used to access the drive.

To use BitLocker a Data Recovery Agent will need to be configured for removable drives. To recover a drive will require highly-controlled access to the Data Recovery Agent private key.

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:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\FVE:RDVManageDRA

Remediation:

To establish the recommended configuration via GP, set the following UI path to Enabled: True (checked):

Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Removable Data Drives\Choose how BitLocker-protected removable drives can be recovered: Allow data recovery agent

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template VolumeEncryption.admx/adml that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Default Value:

Enabled: True. (A DRA is allowed.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.9 Encrypt Data on Removable Media Encrypt data on removable media.		●	●
v7	13.6 Encrypt the Hard Drive of All Mobile Devices. Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.	●	●	●

18.9.11.3.4 (BL) Ensure 'Choose how BitLocker-protected removable drives can be recovered: Recovery Password' is set to 'Enabled: Do not allow 48-digit recovery password' (Automated)

Profile Applicability:

- Level 1 (L1) + BitLocker (BL)
- Level 2 (L2) + BitLocker (BL)
- BitLocker (BL) - optional add-on for when BitLocker is deployed

Description:

This policy setting allows you to control how BitLocker-protected removable data drives are recovered in the absence of the required credentials. This policy setting is applied when you turn on BitLocker.

In "Configure user storage of BitLocker recovery information" select whether users are allowed, required, or not allowed to generate a 48-digit recovery password or a 256-bit recovery key.

The recommended state for this setting is: Enabled: Do not allow 48-digit recovery password.

Rationale:

Administrators should always have a safe, secure way to access encrypted data in the event users cannot access their data.

Additionally, as with any authentication method, a drive can be compromised by guessing or finding the authentication information used to access the drive.

To use BitLocker a Data Recovery Agent will need to be configured for removable drives. To recover a drive will require highly-controlled access to the Data Recovery Agent private key.

Impact:

A 48-digit recovery password will not be permitted for removable drives.

Audit:

Navigate to the UI 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\ Policies\Microsoft\FVE:RDVRecoveryPassword

Remediation:

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

Do not allow 48-digit recovery password:

Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Removable Data Drives\Choose how BitLocker-protected removable drives can be recovered: Recovery Password

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template VolumeEncryption.admx/adml that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Default Value:

Recovery options are specified by the user.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.9 Encrypt Data on Removable Media Encrypt data on removable media.		●	●
v7	13.6 Encrypt the Hard Drive of All Mobile Devices. Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.	●	●	●

18.9.11.3.5 (BL) Ensure 'Choose how BitLocker-protected removable drives can be recovered: Recovery Key' is set to 'Enabled: Do not allow 256-bit recovery key' (Automated)

Profile Applicability:

- Level 1 (L1) + BitLocker (BL)
- Level 2 (L2) + BitLocker (BL)
- BitLocker (BL) - optional add-on for when BitLocker is deployed

Description:

This policy setting allows you to control how BitLocker-protected removable data drives are recovered in the absence of the required credentials. This policy setting is applied when you turn on BitLocker.

In "Configure user storage of BitLocker recovery information" select whether users are allowed, required, or not allowed to generate a 48-digit recovery password or a 256-bit recovery key.

The recommended state for this setting is: Enabled: Do not allow 256-bit recovery key.

Rationale:

Administrators should always have a safe, secure way to access encrypted data in the event users cannot access their data.

Additionally, as with any authentication method, a drive can be compromised by guessing or finding the authentication information used to access the drive.

To use BitLocker a Data Recovery Agent will need to be configured for removable drives. To recover a drive will require highly-controlled access to the Data Recovery Agent private key.

Impact:

A 256-bit recovery key will not be permitted for removable drives.

Audit:

Navigate to the UI 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\ Policies\Microsoft\FVE:RDVRecoveryKey

Remediation:

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

Do not allow 256-bit recovery key:

Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Removable Data Drives\Choose how BitLocker-protected removable drives can be recovered: Recovery Key

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template VolumeEncryption.admx/adml that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Default Value:

Recovery options are specified by the user.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.9 Encrypt Data on Removable Media Encrypt data on removable media.		●	●
v7	13.6 Encrypt the Hard Drive of All Mobile Devices. Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.	●	●	●

18.9.11.3.6 (BL) Ensure 'Choose how BitLocker-protected removable drives can be recovered: Omit recovery options from the BitLocker setup wizard' is set to 'Enabled: True' (Automated)

Profile Applicability:

- Level 1 (L1) + BitLocker (BL)
- Level 2 (L2) + BitLocker (BL)
- BitLocker (BL) - optional add-on for when BitLocker is deployed

Description:

This policy setting allows you to control how BitLocker-protected removable data drives are recovered in the absence of the required credentials. This policy setting is applied when you turn on BitLocker.

Select "Omit recovery options from the BitLocker setup wizard" to prevent users from specifying recovery options when they enable BitLocker on a drive. This means that you will not be able to specify which recovery option to use when you enable BitLocker, instead BitLocker recovery options for the drive are determined by the policy setting.

The recommended state for this setting is: Enabled: True (checked).

Rationale:

Administrators should always have a safe, secure way to access encrypted data in the event users cannot access their data.

Additionally, as with any authentication method, a drive can be compromised by guessing or finding the authentication information used to access the drive.

To use BitLocker a Data Recovery Agent will need to be configured for removable drives. To recover a drive will require highly-controlled access to the Data Recovery Agent private key.

Impact:

The ability to manually select recovery options for removable drives will not be presented to the user in the BitLocker setup wizard.

Audit:

Navigate to the UI 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\ Policies\Microsoft\FVE:RDVHideRecoveryPage

Remediation:

To establish the recommended configuration via GP, set the following UI path to Enabled: True (checked):

Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Removable Data Drives\Choose how BitLocker-protected removable drives can be recovered: Omit recovery options from the BitLocker setup wizard

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template VolumeEncryption.admx/adml that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Default Value:

Recovery options for removable drives are selectable by the user in the BitLocker setup wizard.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.9 <u>Encrypt Data on Removable Media</u> Encrypt data on removable media.		●	●
v7	13.6 <u>Encrypt the Hard Drive of All Mobile Devices.</u> Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.	●	●	●

18.9.11.3.7 (BL) Ensure 'Choose how BitLocker-protected removable drives can be recovered: Save BitLocker recovery information to AD DS for removable data drives' is set to 'Enabled: False' (Automated)

Profile Applicability:

- Level 1 (L1) + BitLocker (BL)
- Level 2 (L2) + BitLocker (BL)
- BitLocker (BL) - optional add-on for when BitLocker is deployed

Description:

This policy setting allows you to control how BitLocker-protected removable data drives are recovered in the absence of the required credentials. This policy setting is applied when you turn on BitLocker.

In "Save BitLocker recovery information to Active Directory Domain Services" choose which BitLocker recovery information to store in AD DS for removable data drives. If you select "Backup recovery password and key package", both the BitLocker recovery password and key package are stored in AD DS. If you select "Backup recovery password only", only the recovery password is stored in AD DS.

The recommended state for this setting is: `Enabled: False` (unchecked).

Rationale:

Administrators should always have a safe, secure way to access encrypted data in the event users cannot access their data.

Additionally, as with any authentication method, a drive can be compromised by guessing or finding the authentication information used to access the drive.

To use BitLocker a Data Recovery Agent will need to be configured for removable drives. To recover a drive will require highly-controlled access to the Data Recovery Agent private key.

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:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\FVE:RDVActiveDirectoryBackup

Remediation:

To establish the recommended configuration via GP, set the following UI path to Enabled: False (unchecked):

Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Removable Data Drives\Choose how BitLocker-protected removable drives can be recovered: Save BitLocker recovery information to AD DS for removable data drives

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template VolumeEncryption.admx/adml that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Default Value:

BitLocker recovery information for removable drives is not backed up to AD DS.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.9 Encrypt Data on Removable Media Encrypt data on removable media.		●	●
v7	13.6 Encrypt the Hard Drive of All Mobile Devices. Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.	●	●	●

18.9.11.3.8 (BL) Ensure 'Choose how BitLocker-protected removable drives can be recovered: Configure storage of BitLocker recovery information to AD DS:' is set to 'Enabled: Backup recovery passwords and key packages' (Automated)

Profile Applicability:

- Level 1 (L1) + BitLocker (BL)
- Level 2 (L2) + BitLocker (BL)
- BitLocker (BL) - optional add-on for when BitLocker is deployed

Description:

This policy setting allows you to control how BitLocker-protected removable data drives are recovered in the absence of the required credentials. This policy setting is applied when you turn on BitLocker.

In "Save BitLocker recovery information to Active Directory Domain Services" choose which BitLocker recovery information to store in AD DS for removable data drives. If you select "Backup recovery password and key package", both the BitLocker recovery password and key package are stored in AD DS. If you select "Backup recovery password only", only the recovery password is stored in AD DS.

The recommended state for this setting is: Enabled: Backup recovery passwords and key packages.

Rationale:

Administrators should always have a safe, secure way to access encrypted data in the event users cannot access their data.

Additionally, as with any authentication method, a drive can be compromised by guessing or finding the authentication information used to access the drive.

To use BitLocker a Data Recovery Agent will need to be configured for removable drives. To recover a drive will require highly-controlled access to the Data Recovery Agent private key.

Impact:

None - this value is ignored when the checkbox above it (Save BitLocker recovery information to AD DS for removable data drives) is False (unchecked), as is required in Rule 18.9.11.3.7. If that checkbox is set to True (checked), both recovery passwords and key packages for removable drives will be saved to AD DS.

Audit:

Navigate to the UI 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\Policies\Microsoft\FVE:RDVActiveDirectoryInfoToStore

Remediation:

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

Backup recovery passwords and key packages:

Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Removable Data Drives\Choose how BitLocker-protected removable drives can be recovered: Configure storage of BitLocker recovery information to AD DS:

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template volumeEncryption.admx/adml that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Default Value:

BitLocker recovery information for removable drives is not backed up to AD DS.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.9 <u>Encrypt Data on Removable Media</u> Encrypt data on removable media.		●	●
v7	13.6 <u>Encrypt the Hard Drive of All Mobile Devices.</u> Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.	●	●	●

18.9.11.3.9 (BL) Ensure 'Choose how BitLocker-protected removable drives can be recovered: Do not enable BitLocker until recovery information is stored to AD DS for removable data drives' is set to 'Enabled: False' (Automated)

Profile Applicability:

- Level 1 (L1) + BitLocker (BL)
- Level 2 (L2) + BitLocker (BL)
- BitLocker (BL) - optional add-on for when BitLocker is deployed

Description:

This policy setting allows you to control how BitLocker-protected removable data drives are recovered in the absence of the required credentials. This policy setting is applied when you turn on BitLocker.

Select the "Do not enable BitLocker until recovery information is stored in AD DS for removable data drives" check box if you want to prevent users from enabling BitLocker unless the computer is connected to the domain and the backup of BitLocker recovery information to AD DS succeeds.

Note: If the "Do not enable BitLocker until recovery information is stored in AD DS for removable data drives" check box is selected, a recovery password is automatically generated.

The recommended state for this setting is: `Enabled: False` (unchecked).

Rationale:

Administrators should always have a safe, secure way to access encrypted data in the event users cannot access their data.

Additionally, as with any authentication method, a drive can be compromised by guessing or finding the authentication information used to access the drive.

To use BitLocker a Data Recovery Agent will need to be configured for removable drives. To recover a drive will require highly-controlled access to the Data Recovery Agent private key.

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:

HKEY_LOCAL_MACHINE\SOFTWARE\ Policies\Microsoft\FVE:RDVRequireActiveDirectoryBackup

Remediation:

To establish the recommended configuration via GP, set the following UI path to Enabled: False (unchecked):

Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Removable Data Drives\Choose how BitLocker-protected removable drives can be recovered: Do not enable BitLocker until recovery information is stored to AD DS for removable data drives

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template volumeEncryption.admx/adml that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Default Value:

BitLocker can be enabled on removable drives without the requirement of storing recovery information to Active Directory first.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.9 <u>Encrypt Data on Removable Media</u> Encrypt data on removable media.		●	●
v7	13.6 <u>Encrypt the Hard Drive of All Mobile Devices.</u> Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.	●	●	●

18.9.11.3.10 (BL) Ensure 'Configure use of hardware-based encryption for removable data drives' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) + BitLocker (BL)
- Level 2 (L2) + BitLocker (BL)
- BitLocker (BL) - optional add-on for when BitLocker is deployed

Description:

This policy setting allows you to manage BitLocker's use of hardware-based encryption on removable data drives and specify which encryption algorithms it can use with hardware-based encryption. Using hardware-based encryption can improve performance of drive operations that involve frequent reading or writing of data to the drive.

You can specify additional options that control whether BitLocker software-based encryption is used instead of hardware-based encryption on computers that do not support hardware-based encryption and whether you want to restrict the encryption algorithms and cipher suites used with hardware-based encryption.

The recommended state for this setting is: Disabled.

Rationale:

From a security perspective hardware-based encryption may introduce vulnerabilities in the hardware encryption of certain self-encrypting drives (SEDs), if the vendor and/or user has not updated the firmware to remediate the vulnerability. For more information visit [ADV180028 - Security Update Guide - Microsoft - Guidance for configuring BitLocker to enforce software encryption.](#)

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:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\FVE:RDVHardwareEncryption

Remediation:

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

Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Removable Data Drives\Configure use of hardware-based encryption for removable data drives

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `VolumeEncryption.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Default Value:

BitLocker will use software-based encryption irrespective of hardware-based encryption availability.

References:

1. <https://msrc.microsoft.com/update-guide/en-US/vulnerability/ADV180028>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.9 <u>Encrypt Data on Removable Media</u> Encrypt data on removable media.		●	●
v7	13.6 <u>Encrypt the Hard Drive of All Mobile Devices.</u> Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.	●	●	●

18.9.11.3.11 (BL) Ensure 'Configure use of passwords for removable data drives' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) + BitLocker (BL)
- Level 2 (L2) + BitLocker (BL)
- BitLocker (BL) - optional add-on for when BitLocker is deployed

Description:

This policy setting allows you to specify whether a password is required to unlock BitLocker-protected removable data drives.

Note: This setting is enforced when turning on BitLocker, not when unlocking a drive. BitLocker will allow unlocking a drive with any of the protectors available on the drive.

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

Rationale:

Using a dictionary-style attack, passwords can be guessed or discovered by repeatedly attempting to unlock a drive. Since this type of BitLocker password does not include anti-dictionary attack protections provided by a TPM, for example, there is no mechanism to slow down use of rapid brute-force attacks against them.

Impact:

The password option will not be available when configuring BitLocker for removable drives.

Audit:

Navigate to the UI 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\Policies\Microsoft\FVE:RDVPassphrase`

Remediation:

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

Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Removable Data Drives\Configure use of passwords for removable data drives

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `VolumeEncryption.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Default Value:

Passwords are supported, without complexity requirements and with an 8 character minimum.

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	13.6 Encrypt the Hard Drive of All Mobile Devices. Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.	●	●	●

18.9.11.3.12 (BL) Ensure 'Configure use of smart cards on removable data drives' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) + BitLocker (BL)
- Level 2 (L2) + BitLocker (BL)
- BitLocker (BL) - optional add-on for when BitLocker is deployed

Description:

This policy setting specifies whether smart cards can be used to authenticate user access to BitLocker-protected removable data drives on a computer.

Smart cards can be used to authenticate user access to the drive. You can require smart card authentication by selecting the "Require use of smart cards on removable data drives" check box.

Note: This setting is enforced when turning on BitLocker, not when unlocking a volume. BitLocker will allow unlocking a drive with any of the protectors available on the drive.

The recommended state for this setting is: Enabled.

Rationale:

A drive can be compromised by guessing or finding the authentication information used to access the drive. For example, a password could be guessed, or a drive set to automatically unlock could be lost or stolen with the computer it automatically unlocks with.

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:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\FVE:RDVAllowUserCert

Remediation:

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

Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Removable Data Drives\Configure use of smart cards on removable data drives

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `VolumeEncryption.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Default Value:

Enabled. (Users are allowed to use smart cards to authenticate their access to BitLocker-protected removable data drives.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.3 Require MFA for Externally-Exposed Applications Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.			
v7	16.3 Require Multi-factor Authentication Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.			

18.9.11.3.13 (BL) Ensure 'Configure use of smart cards on removable data drives: Require use of smart cards on removable data drives' is set to 'Enabled: True' (Automated)

Profile Applicability:

- Level 1 (L1) + BitLocker (BL)
- Level 2 (L2) + BitLocker (BL)
- BitLocker (BL) - optional add-on for when BitLocker is deployed

Description:

This policy setting specifies whether smart cards *must* be used to authenticate user access to BitLocker-protected removable data drives on a computer.

Smart cards can be used to authenticate user access to the drive. You can require smart card authentication by selecting the "Require use of smart cards on removable data drives" check box.

Note: This setting is enforced when turning on BitLocker, not when unlocking a volume. BitLocker will allow unlocking a drive with any of the protectors available on the drive.

The recommended state for this setting is: Enabled: True (checked).

Rationale:

A drive can be compromised by guessing or finding the authentication information used to access the drive. For example, a password could be guessed, or a drive set to automatically unlock could be lost or stolen with the computer it automatically unlocks with.

Impact:

Smart cards will be required to authenticate user access to removable data drives. Use of smart cards requires PKI infrastructure. Users will need to authenticate with the smart card to unlock the removable data drive every time they restart 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:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\FVE:RDVEnforceUserCert

Remediation:

To establish the recommended configuration via GP, set the following UI path to Enabled: True (checked):

Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Removable Data Drives\Configure use of smart cards on removable data drives: Require use of smart cards on removable data drives

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `VolumeEncryption.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Default Value:

Enabled: False (unchecked). (Users are allowed to use smart cards to authenticate their access to BitLocker-protected removable data drives, but it is not required.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.3 <u>Require MFA for Externally-Exposed Applications</u> Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.		●	●
v7	16.3 <u>Require Multi-factor Authentication</u> Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		●	●

18.9.11.3.14 (BL) Ensure 'Deny write access to removable drives not protected by BitLocker' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) + BitLocker (BL)
- Level 2 (L2) + BitLocker (BL)
- BitLocker (BL) - optional add-on for when BitLocker is deployed

Description:

This policy setting configures whether BitLocker protection is required for a computer to be able to write data to a removable data drive.

All removable data drives that are not BitLocker-protected will be mounted as read-only. If the drive is protected by BitLocker, it will be mounted with read and write access.

The recommended state for this setting is: Enabled.

Rationale:

Users may not voluntarily encrypt removable drives prior to saving important data to the drive.

Impact:

All removable data drives that are not BitLocker-protected will be mounted as read-only. If the drive is protected by BitLocker, it will be mounted with read and write access.

Audit:

Navigate to the UI 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\SYSTEM\CurrentControlSet\Policies\Microsoft\FVE:RDVDenyWriteAccess

Remediation:

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

Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Removable Data Drives\Deny write access to removable drives not protected by BitLocker

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `VolumeEncryption.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Default Value:

Disabled. (All removable data drives on the computer will be mounted with read and write access.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.9 Encrypt Data on Removable Media Encrypt data on removable media.		●	●
v7	13.6 Encrypt the Hard Drive of All Mobile Devices. Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.	●	●	●
v7	13.8 Manage System's External Removable Media's Read/write Configurations Configure systems not to write data to external removable media, if there is no business need for supporting such devices.			●

18.9.11.3.15 (BL) Ensure 'Deny write access to removable drives not protected by BitLocker: Do not allow write access to devices configured in another organization' is set to 'Enabled: False' (Automated)

Profile Applicability:

- Level 1 (L1) + BitLocker (BL)
- Level 2 (L2) + BitLocker (BL)
- BitLocker (BL) - optional add-on for when BitLocker is deployed

Description:

This policy setting configures whether the computer will be able to write data to BitLocker-protected removable drives that were configured in another organization.

The recommended state for this setting is: Enabled: False (unchecked).

Rationale:

Restricting write access to BitLocker-protected removable drives that were configured in another organization can hinder legitimate business operations where encrypted data sharing is necessary.

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:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\FVE:RDVDenyCrossOrg

Remediation:

To establish the recommended configuration via GP, set the following UI path to Enabled: False (unchecked):

Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Removable Data Drives\Deny write access to removable drives not protected by BitLocker: Do not allow write access to devices configured in another organization

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `VolumeEncryption.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Default Value:

Enabled: False (unchecked). (Write access will be permitted to BitLocker-protected removable drives that were configured in another organization.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.9 Encrypt Data on Removable Media Encrypt data on removable media.		●	●
v7	13.6 Encrypt the Hard Drive of All Mobile Devices. Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.	●	●	●
v7	13.8 Manage System's External Removable Media's Read/write Configurations Configure systems not to write data to external removable media, if there is no business need for supporting such devices.			●

18.9.11.4 (BL) Ensure 'Disable new DMA devices when this computer is locked' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) + BitLocker (BL)
- Level 2 (L2) + BitLocker (BL)
- BitLocker (BL) - optional add-on for when BitLocker is deployed

Description:

This policy setting allows you to block direct memory access (DMA) for all hot pluggable PCI downstream ports until a user logs into Windows.

The recommended state for this setting is: Enabled.

Note: Microsoft changed the implementation of this setting in Windows 10 R1709 to strengthen its enforcement. As a result, some hardware configurations may experience unexpected problems with this setting in that release (or newer), until updated firmware and/or drivers from the vendor are installed to correct the problem. See the Impact Statement for more information.

Rationale:

A BitLocker-protected computer may be vulnerable to Direct Memory Access (DMA) attacks when the computer is turned on or is in the Standby power state - this includes when the workstation is locked. Enabling this setting will help prevent such an attack while the computer is left unattended.

Impact:

Newly attached hardware devices that use DMA will not function on a locked (or signed out) workstation until the user has unlocked the session or logged in. Some hardware configurations may experience unexpected problems with this setting in Windows 10 R1709 (or newer), requiring updated firmware and/or drivers to correct the problem. See [MSKB 4057300](#) for more information. We recommend testing this setting on all examples of workstation hardware before deploying it on a large scale - to see if vendor firmware and/or driver updates are first required.

Audit:

Navigate to the UI 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\Policies\Microsoft\FVE:DisableExternalDMAUnderLock

Remediation:

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

Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Disable new DMA devices when this computer is locked

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `VolumeEncryption.admx/adml` that is included with the Microsoft Windows 10 Release 1703 Administrative Templates (or newer).

Default Value:

Disabled. (Newly attached DMA devices will function even while the workstation is locked or signed out.)

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™.			

18.9.12 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 Release 1607 & Server 2016 Administrative Templates (or newer).

18.9.12.1 (L2) Ensure 'Allow Use of Camera' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

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:

`HKEY_LOCAL_MACHINE\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 Release 1607 & Server 2016 Administrative Templates (or newer).

Default Value:

Enabled. (Camera devices are enabled.)

18.9.13 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 Release 21H2 Administrative Templates (or newer).

18.9.14 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 Release 1511 Administrative Templates (or newer).

18.9.14.1 (L1) Ensure 'Turn off cloud consumer account state content' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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.

Audit:

Navigate to the UI 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\Policies\Microsoft\Windows\CloudContent:DisableConsumerAccountStateContent
```

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 10 Release 21H2 Administrative Templates (or newer).

Default Value:

Disabled. (Windows experiences are able to use cloud consumer accounts.)

18.9.14.2 (L2) Ensure 'Turn off cloud optimized content' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This policy setting turns off cloud optimized content in all Windows experiences.

The recommended state for this setting is: Enabled.

Rationale:

Due to privacy concerns, data should never be sent to any 3rd party since this data could 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:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CloudContent:DisableCloudOptimizedContent

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 Release 20H2 Administrative Templates (or newer).

Default Value:

Disabled. (Windows experiences will be able to use cloud optimized content.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>			

18.9.14.3 (L1) Ensure 'Turn off Microsoft consumer experiences' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting turns off experiences that help consumers make the most of their devices and Microsoft account.

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:

Having apps silently install in an enterprise managed environment is not good security practice - especially if the apps send data back to a 3rd party.

Impact:

Users will no longer see personalized recommendations from Microsoft and notifications about their Microsoft 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:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CloudContent:DisableWindowsConsumerFeatures

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 Microsoft consumer 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 Release 1511 Administrative Templates (or newer).

Default Value:

Disabled. (Users may see suggestions from Microsoft and notifications about their Microsoft account.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>		●	●

18.9.15 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 Release 1607 & Server 2016 Administrative Templates (or newer).

18.9.15.1 (L1) Ensure 'Require pin for pairing' is set to 'Enabled: First Time' OR 'Enabled: Always' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

```
HKEY_LOCAL_MACHINE\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 Release 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 Release 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.)

18.9.16 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.

18.9.16.1 (L1) Ensure 'Do not display the password reveal button' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

```
HKEY_LOCAL_MACHINE\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.)

18.9.16.2 (L1) Ensure 'Enumerate administrator accounts on elevation' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 malicious user 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:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\CredUI:  
EnumerateAdministrators
```

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.)

18.9.16.3 (L1) Ensure 'Prevent the use of security questions for local accounts' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether security questions can be used to reset local account passwords. The security question feature does not apply to domain accounts, only local accounts on the workstation.

The recommended state for this setting is: Enabled.

Rationale:

Users could establish security questions that are easily guessed or sleuthed by observing the user's social media accounts, making it easier for a malicious actor to change the local user account password and gain access to the computer as that user account.

Impact:

Local user accounts will not be able to set up and use security questions to reset their 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:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System>NoLocalPasswordResetQuestions

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\Prevent the use of security questions for local accounts

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 10 Release 1903 Administrative Templates (or newer).

Default Value:

Not Configured. (Local user accounts are able to set up and use security questions to reset their passwords.)

18.9.17 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 (Release 1507) Administrative Templates (or newer).

**18.9.17.1 (L1) Ensure 'Allow Diagnostic Data' is set to 'Enabled:
Diagnostic data off (not recommended)' or 'Enabled: Send required
diagnostic data' (Automated)**

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

Sending any data to a 3rd party vendor is a security concern and should only be done on an as needed basis.

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:

```
HKEY_LOCAL_MACHINE\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 11 Release 21H2 Administrative Templates (or newer).

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Allow Telemetry*, but it was renamed to *Allow Diagnostic Data* starting with the Windows 11 Release 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>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
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.			

18.9.17.2 (L2) 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 (L2) - High Security/Sensitive Data Environment (limited functionality)

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:

Sending any data to a 3rd party vendor is a security concern and should only be done on an as needed basis.

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:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DataCollection:DisableEnterpriseAuthProxy
--

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 Release 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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>		●	●

18.9.17.3 (L1) Ensure 'Disable OneSettings Downloads' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether Windows attempts to connect with the OneSettings service to download configuration settings.

The recommended state for this setting is: Enabled.

Rationale:

Sending data to a 3rd party vendor is a security concern and should only be done on an as-needed basis.

Impact:

Windows will not connect with the OneSettings service to download configuration 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:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DataCollection:Disable  
OneSettingsDownloads
```

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\Disable OneSettings Downloads
```

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 Release 21H2 Administrative Templates (or newer).

Default Value:

Disabled. (Windows will periodically attempt to connect with the OneSettings service to download configuration settings.)

18.9.17.4 (L1) Ensure 'Do not show feedback notifications' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

Users should not be sending any feedback to 3rd party vendors in an enterprise managed environment.

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:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DataCollection:DoNotShowFeedbackNotifications
```

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 Release 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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>		●	●

18.9.17.5 (L1) Ensure 'Enable OneSettings Auditing' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether Windows records attempts to connect with the OneSettings service to the Operational EventLog.

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 malicious users.

Impact:

There should be no impact to 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:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\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 10 Release 21H2 Administrative Templates (or newer).

Default Value:

Disabled. (Windows will not record attempts to connect with the OneSettings service to the EventLog.)

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.			

18.9.17.6 (L1) Ensure 'Limit Diagnostic Log Collection' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 with 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:

Sending data to a 3rd-party vendor is a security concern and should only be done on an as-needed basis.

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:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DataCollection:LimitDiagnosticLogCollection
```

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 10 Release 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.)

18.9.17.7 (L1) Ensure 'Limit Dump Collection' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting limits the type of dumps that can be collected when more information is needed to troubleshoot a problem.

The recommended state for this setting is: Enabled.

Note: Dumps are only sent when the device has been configured to send optional diagnostic data. Diagnostic data is limited with recommendation Ensure Allow Diagnostic Data is set to Enabled: Diagnostic data off (not recommended) or Enabled: Send required diagnostic data to send only basic information.

Rationale:

Sending data to a 3rd party vendor is a security concern and should only be done on an as needed basis.

Impact:

Windows Error Reporting is limited to sending kernel mini and user mode triage memory dumps, reducing the risk of sending sensitive information 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:

```
HKEY_LOCAL_MACHINE\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 10 Release 21H2 Administrative Templates (or newer).

Default Value:

Disabled. (Microsoft may occasionally collect full or heap dumps if the user has opted to send optional diagnostic data.)

18.9.17.8 (L1) Ensure 'Toggle user control over Insider builds' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines whether users can access the Insider build controls in the Advanced Options for Windows Update. These controls are located under "Get Insider builds," and enable users to make their devices available for downloading and installing Windows preview software.

The recommended state for this setting is: Disabled.

Note: This policy setting applies only to devices running Windows 10 Pro or Windows 10 Enterprise, up until Release 1703. For Release 1709 or newer, Microsoft encourages using the `Manage preview builds` setting (Rule 18.9.103.1.1). We have kept this setting in the benchmark to ensure that any older builds of Windows 10 in the environment are still enforced.

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 an attacker to gain access. It is generally preferred to only use production-ready builds.

Impact:

The item "Get Insider builds" will be unavailable.

Audit:

Navigate to the UI 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\Policies\Microsoft\Windows\PreviewBuilds:AllowBuildPreview

Remediation:

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

Computer Configuration\Policies\Administrative Templates\Windows Components\Data Collection and Preview Builds\Toggle user control over Insider builds

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `AllowBuildPreview.admx/adml` that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

Default Value:

Enabled. (Users can download and install Windows preview software on their devices.)

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	●	●	●

18.9.18 Delivery Optimization

This section contains settings for Delivery Optimization.

This Group Policy section is provided by the Group Policy template `DeliveryOptimization.admx/adml` that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

18.9.18.1 (L1) Ensure 'Download Mode' is NOT set to 'Enabled: Internet' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting specifies the download method that Delivery Optimization can use in downloads of Windows Updates, Apps and App updates. The following methods are supported:

- 0 = HTTP only, no peering.
- 1 = HTTP blended with peering behind the same NAT.
- 2 = HTTP blended with peering across a private group. Peering occurs on devices in the same Active Directory Site (if exist) or the same domain by default. When this option is selected, peering will cross NATs. To create a custom group use Group ID in combination with Mode 2.
- 3 = HTTP blended with Internet Peering.
- 99 = Simple download mode with no peering. Delivery Optimization downloads using HTTP only and does not attempt to contact the Delivery Optimization cloud services.
- 100 = Bypass mode. Do not use Delivery Optimization and use BITS instead.

The recommended state for this setting is any value EXCEPT: `Enabled: Internet (3)`.

Note: The default on all SKUs other than Enterprise, Enterprise LTSB or Education is `Enabled: Internet (3)`, so on other SKUs, be sure to set this to a different value.

Rationale:

Due to privacy concerns and security risks, updates should only be downloaded directly from Microsoft, or from a trusted machine on the internal network that received *its* updates from a trusted source and approved by the network administrator.

Impact:

Machines will not be able to download updates from peers on the Internet. If set to Enabled: HTTP only (0), Enabled: Simple (99), or Enabled: Bypass (100), machines will not be able to download updates from other machines on the same LAN.

Audit:

Navigate to the UI 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\Policies\Microsoft\Windows\DeliveryOptimization:D  
ODownloadMode
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to any value *other than* Enabled: Internet (3):

```
Computer Configuration\Policies\Administrative Templates\Windows  
Components\Delivery Optimization\Download Mode
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `DeliveryOptimization.admx/adml` that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

Default Value:

Enterprise, Enterprise LTSB and Education SKUs: Enabled: LAN (1)

All other SKUs: Enabled: Internet (3)

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.	●	●	●

18.9.19 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).

18.9.20 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.

18.9.21 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).

18.9.22 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 (Release 1507) Administrative Templates.

18.9.23 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.

18.9.24 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).

18.9.25 EMET

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 `EMET.admx/adml` that is included with Microsoft EMET.

EMET is free and supported security software developed by Microsoft that allows an enterprise to apply exploit mitigations to applications that run on Windows. Many of these mitigations were later coded directly into Windows 10 and Server 2016.

Note: Although EMET is quite effective at enhancing exploit protection on Windows workstation OSes prior to Windows 10, it is highly recommended that compatibility testing is done on typical workstation configurations (including all CIS-recommended EMET settings) before widespread deployment to your environment.

Note #2: EMET has been reported to be very problematic on 32-bit OSes - we only recommend using it with 64-bit OSes.

Note #3: Microsoft has announced that EMET will be End-Of-Life (EOL) on July 31, 2018. This does not mean the software will stop working, only that Microsoft will not update it any further past that date, nor troubleshoot new problems with it. They are instead recommending that workstations be upgraded to Windows 10.

18.9.26 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).

18.9.27 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.

18.9.27.1 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.

18.9.27.1.1 (L1) Ensure 'Application: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 malicious users.

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:

HKEY_LOCAL_MACHINE\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.)

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.		●	●

18.9.27.1.2 (L1) Ensure 'Application: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 4 terabytes (4,194,240 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 malicious users.

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.

The consequence of this configuration is that older events will be removed from the logs. Attackers 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 an attacker 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 attacker's activities.

Audit:

Navigate to the UI 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\ 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.)

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.		●	●

18.9.27.2 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.

18.9.27.2.1 (L1) Ensure 'Security: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 malicious users.

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:

HKEY_LOCAL_MACHINE\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.)

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.	●	●	

18.9.27.2.2 (L1) Ensure 'Security: Specify the maximum log file size (KB)' is set to 'Enabled: 196,608 or greater' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 4 terabytes (4,194,240 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 malicious users.

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.

The consequence of this configuration is that older events will be removed from the logs. Attackers 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 an attacker 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 attacker's activities.

Audit:

Navigate to the UI 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\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.)

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.		●	●

18.9.27.3 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.

18.9.27.3.1 (L1) Ensure 'Setup: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 malicious users.

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:

`HKEY_LOCAL_MACHINE\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.)

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.	●	●	

18.9.27.3.2 (L1) Ensure 'Setup: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 4 terabytes (4,194,240 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 malicious users

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.

The consequence of this configuration is that older events will be removed from the logs. Attackers 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 an attacker 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 attacker's activities.

Audit:

Navigate to the UI 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\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.)

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.		●	●

18.9.27.4 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.

18.9.27.4.1 (L1) Ensure 'System: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 malicious users.

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:

<code>HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\EventLog\System:Retention</code>

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.)

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.	●	●	

18.9.27.4.2 (L1) Ensure 'System: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 4 terabytes (4,194,240 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 malicious users

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.

The consequence of this configuration is that older events will be removed from the logs. Attackers 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 an attacker 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 attacker's activities.

Audit:

Navigate to the UI 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\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.)

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.		●	●

18.9.28 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 (Release 1507) Administrative Templates (or newer).

18.9.29 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.

18.9.30 Family Safety (formerly Parental Controls)

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 `ParentalControls.admx/adml` that is only included with the Microsoft Windows Vista through the Windows 10 RTM (Release 1507) Administrative Templates.

Note: This section was initially named *Parental Controls* but was renamed by Microsoft to *Family Safety* starting with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

18.9.31 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.

18.9.31.1 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.

18.9.31.2 (L1) Ensure 'Turn off Data Execution Prevention for Explorer' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

```
HKEY_LOCAL_MACHINE\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.)

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.		●	●

18.9.31.3 (L1) Ensure 'Turn off heap termination on corruption' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Explorer>NoHeapTerminationOnCorruption

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.)

18.9.31.4 (L1) Ensure 'Turn off shell protocol protected mode' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorerr:PreXPSP2ShellProtocolBehavior`

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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p><u>8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies</u></p> <p>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.</p>			

18.9.32 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).

18.9.33 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 Release 1703 Administrative Templates (or newer).

18.9.34 Game 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 `GameExplorer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.35 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 Release 1709 Administrative Templates (or newer).

18.9.36 HomeGroup

This section contains recommendations related to the HomeGroup feature, which is available in all workstations of Windows from Windows 7 through Windows 10 Release 1709. Microsoft removed it from Windows starting with Windows 10 Release 1803.

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).

18.9.36.1 (L1) Ensure 'Prevent the computer from joining a homegroup' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

By default, users can add their computer to a HomeGroup on a home network.

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

Note: The HomeGroup feature is available in all workstation releases of Windows from Windows 7 through Windows 10 Release 1709. Microsoft removed the feature completely starting with Windows 10 Release 1803. However, if your environment still contains **any** Windows 10 Release 1709 (or older) workstations, then this setting remains important to disable HomeGroup on those systems.

Rationale:

While resources on a domain-joined computer cannot be shared with a HomeGroup, information from the domain-joined computer can be leaked to other computers in the HomeGroup.

Impact:

A user on this computer will not be able to add this computer to a HomeGroup. This setting does not affect other network sharing features. Mobile users who access printers and other shared devices on their home networks will not be able to leverage the ease of use provided by HomeGroup functionality.

Audit:

Navigate to the UI 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\Policies\Microsoft\Windows\HomeGroup:DisableHomeGroup

Remediation:

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

Computer Configuration\Policies\Administrative Templates\Windows Components\HomeGroup\Prevent the computer from joining a homegroup

Note: This Group Policy path may not exist by default. It 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).

Default Value:

Disabled. (A user can add their computer to a HomeGroup. However, data on a domain-joined computer is not shared with the HomeGroup.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>		●	●

18.9.37 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 Release 21H2 Administrative Templates (or newer).

18.9.38 Import Video

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 `CaptureWizard.admx/adml` that is only included with the Microsoft Windows Vista and Windows Server 2008 (non-R2) Administrative Templates.

18.9.39 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 `IetRes.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](#).

18.9.40 Internet Information 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 `IIS.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.41 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).

18.9.41.1 (L2) Ensure 'Turn off location' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

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:

```
HKEY_LOCAL_MACHINE\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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

18.9.42 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).

18.9.43 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 Release 1511 Administrative Templates (or newer).

18.9.44 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 Release 1607 & Server 2016 Administrative Templates (or newer).

18.9.45 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 Release 1709 Administrative Templates (or newer).

18.9.45.1 (L2) Ensure 'Allow Message Service Cloud Sync' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

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 a high security environment, data should never be sent to any 3rd party since this data could 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:

```
HKEY_LOCAL_MACHINE\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 Release 1709 Administrative Templates (or newer).

Default Value:

Enabled. (Cellular text messages can be backed up and restored to Microsoft's cloud services.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.9.46 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 Release 1703 Administrative Templates (or newer).

18.9.46.1 (L1) Ensure 'Block all consumer Microsoft account user authentication' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

HKEY_LOCAL_MACHINE\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 Release 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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.3 Disable Dormant Accounts Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.	●	●	●
v7	16.8 Disable Any Unassociated Accounts Disable any account that cannot be associated with a business process or business owner.	●	●	●

18.9.47 Microsoft Defender Antivirus (formerly Windows Defender and Windows Defender Antivirus)

This section contains recommendations related to Microsoft Defender Antivirus.

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: This section was originally named *Windows Defender* but was renamed by Microsoft to *Windows Defender Antivirus* starting with the Microsoft Windows 10 Release 1703 Administrative Templates. It was renamed (again) to *Microsoft Defender Antivirus* starting with the Microsoft Windows 10 Release 2004 Administrative Templates.

18.9.47.1 Client 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 `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.9.47.2 Device Control

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 the Microsoft Windows 11 Release 21H2 Administrative Templates (or newer).

18.9.47.3 Exclusions

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 the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.9.47.4 MAPS

This section contains recommendations related to Microsoft Active Protection Service (MAPS).

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.9.47.4.1 (L1) Ensure 'Configure local setting override for reporting to Microsoft MAPS' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting configures a local override for the configuration to join Microsoft Active Protection Service (MAPS), which Microsoft renamed to *Windows Defender Antivirus Cloud Protection Service* and then *Microsoft Defender Antivirus Cloud Protection Service*. This setting can only be set by Group Policy.

The recommended state for this setting is: Disabled.

Rationale:

The decision on whether or not to participate in Microsoft MAPS / Microsoft Defender Antivirus Cloud Protection Service for malicious software reporting should be made centrally in an enterprise managed environment, so that all computers within it behave consistently in that regard. Configuring this setting to Disabled ensures that the decision remains centrally managed.

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:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows
Defender\Spynet:LocalSettingOverrideSpynetReporting

Remediation:

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

Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\MAPS\Configure local setting override for reporting to Microsoft MAPS

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Default Value:

Disabled. (Group Policy will take priority over the local preference setting.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>			

18.9.47.4.2 (L2) Ensure 'Join Microsoft MAPS' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This policy setting allows you to join Microsoft Active Protection Service (MAPS), which Microsoft renamed to *Windows Defender Antivirus Cloud Protection Service* and then *Microsoft Defender Antivirus Cloud Protection Service*. Microsoft MAPS / Microsoft Defender Antivirus Cloud Protection Service is the online community that helps you choose how to respond to potential threats. The community also helps stop the spread of new malicious software infections. You can choose to send basic or additional information about detected software. Additional information helps Microsoft create new definitions and help it to protect your computer.

Possible options are:

- (0x0) Disabled (default)
- (0x1) Basic membership
- (0x2) Advanced membership

Basic membership will send basic information to Microsoft about software that has been detected including where the software came from the actions that you apply or that are applied automatically and whether the actions were successful.

Advanced membership in addition to basic information will send more information to Microsoft about malicious software spyware and potentially unwanted software including the location of the software file names how the software operates and how it has impacted your computer.

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

Rationale:

The information that would be sent can include things like location of detected items on your computer if harmful software was removed. The information would be automatically collected and sent. In some instances personal information might unintentionally be sent to Microsoft. However, Microsoft states that it will not use this information to identify you or contact you.

For privacy reasons in high security environments, it is best to prevent these data submissions altogether.

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 in effect when the following registry value does not exist, or when it exists with a value of 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows  
Defender\Spynet:SpynetReporting
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows  
Components\Microsoft Defender Antivirus\MAPS\Join Microsoft MAPS
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Default Value:

Disabled. (Microsoft MAPS / Microsoft Defender Antivirus Cloud Protection Service will not be joined.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>			

18.9.47.5 Microsoft Defender Exploit Guard (formerly Windows Defender Exploit Guard)

This section contains Microsoft Defender Exploit Guard settings.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 10 Release 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 Release 2004 Administrative Templates.

18.9.47.5.1 Attack Surface Reduction

This section contains Attack Surface Reduction settings.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.9.47.5.1.1 (L1) Ensure 'Configure Attack Surface Reduction rules' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls the state for the Attack Surface Reduction (ASR) rules.

The recommended state for this setting is: Enabled.

Rationale:

Attack surface reduction helps prevent actions and apps that are typically used by exploit-seeking malware to infect machines.

Impact:

When a rule is triggered, a notification will be displayed from the Action Center.

Audit:

Navigate to the UI 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\ Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR:ExploitGuard_ASRule

Remediation:

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

Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Microsoft Defender Exploit Guard\Attack Surface Reduction\Configure Attack Surface Reduction rules

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template WindowsDefender.admx/adml that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

Default Value:

Disabled. (No ASR rules will be configured.)

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.		●	●

18.9.47.5.1.2 (L1) Ensure 'Configure Attack Surface Reduction rules: Set the state for each ASR rule' is configured (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting sets the Attack Surface Reduction rules.

The recommended state for this setting is:

26190899-1602-49e8-8b27-eb1d0a1ce869 - 1 (Block Office communication application from creating child processes)

3b576869-a4ec-4529-8536-b80a7769e899 - 1 (Block Office applications from creating executable content)

5beb7efe-fd9a-4556-801d-275e5ffc04cc - 1 (Block execution of potentially obfuscated scripts)

75668c1f-73b5-4cf0-bb93-3ecf5cb7cc84 - 1 (Block Office applications from injecting code into other processes)

7674ba52-37eb-4a4f-a9a1-f0f9a1619a2c - 1 (Block Adobe Reader from creating child processes)

92e97fa1-2edf-4476-bdd6-9dd0b4dddc7b - 1 (Block Win32 API calls from Office macro)

9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2 - 1 (Block credential stealing from the

Windows local security authority subsystem (lsass.exe))

b2b3f03d-6a65-4f7b-a9c7-1c7ef74a9ba4 - 1 (Block untrusted and unsigned processes that run from USB)

be9ba2d9-53ea-4cdc-84e5-9b1eeee46550 - 1 (Block executable content from email client and webmail)

d3e037e1-3eb8-44c8-a917-57927947596d - 1 (Block JavaScript or VBScript from launching downloaded executable content)

d4f940ab-401b-4efc-aadc-ad5f3c50688a - 1 (Block Office applications from creating child processes)

e6db77e5-3df2-4cf1-b95a-636979351e5b - 1 (Block persistence through WMI event subscription)

Note: More information on ASR rules can be found at the following link: [Use Attack surface reduction rules to prevent malware infection | Microsoft Docs](#)

Rationale:

Attack surface reduction helps prevent actions and apps that are typically used by exploit-seeking malware to infect machines.

Impact:

When a rule is triggered, a notification will be displayed from the Action Center.

Audit:

Navigate to the UI 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\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules:26190899-1602-49e8-8b27-eb1d0a1ce869  
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules:3b576869-a4ec-4529-8536-b80a7769e899  
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules:5beb7efe-fd9a-4556-801d-275e5ffc04cc  
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules:75668c1f-73b5-4cf0-bb93-3ecf5cb7cc84  
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules:7674ba52-37eb-4a4f-a9a1-f0f9a1619a2c  
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules:92e97fa1-2edf-4476-bdd6-9dd0b4dddc7b  
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules:9e6c4e1f-7d60-472f-bala-a39ef669e4b2  
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules:b2b3f03d-6a65-4f7b-a9c7-1c7ef74a9ba4  
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules:be9ba2d9-53ea-4cdc-84e5-9bleeee46550  
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules:d3e037e1-3eb8-44c8-a917-57927947596d  
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules:d4f940ab-401b-4efc-aadc-ad5f3c50688a  
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules:e6db77e5-3df2-4cf1-b95a-636979351e5b
```

Remediation:

To establish the recommended configuration via GP, set the following UI path so that

26190899-1602-49e8-8b27-eb1d0a1ce869, 3b576869-a4ec-4529-8536-b80a7769e899,
5beb7efe-fd9a-4556-801d-275e5ffc04cc, 75668c1f-73b5-4cf0-bb93-3ecf5cb7cc84,
7674ba52-37eb-4a4f-a9a1-f0f9a1619a2c, 92e97fa1-2edf-4476-bdd6-9dd0b4dddc7b,
9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2, b2b3f03d-6a65-4f7b-a9c7-1c7ef74a9ba4,
be9ba2d9-53ea-4cdc-84e5-9b1eeee46550, d3e037e1-3eb8-44c8-a917-57927947596d,
d4f940ab-401b-4efc-aadc-ad5f3c50688a, and e6db77e5-3df2-4cf1-b95a-636979351e5b
are each set to a value of 1:

Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Microsoft Defender Exploit Guard\Attack Surface Reduction\Configure Attack Surface Reduction rules: Set the state for each ASR rule

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template WindowsDefender.admx/adml that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

Default Value:

Disabled. (No ASR rules will be configured.)

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.		●	●

18.9.47.5.2 Controlled Folder 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 `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.9.47.5.3 Network Protection

This section contains Windows Network Protection settings.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

18.9.47.5.3.1 (L1) Ensure 'Prevent users and apps from accessing dangerous websites' is set to 'Enabled: Block' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls Microsoft Defender Exploit Guard network protection.

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

Rationale:

This setting can help prevent employees from using any application to access dangerous domains that may host phishing scams, exploit-hosting sites, and other malicious content on the Internet.

Impact:

Users and applications will not be able to access dangerous domains.

Audit:

Navigate to the UI 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\Policies\Microsoft\windows Defender\Windows  
Defender Exploit Guard\Network Protection:EnableNetworkProtection
```

Remediation:

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

Block:

Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender Antivirus\Windows Defender Exploit Guard\Network Protection\Prevent users and apps from accessing dangerous websites

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template WindowsDefender.admx/adml that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

Default Value:

Disabled. (Users and applications will not be blocked from connecting to dangerous domains.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.3 Maintain and Enforce Network-Based URL Filters Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.		●	●
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	7.4 Maintain and Enforce Network-Based URL Filters Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.		●	●
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.		●	●

18.9.47.6 MpEngine

This section contains recommendations for MpEngine.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 10 Release 1703 Administrative Templates (or newer).

18.9.47.6.1 (L2) Ensure 'Enable file hash computation feature' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This setting determines whether hash values are computed for files scanned by Microsoft Defender.

The recommended state for this setting is: Enabled.

Rationale:

When running an antivirus solution such as Microsoft Defender Antivirus, it is important to ensure that it is configured to monitor for suspicious and known malicious activity. File hashes are a reliable way of detecting changes to files, and can speed up the scan process by skipping files that have not changed since they were last scanned and determined to be safe. A changed file hash can also be cause for additional scrutiny.

Impact:

This setting could cause performance degradation during initial deployment and for users where new executable content is frequently being created (such as software developers), or where applications are frequently installed or updated.

For more information on this setting, please visit [Security baseline \(FINAL\): Windows 10 and Windows Server, version 2004 - Microsoft Tech Community - 1543631](#).

Note: The impact of this setting should be monitored closely during deployment to ensure user and system performance impact is within acceptable limits.

Audit:

Navigate to the UI 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\ Policies\Microsoft\Windows
Defender\ MpEngine:EnableFileHashComputation

Remediation:

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

Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\ MpEngine\Enable file hash computation feature

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template WindowsDefender.admx/adml that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

Default Value:

Disabled. (File hash values are not computed during scans.)

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.		●	●

18.9.47.7 Network Inspection 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 `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.9.47.8 Quarantine

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 the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.9.47.9 Real-time Protection

This section contains settings related to Real-time Protection.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.9.47.9.1 (L1) Ensure 'Scan all downloaded files and attachments' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting configures scanning for all downloaded files and attachments.

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

Rationale:

When running an antivirus solution such as Microsoft Defender Antivirus, it is important to ensure that it is configured to heuristically monitor in real-time for suspicious and known malicious 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. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection:DisableIOAVProtection
```

Remediation:

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

Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Real-Time Protection\Scan all downloaded files and attachments

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template WindowsDefender.admx/adml that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Default Value:

Enabled. (All downloaded files and attachments will be scanned.)

References:

1. <https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-antivirus/configure-real-time-protection-microsoft-defender-antivirus>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<u>8.1 Utilize Centrally Managed Anti-malware Software</u> Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.		●	●

18.9.47.9.2 (L1) Ensure 'Turn off real-time protection' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting configures real-time protection prompts for known malware detection.

Microsoft Defender Antivirus alerts you when malware or potentially unwanted software attempts to install itself or to run on your computer.

The recommended state for this setting is: Disabled.

Rationale:

When running an antivirus solution such as Microsoft Defender Antivirus, it is important to ensure that it is configured to heuristically monitor in real-time for suspicious and known malicious 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. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection:DisableRealtimeMonitoring
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Real-Time Protection\Turn off real-time protection
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Default Value:

Disabled. (Microsoft Defender Antivirus will prompt users to take actions on malware detections.)

References:

1. <https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-antivirus/configure-real-time-protection-microsoft-defender-antivirus>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
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.		●	●

18.9.47.9.3 (L1) Ensure 'Turn on behavior monitoring' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting allows you to configure behavior monitoring for Microsoft Defender Antivirus.

The recommended state for this setting is: Enabled.

Rationale:

When running an antivirus solution such as Microsoft Defender Antivirus, it is important to ensure that it is configured to heuristically monitor in real-time for suspicious and known malicious 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. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection:DisableBehaviorMonitoring
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Real-Time Protection\Turn on behavior monitoring
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Default Value:

Enabled. (Behavior monitoring will be enabled.)

References:

1. <https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-antivirus/configure-real-time-protection-microsoft-defender-antivirus>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.7 Use Behavior-Based Anti-Malware Software Use behavior-based anti-malware software.	●	●	
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.	●	●	

18.9.47.9.4 (L1) Ensure 'Turn on script scanning' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting allows script scanning to be turned on/off. Script scanning intercepts scripts then scans them before they are executed on the system.

The recommended state for this setting is: Enabled.

Rationale:

When running an antivirus solution such as Microsoft Defender Antivirus, it is important to ensure that it is configured to heuristically monitor in real-time for suspicious and known malicious 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. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection:DisableScriptScanning
```

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Real-Time Protection\Turn on script scanning
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 10 Release 21H2 Administrative Templates (or newer).

Default Value:

Enabled. (Script scanning will be enabled.)

References:

1. <https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-advanced-scan-types-microsoft-defender-antivirus?view=o365-worldwide>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.7 Use Behavior-Based Anti-Malware Software Use behavior-based anti-malware software.		●	●
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.		●	●

18.9.47.10 Remediation

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 the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.9.47.11 Reporting

This section contains settings related to Microsoft Defender Reporting.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.9.47.11.1 (L2) Ensure 'Configure Watson events' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This policy setting allows you to configure whether or not Watson events are sent.

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

Rationale:

Watson events are the reports that get sent to Microsoft when a program or service crashes or fails, including the possibility of automatic submission. Preventing this information from being sent can help reduce privacy concerns.

Impact:

Watson events will not be sent to Microsoft automatically when a program or service crashes or fails.

Audit:

Navigate to the UI 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\Policies\Microsoft\Windows  
Defender\Reporting:DisableGenericRePorts
```

Remediation:

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

Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Reporting\Configure Watson events

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Default Value:

Enabled. (Watson events *will* be sent to Microsoft automatically when a program or service crashes or fails.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
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.			●

18.9.47.12 Scan

This section contains settings related to Microsoft Defender scanning.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.9.47.12.1 (L1) Ensure 'Scan removable drives' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting allows you to manage whether or not to scan for malicious software and unwanted software in the contents of removable drives, such as USB flash drives, when running a full scan.

The recommended state for this setting is: Enabled.

Rationale:

It is important to ensure that any present removable drives are always included in any type of scan, as removable drives are more likely to contain malicious software brought in to the enterprise managed environment from an external, unmanaged computer.

Impact:

Removable drives will be scanned during any type of scan by Microsoft Defender Antivirus.

Audit:

Navigate to the UI 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\Policies\Microsoft\Windows Defender\Scan:DisableRemovableDriveScanning

Remediation:

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

Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Scan\Scan removable drives

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template WindowsDefender.admx/adml that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Default Value:

Disabled. (Removable drives will not be scanned during a full scan. Removable drives may still be scanned during quick scan and custom scan.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>10.4 Configure Automatic Anti-Malware Scanning of Removable Media</p> <p>Configure anti-malware software to automatically scan removable media.</p>		●	●
v7	<p>8.4 Configure Anti-Malware Scanning of Removable Devices</p> <p>Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected.</p>	●	●	●

18.9.47.12.2 (L1) Ensure 'Turn on e-mail scanning' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting allows you to configure e-mail scanning. When e-mail scanning is enabled, the engine will parse the mailbox and mail files, according to their specific format, in order to analyze the mail bodies and attachments. Several e-mail formats are currently supported, for example: pst (Outlook), dbx, mbx, mime (Outlook Express), binhex (Mac).

The recommended state for this setting is: Enabled.

Rationale:

Incoming e-mails should be scanned by an antivirus solution such as Microsoft Defender Antivirus, as email attachments are a commonly used attack vector to infiltrate computers with malicious software.

Impact:

E-mail scanning by Microsoft Defender Antivirus will 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:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows
Defender\Scan:DisableEmailScanning

Remediation:

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

Computer Configuration\Policies\Administrative Templates\Windows
Components\Microsoft Defender Antivirus\Scan\Turn on e-mail scanning

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template WindowsDefender.admx/adml that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Default Value:

Disabled. (E-mail scanning by Microsoft Defender Antivirus will be disabled.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
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.	●	●	●

18.9.47.13 Security Intelligence Updates (formerly Signature Updates)

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 the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Note: This section was initially named *Signature Updates* but was renamed by Microsoft to *Security Intelligence Updates* starting with the Microsoft Windows 10 Release 1903 Administrative Templates.

18.9.47.14 Threats

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 the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.9.47.15 (L1) Ensure 'Configure detection for potentially unwanted applications' is set to 'Enabled: Block' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls detection and action for Potentially Unwanted Applications (PUA), which are sneaky unwanted application bundlers or their bundled applications, that can deliver adware or malware.

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

For more information, see this link: [Block potentially unwanted applications with Microsoft Defender Antivirus | Microsoft Docs](#)

Rationale:

Potentially unwanted applications can increase the risk of your network being infected with malware, cause malware infections to be harder to identify, and can waste IT resources in cleaning up the applications. They should be blocked from installation.

Impact:

Applications that are identified by Microsoft as PUA will be blocked at download and install time.

Audit:

Navigate to the UI 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\Policies\Microsoft\Windows_Defender:PUAProtection

Remediation:

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

Block:

Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Configure detection for potentially unwanted applications

Note: This Group Policy path is provided by the Group Policy template WindowsDefender.admx/adml that is included with the Microsoft Windows 10 Release 1809 & Server 2019 Administrative Templates (or newer).

Default Value:

Disabled. (Applications that are identified by Microsoft as PUA will not be blocked.)

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.		●	●
v8	10.6 Centrally Manage Anti-Malware Software Centrally manage anti-malware software.		●	●
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.			●
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.		●	●

18.9.47.16 (L1) Ensure 'Turn off Microsoft Defender AntiVirus' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting turns off Microsoft Defender Antivirus. If the setting is configured to Disabled, Microsoft Defender Antivirus runs and computers are scanned for malware and other potentially unwanted software.

The recommended state for this setting is: Disabled.

Rationale:

It is important to ensure a current, updated antivirus product is scanning each computer for malicious file activity. Microsoft provides a competent solution out of the box in Microsoft Defender Antivirus.

Organizations that choose to purchase a reputable 3rd-party antivirus solution may choose to exempt themselves from this recommendation in lieu of the commercial alternative.

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:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows
Defender:DisableAntiSpyware

Remediation:

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

Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Turn off Microsoft Defender AntiVirus

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.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 *Turn off Windows Defender*, but it was renamed to *Windows Defender Antivirus* starting with the Windows 10 Release 1703 Administrative Templates. It was again renamed to *Turn off Microsoft Defender Antivirus* starting with the Windows 10 Release 2004 Administrative Templates.

Default Value:

Disabled. (Microsoft Defender Antivirus runs and computers are scanned for malware and other potentially unwanted software.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.6 Centrally Manage Anti-Malware Software Centrally manage anti-malware software.	●	●	●
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.	●	●	●

18.9.48 Microsoft Defender Application Guard (formerly Windows Defender Application Guard)

This section contains settings related to Microsoft Defender Application Guard.

This Group Policy section is provided by the Group Policy template `AppHVSI.admx/adml` that is included with the Microsoft Windows 10 Release 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 Release 2004 Administrative Templates.

18.9.48.1 (NG) Ensure 'Allow auditing events in Microsoft Defender Application Guard' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) + Next Generation Windows Security (NG)
- Level 1 (L1) + BitLocker (BL) + Next Generation Windows Security (NG)
- Level 2 (L2) + Next Generation Windows Security (NG)
- Level 2 (L2) + BitLocker (BL) + Next Generation Windows Security (NG)
- Next Generation Windows Security (NG) - optional add-on for use in the newest hardware and configuration environments

Description:

This policy setting allows you to decide whether auditing events can be collected from Microsoft Defender Application Guard.

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

Note: Microsoft Defender Application Guard requires a 64-bit version of Windows and a CPU supporting hardware-assisted CPU virtualization (Intel VT-x or AMD-V). This feature is not officially supported on virtual hardware, although it can work on VMs (especially for testing) provided that the hardware-assisted CPU virtualization feature is exposed by the host to the guest VM.

More information on system requirements for this feature can be found at [System requirements for Microsoft Defender Application Guard \(Windows 10\) | Microsoft Docs](#)

Note #2: Credential Guard and Device Guard are not currently supported when using Azure IaaS VMs.

Rationale:

Auditing of Microsoft Defender Application Guard events may be useful when investigating a security incident.

Impact:

Microsoft Defender Application Guard will inherit its auditing policies from Microsoft Edge and start to audit system events specifically for Microsoft Defender Application Guard. Collected logs are available for review on Microsoft Edge, outside of Application Guard.

Audit:

Navigate to the UI 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\Policies\Microsoft\AppHVSI:AuditApplicationGuard

Remediation:

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

Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Application Guard\Allow auditing events in Microsoft Defender Application Guard

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template AppHVSI.admx/adml that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Allow auditing events in Windows Defender Application Guard*, but it was renamed to *Allow auditing events in Microsoft Defender Application Guard* starting with the Windows 10 Release 2004 Administrative Templates.

Default Value:

Disabled. (Audit event logs aren't collected for Microsoft Defender Application Guard.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

18.9.48.2 (NG) Ensure 'Allow camera and microphone access in Microsoft Defender Application Guard' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) + Next Generation Windows Security (NG)
- Level 1 (L1) + BitLocker (BL) + Next Generation Windows Security (NG)
- Level 2 (L2) + Next Generation Windows Security (NG)
- Level 2 (L2) + BitLocker (BL) + Next Generation Windows Security (NG)
- Next Generation Windows Security (NG) - optional add-on for use in the newest hardware and configuration environments

Description:

The policy allows you to determine whether applications inside Microsoft Defender Application Guard can access the device's camera and microphone.

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

Note: Microsoft Defender Application Guard requires a 64-bit version of Windows and a CPU supporting hardware-assisted CPU virtualization (Intel VT-x or AMD-V). This feature is not officially supported on virtual hardware, although it can work on VMs (especially for testing) provided that the hardware-assisted CPU virtualization feature is exposed by the host to the guest VM.

More information on system requirements for this feature can be found at [System requirements for Microsoft Defender Application Guard \(Windows 10\) | Microsoft Docs](#)

Note #2: Credential Guard and Device Guard are not currently supported when using Azure IaaS VMs.

Rationale:

In effort to stop sensitive information from being obtained for malicious use, untrusted sites within the Microsoft Defender Application Guard container should not be accessing the computers microphone or camera.

Impact:

This is the default value so impact should be minimal to enforce 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:

HKEY_LOCAL_MACHINE\SOFTWARE\ Policies\Microsoft\AppHVSI:AllowCameraMicrophoneRedirection

Remediation:

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

Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Application Guard\Allow camera and microphone access in Microsoft Defender Application Guard

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `AppHVSI.admx/adml` that is included with the Microsoft Windows 10 Release 1809 & Server 2019 Administrative Templates (or newer).

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Allow camera and microphone access in Windows Defender Application Guard*, but it was renamed to *Allow camera and microphone access in Microsoft Defender Application Guard* starting with the Windows 10 Release 2004 Administrative Templates.

Default Value:

Disabled. (Applications inside Microsoft Defender Application Guard will be unable to access the camera and microphone on the user's device.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.9.48.3 (NG) Ensure 'Allow data persistence for Microsoft Defender Application Guard' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) + Next Generation Windows Security (NG)
- Level 1 (L1) + BitLocker (BL) + Next Generation Windows Security (NG)
- Level 2 (L2) + Next Generation Windows Security (NG)
- Level 2 (L2) + BitLocker (BL) + Next Generation Windows Security (NG)
- Next Generation Windows Security (NG) - optional add-on for use in the newest hardware and configuration environments

Description:

This policy setting allows you to decide whether data should persist across different sessions in Microsoft Defender Application Guard.

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

Note: Microsoft Defender Application Guard requires a 64-bit version of Windows and a CPU supporting hardware-assisted CPU virtualization (Intel VT-x or AMD-V). This feature is not officially supported on virtual hardware, although it can work on VMs (especially for testing) provided that the hardware-assisted CPU virtualization feature is exposed by the host to the guest VM.

More information on system requirements for this feature can be found at [System requirements for Microsoft Defender Application Guard \(Windows 10\) | Microsoft Docs](#)

Note #2: Credential Guard and Device Guard are not currently supported when using Azure IaaS VMs.

Rationale:

The primary purpose of Microsoft Defender Application Guard is to present a "sandboxed container" for visiting untrusted websites. If data persistence is allowed, then it reduces the effectiveness of the sandboxing, and malicious content will be able to remain active in the Microsoft Defender Application Guard container between sessions.

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:

HKEY_LOCAL_MACHINE\SOFTWARE\ Policies\Microsoft\AppHVSI:AllowPersistence

Remediation:

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

Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Application Guard\Allow data persistence for Microsoft Defender Application Guard

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `AppHVSI.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Allow data persistence for Windows Defender Application Guard*, but it was renamed to *Allow data persistence for Microsoft Defender Application Guard* starting with the Windows 10 Release 2004 Administrative Templates.

Default Value:

`Disabled`. (Microsoft Defender Application Guard deletes all user data within the Microsoft Defender Application Guard container.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 <u>Enable Anti-Exploitation Features</u> 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 <u>Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies</u> 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.		●	●

18.9.48.4 (NG) Ensure 'Allow files to download and save to the host operating system from Microsoft Defender Application Guard' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) + Next Generation Windows Security (NG)
- Level 1 (L1) + BitLocker (BL) + Next Generation Windows Security (NG)
- Level 2 (L2) + Next Generation Windows Security (NG)
- Level 2 (L2) + BitLocker (BL) + Next Generation Windows Security (NG)
- Next Generation Windows Security (NG) - optional add-on for use in the newest hardware and configuration environments

Description:

This policy setting determines whether to save downloaded files to the host operating system from the Microsoft Defender Application Guard container.

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

Note: Microsoft Defender Application Guard requires a 64-bit version of Windows and a CPU supporting hardware-assisted CPU virtualization (Intel VT-x or AMD-V). This feature is not officially supported on virtual hardware, although it can work on VMs (especially for testing) provided that the hardware-assisted CPU virtualization feature is exposed by the host to the guest VM.

More information on system requirements for this feature can be found at [System requirements for Microsoft Defender Application Guard \(Windows 10\) | Microsoft Docs](#)

Note #2: Credential Guard and Device Guard are not currently supported when using Azure IaaS VMs.

Rationale:

The primary purpose of Microsoft Defender Application Guard is to present a "sandboxed container". Potentially malicious files should not be copied to the host OS from the sandboxed environment, which could put the host at 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:

HKEY_LOCAL_MACHINE\SOFTWARE\ Policies\Microsoft\AppHVSI:SaveFilesToHost

Remediation:

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

Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Application Guard\Allow files to download and save to the host operating system from Microsoft Defender Application Guard

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `AppHVSI.admx/adml` that is included with the Microsoft Windows 10 Release 1803 Administrative Templates (or newer).

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Allow files to download and save to the host operating system from Windows Defender Application Guard*, but it was renamed to *Allow files to download and save to the host operating system from Microsoft Defender Application Guard* starting with the Windows 10 Release 2004 Administrative Templates.

Default Value:

Disabled. (Users can't save downloaded files from the Microsoft Defender Application Guard container to the host operating system.)

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.		●	●

18.9.48.5 (NG) Ensure 'Configure Microsoft Defender Application Guard clipboard settings: Clipboard behavior setting' is set to 'Enabled: Enable clipboard operation from an isolated session to the host' (Automated)

Profile Applicability:

- Level 1 (L1) + Next Generation Windows Security (NG)
- Level 1 (L1) + BitLocker (BL) + Next Generation Windows Security (NG)
- Level 2 (L2) + Next Generation Windows Security (NG)
- Level 2 (L2) + BitLocker (BL) + Next Generation Windows Security (NG)
- Next Generation Windows Security (NG) - optional add-on for use in the newest hardware and configuration environments

Description:

This policy setting allows you to decide how the clipboard behaves while in Microsoft Defender Application Guard.

The recommended state for this setting is: Enabled: Enable clipboard operation from an isolated session to the host.

Note: Microsoft Defender Application Guard requires a 64-bit version of Windows and a CPU supporting hardware-assisted CPU virtualization (Intel VT-x or AMD-V). This feature is not officially supported on virtual hardware, although it can work on VMs (especially for testing) provided that the hardware-assisted CPU virtualization feature is exposed by the host to the guest VM.

More information on system requirements for this feature can be found at [System requirements for Microsoft Defender Application Guard \(Windows 10\) | Microsoft Docs](#)

Note #2: Credential Guard and Device Guard are not currently supported when using Azure IaaS VMs.

Rationale:

The primary purpose of Microsoft Defender Application Guard is to present a "sandboxed container" for visiting untrusted websites. If the host clipboard is made available to Microsoft Defender Application Guard, a compromised Microsoft Defender Application Guard session will have access to its content, potentially exposing sensitive information to a malicious website or application. However, the risk is reduced if the Microsoft Defender Application Guard clipboard is made accessible to the host, and indeed that functionality may often be necessary from an operational standpoint.

Impact:

Microsoft Defender Application Guard sessions will not be able to access the host device's clipboard, however the host device **will** be able to access the Microsoft Defender Application Guard session clipboard.

Audit:

Navigate to the UI 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\Policies\Microsoft\AppHVSIClipboardSettings

Remediation:

To establish the recommended configuration via GP, set the following UI path to **Enabled**:
Enable clipboard operation from an isolated session to the host

Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Application Guard\Configure Microsoft Defender Application Guard clipboard settings: Clipboard behavior setting

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `AppHVSIC.admx/adml` that is included with the Microsoft Windows 10 Release 1703 Administrative Templates (or newer).

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Configure Windows Defender Application Guard clipboard settings: Clipboard behavior setting*, but it was renamed to *Configure Microsoft Defender Application Guard clipboard settings: Clipboard behavior setting* starting with the Windows 10 Release 2004 Administrative Templates.

Default Value:

Disabled. (All clipboard functionality is turned off in Microsoft Defender Application Guard.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 <u>Enable Anti-Exploitation Features</u> 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 <u>Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies</u> 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.		●	●

18.9.48.6 (NG) Ensure 'Turn on Microsoft Defender Application Guard in Managed Mode' is set to 'Enabled: 1' (Automated)

Profile Applicability:

- Level 1 (L1) + Next Generation Windows Security (NG)
- Level 1 (L1) + BitLocker (BL) + Next Generation Windows Security (NG)
- Level 2 (L2) + Next Generation Windows Security (NG)
- Level 2 (L2) + BitLocker (BL) + Next Generation Windows Security (NG)
- Next Generation Windows Security (NG) - optional add-on for use in the newest hardware and configuration environments

Description:

This policy setting enables application isolation through Microsoft Defender Application Guard (Application Guard).

There are 4 options available:

- 0. Disable Microsoft Defender Application Guard
- 1. Enable Microsoft Defender Application Guard for Microsoft Edge ONLY
- 2. Enable Microsoft Defender Application Guard for Microsoft Office ONLY
- 3. Enable Microsoft Defender Application Guard for Microsoft Edge AND Microsoft Office

The recommended state for this setting is: `Enabled: 1` (Enable Microsoft Defender Application Guard for Microsoft Edge ONLY).

Note: Microsoft Defender Application Guard requires a 64-bit version of Windows and a CPU supporting hardware-assisted CPU virtualization (Intel VT-x or AMD-V). This feature is not officially supported on virtual hardware, although it can work on VMs (especially for testing) provided that the hardware-assisted CPU virtualization feature is exposed by the host to the guest VM.

More information on system requirements for this feature can be found at [System requirements for Microsoft Defender Application Guard \(Windows 10\) | Microsoft Docs](#)

Note #2: At time of publication, Microsoft Defender Application Guard in all currently released versions of Windows 10 does not yet support protection for Microsoft Office, only for Microsoft Edge. Therefore the additional available options of 2 and 3 in this setting are not yet valid.

Note #3: Credential Guard and Device Guard are not currently supported when using Azure IaaS VMs.

Rationale:

Microsoft Defender Application Guard uses Windows Hypervisor to create a virtualized environment for apps that are configured to use virtualization-based security isolation. While in isolation, improper user interactions and app vulnerabilities can't compromise the kernel or any other apps running outside of the virtualized environment.

Impact:

Microsoft Defender Application Guard will be turned on for Microsoft Edge.

Note: Microsoft Defender Application Guard requires the *Internet Connection Sharing (ICS) (SharedAccess)* service in order to operate, so an exception to disabling this service (see Section 5) will be required if choosing to enable Microsoft Defender Application Guard.

Audit:

Navigate to the UI 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\Policies\Microsoft\AppHVSI:AllowAppHVSI_Providerset
```

Remediation:

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

1:

Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Application Guard\Turn on Microsoft Defender Application Guard in Managed Mode

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `AppHVSI.admx/adml` that is included with the Microsoft Windows 10 Release 1703 Administrative Templates (or newer).

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Turn on Windows Defender Application Guard in Enterprise Mode*, but it was renamed to *Turn on Windows Defender Application Guard in Managed Mode* starting with the Windows 10 Release 1903 Administrative Templates. It was again renamed to *Turn on Microsoft Defender Application Guard in Managed Mode* starting with the Windows 10 Release 2004 Administrative Templates.

Default Value:

Disabled. (Microsoft Defender Application Guard is turned off.)

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.	●	●	●

18.9.49 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 Release 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 Release 2004 Administrative Templates.

18.9.50 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 (Release 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](#).

18.9.51 Microsoft FIDO 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 `FidoAuth.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

18.9.52 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 Release 1607 & Server 2016 Administrative Templates (or newer).

18.9.53 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 Release 1607 & Server 2016 Administrative Templates (or newer).

18.9.54 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.

18.9.55 Network Access 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 `NAPXPQec.admx/adml` that is only included with the Microsoft Windows Server 2008 (non-R2) through the Windows 8.1 Update & Server 2012 R2 Update Administrative Templates.

18.9.56 Network Projector

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 `NetworkProjection.admx/adml` that is only included with the Microsoft Windows Vista through the Windows 8.1 Update & Server 2012 R2 Update Administrative Templates.

18.9.57 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 Release 21H1 Administrative Templates (or newer).

18.9.57.1 (L2) Ensure 'Enable news and interests on the taskbar' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This policy setting specifies whether the *news and interests* feature is allowed on the device.

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

Rationale:

Due to privacy concerns, apps and features such as *news and interests* on the Windows taskbar should be treated as a possible security risk due to the potential of data being sent back to 3rd parties, such as Microsoft.

In addition, the app may display inappropriate *news and interests* within the feed.

Impact:

The *news and interests* feature on the Windows taskbar will not be available on the device.

Note: At time of benchmark publication, this setting does not hide or disable the taskbar menu options for the *news and interests* feature, however attempting to turn the feature back on does not cause any visible change. It is possible that Microsoft will modify this behavior to "gray out" the taskbar menu options in a future OS update.

Audit:

Navigate to the UI 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\Policies\Microsoft\Windows\Windows Feeds:EnableFeeds

Remediation:

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

Computer Configuration\Policies\Administrative Templates\Windows Components\News and interests\Enable news and interests on the taskbar

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `Feeds.admx/adml` that is included with the Microsoft Windows 10 Release 21H1 Administrative Templates (or newer).

Default Value:

Enabled. (The *news and interests* feature is available on the device.)

References:

1. <https://techcommunity.microsoft.com/t5/windows-it-pro-blog/group-configuration-news-and-interests-on-the-windows-taskbar/ba-p/2281005/page/2#comments>

18.9.58 OneDrive (formerly SkyDrive)

This section contains recommendations related to OneDrive.

The Group Policy settings contained within this section are provided by the Group Policy template `SkyDrive.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Note: This section was initially named *SkyDrive* but was renamed by Microsoft to *OneDrive* starting with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates.

18.9.58.1 (L1) Ensure 'Prevent the usage of OneDrive for file storage' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting lets you prevent apps and features from working with files on OneDrive using the Next Generation Sync Client.

The recommended state for this setting is: Enabled.

Rationale:

Enabling this setting prevents users from accidentally (or intentionally) uploading confidential or sensitive corporate information to the OneDrive cloud service using the Next Generation Sync Client.

Note: This security concern applies to *any* cloud-based file storage application installed on a workstation, not just the one supplied with Windows.

Impact:

Users can't access OneDrive from the OneDrive app and file picker. Windows Store apps can't access OneDrive using the `WinRT` API. OneDrive doesn't appear in the navigation pane in File Explorer. OneDrive files aren't kept in sync with the cloud. Users can't automatically upload photos and videos from the camera roll folder.

Note: If your organization uses Office 365, be aware that this setting will prevent users from saving files to OneDrive/SkyDrive.

Note #2: If your organization has decided to implement **OneDrive for Business** and therefore needs to except itself from this recommendation, we highly suggest that you also obtain and utilize the `OneDrive.admx/adml` template that is bundled with the latest OneDrive client, as noted [at this link](#) (this template is not included with the Windows Administrative Templates). Two alternative OneDrive settings in particular from that template are worth your consideration:

- *Allow syncing OneDrive accounts for only specific organizations* - a computer-based setting that restricts OneDrive client connections to only **approved** tenant IDs.
- *Prevent users from synchronizing personal OneDrive accounts* - a user-based setting that prevents use of consumer OneDrive (i.e. non-business).

Audit:

Navigate to the UI 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\Policies\Microsoft\Windows\OneDrive:DisableFileSyncNGSC
```

Remediation:

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

Computer Configuration\Policies\Administrative Templates\Windows Components\OneDrive\Prevent the usage of OneDrive for file storage

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `SkyDrive.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer). However, we strongly recommend you only use the version included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer). Older versions of the templates had conflicting settings in different template files for both OneDrive & SkyDrive, until it was cleaned up properly in the above version.

Note #2: In older Microsoft Windows Administrative Templates, this setting was named *Prevent the usage of SkyDrive for file storage*, but it was renamed starting with the Windows 10 RTM (Release 1507) Administrative Templates.

Default Value:

Disabled. (Apps and features can work with OneDrive file storage using the Next Generation Sync Client.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	13.4 <u>Only Allow Access to Authorized Cloud Storage or Email Providers</u> Only allow access to authorized cloud storage or email providers.		●	●

18.9.59 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.

18.9.60 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 Release 1809 and Server 2019 Administrative Templates (or newer).

18.9.61 Password Synchronization

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 `PswdSync.admx/adml` that is only included with the Microsoft Windows Vista through the Windows 8.1 Update & Server 2012 R2 Update Administrative Templates.

18.9.62 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).

18.9.63 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.

18.9.64 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 Release 1709 Administrative Templates (or newer).

18.9.64.1 (L2) Ensure 'Turn off Push To Install service' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

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:

```
HKEY_LOCAL_MACHINE\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 Release 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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.	●	●	●

18.9.65 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.

18.9.65.1 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.

18.9.65.2 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.

18.9.65.2.1 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).

18.9.65.2.2 (L1) Ensure 'Do not allow passwords to be saved' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

An attacker with physical access to the computer may be able to break the protection guarding saved passwords. An attacker 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:

HKEY_LOCAL_MACHINE\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.)

18.9.65.3 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.

18.9.65.3.1 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).

18.9.65.3.2 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.

18.9.65.3.2.1 (L2) Ensure 'Allow users to connect remotely by using Remote Desktop Services' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This policy setting allows you to configure remote access to computers by using Remote Desktop Services.

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

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 access to legitimate users who need to log on to the console of the computer, unauthorized users could download and execute malicious code to elevate their privileges.

Impact:

None - this is the default configuration, unless Remote Desktop Services has been manually enabled on the Remote tab in the System Properties sheet.

Audit:

Navigate to the UI 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\Policies\Microsoft\Windows NT\Terminal Services:fDenyTSConnections
--

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\Connections\Allow users to connect remotely by using Remote Desktop Services
```

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 initially named *Allow users to connect remotely using Terminal Services*, but it was renamed to *Allow users to connect remotely using Remote Desktop Services* in the Windows 7 & Server 2008 R2 Administrative Templates. It was finally renamed (again) to *Allow users to connect remotely by using Remote Desktop Services* starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

Default Value:

Disabled. (Users cannot connect remotely to the target computer by using Remote Desktop Services, unless it has been manually enabled from the Remote tab in the System Properties sheet.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.9.65.3.3 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.

18.9.65.3.3.1 (L2) Ensure 'Allow UI Automation redirection' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

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:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services:EnableUiAutomation
```

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 Release 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>

18.9.65.3.3.2 (L2) Ensure 'Do not allow COM port redirection' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

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:

HKEY_LOCAL_MACHINE\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/adm1 that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Remote Desktop Services allows COM port redirection.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>			

18.9.65.3.3.3 (L1) Ensure 'Do not allow drive redirection' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

HKEY_LOCAL_MACHINE\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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>			

18.9.65.3.3.4 (L2) Ensure 'Do not allow location redirection' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

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:

HKEY_LOCAL_MACHINE\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 Release 21H2 Administrative Templates (or newer).

Default Value:

Disabled. (Users can redirect their location data to the remote computer.)

18.9.65.3.3.5 (L2) Ensure 'Do not allow LPT port redirection' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

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:

HKEY_LOCAL_MACHINE\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/adm1 that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Disabled. (Remote Desktop Services allows LPT port redirection.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>			

18.9.65.3.3.6 (L2) Ensure 'Do not allow supported Plug and Play device redirection' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

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:

HKEY_LOCAL_MACHINE\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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>		●	●

18.9.65.3.4 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.

18.9.65.3.5 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.

18.9.65.3.6 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.

18.9.65.3.7 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.

18.9.65.3.8 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.

18.9.65.3.9 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.

18.9.65.3.9.1 (L1) Ensure 'Always prompt for password upon connection' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 an attacker 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:

HKEY_LOCAL_MACHINE\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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.9.65.3.9.2 (L1) Ensure 'Require secure RPC communication' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 expose 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:

HKEY_LOCAL_MACHINE\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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>			

18.9.65.3.9.3 (L1) Ensure 'Require use of specific security layer for remote (RDP) connections' is set to 'Enabled: SSL' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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) version 1.0, not the older (and less secure) SSL protocol.

Rationale:

The native Remote Desktop Protocol (RDP) encryption is now considered a weak protocol, so enforcing the use of stronger Transport Layer Security (TLS) encryption for all RDP communications between clients and RD Session Host servers is preferred.

Impact:

TLS 1.0 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 workstation 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:

HKEY_LOCAL_MACHINE\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:

Negotiate. (The most secure method that is supported by the client is enforced. If TLS is supported, it is used to authenticate the RD Session Host server. If TLS is not supported, native RDP encryption is used, but the RD Session Host server is not authenticated.)

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	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.			

18.9.65.3.9.4 (L1) Ensure 'Require user authentication for remote connections by using Network Level Authentication' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

HKEY_LOCAL_MACHINE\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:

Windows 7 and older: Disabled.

Windows 8.0 and newer: Enabled.

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	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.	●	●	

18.9.65.3.9.5 (L1) Ensure 'Set client connection encryption level' is set to 'Enabled: High Level' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 an attacker 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:

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.)

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	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.	●	●	●

18.9.65.3.10 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.

18.9.65.3.10.1 (L2) 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 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

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.

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.

Audit:

Navigate to the UI 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\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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

18.9.65.3.10.2 (L2) Ensure 'Set time limit for disconnected sessions' is set to 'Enabled: 1 minute' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This policy setting allows you to configure a time limit for disconnected Remote Desktop Services sessions.

The recommended state for this setting is: Enabled: 1 minute.

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 disconnected but still active 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. This setting is important to ensure a disconnected session is properly terminated.

Impact:

Disconnected Remote Desktop sessions are deleted from the server after 1 minute. Note that disconnected session time limits do not apply to console sessions.

Audit:

Navigate to the UI 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\Policies\Microsoft\Windows NT\Terminal Services:MaxDisconnectionTime
--

Remediation:

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

1 minute:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Session Time Limits\Set time limit for disconnected 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.

Default Value:

Disabled. (Disconnected Remote Desktop sessions are maintained for an unlimited time on the server.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

18.9.65.3.11 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.

18.9.65.3.11.1 (L1) Ensure 'Do not delete temp folders upon exit' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

```
HKEY_LOCAL_MACHINE\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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>			

18.9.66 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.

18.9.66.1 (L1) Ensure 'Prevent downloading of enclosures' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

```
HKEY_LOCAL_MACHINE\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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>9.4 Restrict Unnecessary or Unauthorized Browser and Email Client Extensions</p> <p>Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.</p>		●	●
v7	<p>7.2 Disable Unnecessary or Unauthorized Browser or Email Client Plugins</p> <p>Uninstall or disable any unauthorized browser or email client plugins or add-on applications.</p>		●	●

18.9.67 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.

18.9.67.1 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 Release 1511 Administrative Templates.

18.9.67.2 (L2) Ensure 'Allow Cloud Search' is set to 'Enabled: Disable Cloud Search' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

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:

Due to privacy concerns, data should never be sent to any 3rd party since this data could 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:

HKEY_LOCAL_MACHINE\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 Release 1709 Administrative Templates (or newer).

Default Value:

Enabled: Enable Cloud Search. (Allow search and Cortana to search cloud sources like OneDrive and SharePoint.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</p> <p>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.</p>		●	●
v7	<p>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>		●	●

18.9.67.3 (L1) Ensure 'Allow Cortana' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting specifies whether Cortana is allowed on the device.

The recommended state for this setting is: Disabled.

Rationale:

If Cortana is enabled, sensitive information could be contained in search history and sent out to Microsoft.

Impact:

Cortana will be turned off. Users will still be able to use search to find things on the device and on 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:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Windows
Search:AllowCortana

Remediation:

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

Computer Configuration\Policies\Administrative Templates\Windows
Components\Search\Allow Cortana

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 RTM (Release 1507) Administrative Templates (or newer).

Default Value:

Enabled. (Cortana will be allowed on the device.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>			

18.9.67.4 (L1) Ensure 'Allow Cortana above lock screen' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines whether or not the user can interact with Cortana using speech while the system is locked.

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

Rationale:

Access to any computer resource should not be allowed when the device is locked.

Impact:

The system will need to be unlocked for the user to interact with Cortana using speech.

Audit:

Navigate to the UI 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\Policies\Microsoft\Windows\Windows Search:AllowCortanaAboveLock`

Remediation:

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

`Computer Configuration\Policies\Administrative Templates\Windows Components\Search\Allow Cortana above lock screen`

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 Release 1607 & Server 2016 Administrative Templates (or newer).

Default Value:

`Enabled`. (The user can interact with Cortana using speech while the system is locked.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.			

18.9.67.5 (L1) Ensure 'Allow indexing of encrypted files' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

```
HKEY_LOCAL_MACHINE\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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
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.			●

18.9.67.6 (L1) Ensure 'Allow search and Cortana to use location' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting specifies whether search and Cortana can provide location aware search and Cortana results.

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

Rationale:

In an enterprise managed environment, allowing Cortana and Search to have access to location data is unnecessary. Organizations likely do not want this information shared out.

Impact:

Search and Cortana will not have access to location 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:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Windows  
Search:AllowSearchToUseLocation
```

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 and Cortana to use location
```

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 RTM (Release 1507) Administrative Templates (or newer).

Default Value:

Enabled. (Search and Cortana can access location information.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>			

18.9.68 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.

18.9.69 Server for NIS

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 `snis.admx/adml` that is only included with the Microsoft Windows Vista through the Windows 8.1 Update & Server 2012 R2 Update Administrative Templates.

18.9.70 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.

18.9.71 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.

18.9.72 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 (Release 1507) Administrative Templates (or newer).

18.9.72.1 (L2) Ensure 'Turn off KMS Client Online AVS Validation' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

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. Preventing this information from being sent can help reduce privacy concerns in high security environments.

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:

HKEY_LOCAL_MACHINE\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 (Release 1507) Administrative Templates (or newer).

Default Value:

Disabled. (KMS client activation data will automatically be sent to Microsoft when the device activates.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>		●	●

18.9.73 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.

18.9.74 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 Release 1703 Administrative Templates (or newer).

18.9.75 Store

This section contains recommendations related to the Microsoft Store.

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 Release 1511 Administrative Templates (or newer).

18.9.75.1 (L2) Ensure 'Disable all apps from Microsoft Store' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This setting configures the launch of all apps from the Microsoft Store that came pre-installed or were downloaded.

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

Note: This policy setting only applies to Windows 10 Enterprise and Windows 10 Education editions.

Note #2: The name of this setting and the Enabled/Disabled values are incorrectly worded – logically, the title implies that configuring it to `Enabled` will disable all apps from the Microsoft Store, and configuring it to `Disabled` will enable all apps from the Microsoft Store. The opposite is true (and is consistent with the GPME help text). This is a logical wording mistake by Microsoft in the Administrative Template.

Rationale:

The Store service is a retail outlet built into Windows, primarily for consumer use. In an enterprise managed environment the IT department should be managing the installation of all applications to reduce the risk of the installation of vulnerable software.

Impact:

All apps from the Microsoft Store that came pre-installed or were downloaded are prevented from launching. Existing Microsoft Store apps will not be updated. Microsoft Store is 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:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsStore:DisableStoreApps

Remediation:

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

Computer Configuration\Policies\Administrative Templates\Windows Components\Store\Disable all apps from Microsoft Store

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WindowsStore.admx/adml` that is included with the Microsoft Windows 10 Release 1511 Administrative Templates (or newer).

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Disable all apps from Windows Store*, but it was renamed starting with the Windows 10 Release 1803 Administrative Templates.

Default Value:

Enabled. (Microsoft Store apps are permitted to be launched and updated. Microsoft Store is enabled.)

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.		●	●

18.9.75.2 (L1) Ensure 'Only display the private store within the Microsoft Store' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting denies access to the retail catalog in the Microsoft Store, but displays the private store.

The recommended state for this setting is: Enabled.

Rationale:

Allowing the private store will allow an organization to control the apps that users have access to add to a system. This will help ensure that unapproved malicious apps are not running on a system.

Impact:

Users will not be able to view the retail catalog in the Microsoft Store, but they will be able to view apps in the private 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:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsStore:RequirePrivateStoreOnly
```

Remediation:

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

Computer Configuration\Policies\Administrative Templates\Windows Components\Store\Only display the private store within the Microsoft Store

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template WindowsStore.admx/adml that is included with the Microsoft Windows 10 Release 1607 Administrative Templates (or newer).

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Only display the private store within the Windows Store app*, but it was renamed starting with the Windows 10 Release 1803 Administrative Templates.

Default Value:

Disabled. (Users can access the retail catalog in the Microsoft Store.)

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.		●	●

18.9.75.3 (L1) Ensure 'Turn off Automatic Download and Install of updates' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting enables or disables the automatic download and installation of Microsoft Store app updates.

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

Rationale:

Keeping your system properly patched can help protect against 0 day vulnerabilities.

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:

`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsStore:AutoDownload`

Remediation:

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

`Computer Configuration\Policies\Administrative Templates\Windows Components\Store\Turn off Automatic Download and Install of updates`

Note: This Group Policy path may not exist by default. It 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 Release 1511 Administrative Templates (or newer).

Default Value:

Disabled. (Microsoft Store automatically downloads and installs updates for Microsoft Store apps.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><u>7.3 Perform Automated Operating System Patch Management</u> Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.</p>	●	●	●
v7	<p><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>	●	●	●

18.9.75.4 (L1) Ensure 'Turn off the offer to update to the latest version of Windows' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Enables or disables the Microsoft Store offer to update to the latest version of Windows.

The recommended state for this setting is: Enabled.

Rationale:

Unplanned OS upgrades can lead to more preventable support calls. The IT department should be managing and approving all upgrades and updates.

Impact:

The Microsoft Store application will not offer updates to the latest version of 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:

`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsStore:DisableOSUpgrade`

Remediation:

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

`Computer Configuration\Policies\Administrative Templates\Windows Components\Store\Turn off the offer to update to the latest version of Windows`

Note: This Group Policy path may not exist by default. It 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 Release 1511 Administrative Templates (or newer).

Default Value:

Disabled. (The Microsoft Store application will offer updates to the latest version of Windows.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><u>7.3 Perform Automated Operating System Patch Management</u> Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.</p>	●	●	●
v7	<p><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>	●	●	●

18.9.75.5 (L2) Ensure 'Turn off the Store application' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This setting denies or allows access to the Store application.

The recommended state for this setting is: Enabled.

Note: Per [Microsoft TechNet](#) and [MSKB 3135657](#), this policy setting does not apply to any Windows 10 editions other than Enterprise and Education.

Rationale:

Only applications approved by an IT department should be installed. Allowing users to install 3rd party applications can lead to missed patches and potential zero day vulnerabilities.

Impact:

Access to the Microsoft Store application 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:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsStore:RemoveWindowsStore
```

Remediation:

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

Computer Configuration\Policies\Administrative Templates\Windows Components\Store\Turn off the Store application

Note: This Group Policy path may not exist by default. It 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, or by the Group Policy template `WindowsStore.admx/adml` that is included with the Microsoft Windows 10 Release 1511 Administrative Templates (or newer).

Default Value:

Disabled. (Access to the Microsoft Store application is allowed.)

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.		●	●

18.9.76 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).

18.9.77 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.

18.9.78 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.

18.9.79 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 Release 21H2 Administrative Templates (or newer).

18.9.80 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 (Release 1507) Administrative Templates and Microsoft Windows 10 Release 1511 Administrative Templates.

18.9.81 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 Release 21H2 Administrative Templates (or newer).

18.9.81.1 (L1) Ensure 'Allow widgets' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting specifies whether the widgets feature is allowed on the device. The widgets feature provides information such as, weather, news, sports, stocks, traffic, and entertainment (not an inclusive list).

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

Rationale:

Due to privacy concerns, apps and features such as widgets on the Windows taskbar should be treated as a possible security risk due to the potential of data being sent back to 3rd parties, such as Microsoft.

Impact:

The widget feature on the Windows taskbar will not be available 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:

`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Dsh:AllowNewsAndInterests`

Remediation:

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

Computer Configuration\Policies\Administrative Templates\Windows Components\Widgets\Allow Widgets

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `NewsAndInterests.admx/adml` that is included with the Microsoft Windows 10 Release 21H2 Administrative Templates (or newer).

Default Value:

Enabled. (Widget feature is allowed on the device.)

18.9.82 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.

18.9.83 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.

18.9.84 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.

18.9.85 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 Release 1703 Administrative Templates (or newer).

18.9.85.1 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 Release 1703 Administrative Templates (or newer).

18.9.85.1.1 (L1) Ensure 'Configure Windows Defender SmartScreen' is set to 'Enabled: Warn and prevent bypass' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting allows you to manage the behavior of Windows Defender SmartScreen. Windows Defender 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 Defender 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 before they are allowed to run 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 locations:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System:EnableSmartScreen  
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System:ShellSmartScreenLevel
```

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 Release 1703 Administrative Templates.

Default Value:

Disabled. (Windows Defender SmartScreen behavior is managed by administrators on the PC by using Windows Defender SmartScreen Settings in Action Center.)

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.		●	●

18.9.85.2 Microsoft Edge

This section contains recommendations for Microsoft Edge-related Windows Defender SmartScreen settings.

The Group Policy settings contained within this section are provided by the Group Policy template `SmartScreen.admx/adml` that is included with the Microsoft Windows 10 Release 1703 Administrative Templates (or newer).

18.9.85.2.1 (L1) Ensure 'Configure Windows Defender SmartScreen' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting lets you decide whether to turn on SmartScreen Filter. SmartScreen Filter provides warning messages to help protect your employees from potential phishing scams and malicious software.

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

Rationale:

SmartScreen serves an important purpose as it helps to warn users of possible malicious sites and files. Allowing users to turn off this setting can make the browser become more 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:

<code>HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\MicrosoftEdge\PhishingFilter:EnabledV9</code>
--

Remediation:

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

Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender SmartScreen\Microsoft Edge\Configure Windows Defender SmartScreen

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MicrosoftEdge.admx/adml` that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

Note #2: In the Microsoft Windows 10 RTM (Release 1507) Administrative Templates, this setting was initially named *Allows you to configure SmartScreen*. In the Microsoft Windows 10 Release 1511 Administrative Templates, it was renamed to *Turn off the SmartScreen Filter*. In the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates, it was renamed (again) to *Configure SmartScreen Filter*. Finally, it was given its current name of *Configure Windows Defender SmartScreen* starting with the Windows 10 Release 1703 Administrative Templates.

Default Value:

Enabled. (SmartScreen Filter is turned on.)

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	8.1 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.	●	●	●

18.9.85.2.2 (L1) Ensure 'Prevent bypassing Windows Defender SmartScreen prompts for sites' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting lets you decide whether employees can override the SmartScreen Filter warnings about potentially malicious websites.

The recommended state for this setting is: Enabled.

Rationale:

SmartScreen will warn an employee if a website is potentially malicious. Enabling this setting prevents these warnings from being bypassed.

Impact:

Employees will not be able to ignore SmartScreen Filter warnings, and they will be blocked from going to potentially malicious websites that SmartScreen detects.

Audit:

Navigate to the UI 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\Policies\Microsoft\MicrosoftEdge\PhishingFilter:PreventOverride

Remediation:

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

Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender SmartScreen\Microsoft Edge\Prevent bypassing Windows Defender SmartScreen prompts for sites

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MicrosoftEdge.admx/adml that is included with the Microsoft Windows 10 Release 1511 Administrative Templates (or newer).

Note #2: In the Microsoft Windows 10 Release 1511 Administrative Templates, this setting was initially named *Don't allow SmartScreen Filter warning overrides*. In the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates, this setting was renamed to *Prevent bypassing SmartScreen prompts for sites*. Finally, it was given its current name of *Prevent bypassing Windows Defender SmartScreen prompts for sites* starting with the Windows 10 Release 1703 Administrative Templates.

Default Value:

Disabled. (Employees will be able to ignore SmartScreen Filter warnings about potentially malicious websites and continue to the site.)

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	8.1 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.	●	●	●

18.9.86 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.

18.9.87 Windows Game Recording and Broadcasting

This section contains settings for Windows Game Recording and Broadcasting.

This Group Policy section is provided by the Group Policy template `GameDVR.admx/adml` that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

18.9.87.1 (L1) Ensure 'Enables or disables Windows Game Recording and Broadcasting' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting enables or disables the Windows Game Recording and Broadcasting features.

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

Rationale:

If this setting is allowed, users could record and broadcast session info to external sites, which is both a risk of accidentally exposing sensitive company data (on-screen) outside the company as well as a privacy concern.

Impact:

Windows Game Recording 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:

`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\GameDVR:AllowGameDVR`

Remediation:

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

Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Game Recording and Broadcasting\Enables or disables Windows Game Recording and Broadcasting

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `GameDVR.admx/adml` that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

Default Value:

Enabled. (Recording and Broadcasting (streaming) is allowed.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>		●	●

18.9.88 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 (Release 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 Release 1607 & Server 2016 Administrative Templates.

18.9.89 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 Release 1607 & Server 2016 Administrative Templates (or newer).

18.9.89.1 (L2) Ensure 'Allow suggested apps in Windows Ink Workspace' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

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:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsInkWorkspace:AllowSuggestedAppsInWindowsInkWorkspace
```

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 Release 1607 & Server 2016 Administrative Templates (or newer).

Default Value:

Enabled. (The suggested apps in Windows Ink Workspace will be allowed.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

18.9.89.2 (L1) Ensure 'Allow Windows Ink Workspace' is set to 'Enabled: On, but disallow access above lock' OR 'Disabled' but not 'Enabled: On' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 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:

HKEY_LOCAL_MACHINE\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 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 Release 1607 & Server 2016 Administrative Templates (or newer).

Default Value:

Enabled. (Windows Ink Workspace is permitted above the lock screen.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.	●	●	●

18.9.90 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.

18.9.90.1 (L1) Ensure 'Allow user control over installs' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

HKEY_LOCAL_MACHINE\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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>2.5 Allowlist Authorized Software</p> <p>Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.</p>		●	●

18.9.90.2 (L1) Ensure 'Always install with elevated privileges' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

HKEY_LOCAL_MACHINE\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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>5.4 <u>Restrict Administrator Privileges to Dedicated Administrator Accounts</u></p> <p>Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.</p>	●	●	●
v7	<p>4.3 <u>Ensure the Use of Dedicated Administrative Accounts</u></p> <p>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.</p>	●	●	●

18.9.90.3 (L2) Ensure 'Prevent Internet Explorer security prompt for Windows Installer scripts' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

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:

HKEY_LOCAL_MACHINE\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.)

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.			

18.9.91 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.

18.9.91.1 (L1) Ensure 'Sign-in and lock last interactive user automatically after a restart' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:  
DisableAutomaticRestartSignOn
```

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 Release 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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

18.9.92 Windows Mail

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 `WindowsMail.admx/adml` that is only included with the Microsoft Windows Vista through the Windows 10 Release 1703 Administrative Templates.

18.9.93 Windows Media 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 `MediaCenter.admx/adml` that is only included with the Microsoft Windows Vista through Windows 10 Release 1511 Administrative Templates.

18.9.94 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.

18.9.95 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.

18.9.96 Windows Meeting Space

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 `WindowsCollaboration.admx/adml` that is only included with the Microsoft Windows Vista and Server 2008 (non-R2) Administrative Templates.

18.9.97 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.

18.9.98 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.

18.9.99 Windows Movie Maker

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 `MovieMaker.admx/adml` that is only included with the Microsoft Windows Vista and Server 2008 (non-R2) Administrative Templates.

18.9.100 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).

18.9.100.1 (L1) Ensure 'Turn on PowerShell Script Block Logging' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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.

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:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging:EnableScriptBlockLogging
```

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 (Release 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

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.		●	●

18.9.100.2 (L1) Ensure 'Turn on PowerShell Transcription' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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: Disabled.

Rationale:

If this setting is enabled there is a risk that passwords could get stored in plain text in the `PowerShell_transcript` output file.

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:

`HKEY_LOCAL_MACHINE\SOFTWARE\ Policies\Microsoft\Windows\PowerShell\Transcription:EnableTranscripting`

Remediation:

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

`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 (Release 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.)

18.9.101 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).

18.9.102 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.

18.9.102.1 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.

18.9.102.1.1 (L1) Ensure 'Allow Basic authentication' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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`.

Note: Clients that use Microsoft's Exchange Online service (Office 365) will require an exception to this recommendation, to instead have this setting set to Enabled. Exchange Online uses Basic authentication over HTTPS, and so the Exchange Online authentication traffic will still be safely encrypted.

Rationale:

Basic authentication is less robust than other authentication methods available in WinRM because credentials including passwords are transmitted in plain text. An attacker 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:

HKEY_LOCAL_MACHINE\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.)

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.		●	●

18.9.102.1.2 (L1) Ensure 'Allow unencrypted traffic' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 an attacker 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:

HKEY_LOCAL_MACHINE\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.)

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.			

18.9.102.1.3 (L1) Ensure 'Disallow Digest authentication' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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, an attacker 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:

HKEY_LOCAL_MACHINE\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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>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).</p>			
v7	<p>16.5 Encrypt Transmittal of Username and Authentication Credentials Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.</p>			

18.9.102.2 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.

18.9.102.2.1 (L1) Ensure 'Allow Basic authentication' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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. An attacker 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:

```
HKEY_LOCAL_MACHINE\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.)

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.	●	●	

18.9.102.2.2 (L2) Ensure 'Allow remote server management through WinRM' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

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:

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 object is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\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:

Disabled. (The WinRM service will not respond to requests from a remote computer, regardless of whether or not any WinRM listeners are configured.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>		●	●

18.9.102.2.3 (L1) Ensure 'Allow unencrypted traffic' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 an attacker 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:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WinRM\Service: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 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.)

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.			

18.9.102.2.4 (L1) Ensure 'Disallow WinRM from storing RunAs credentials' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

HKEY_LOCAL_MACHINE\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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
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.			

18.9.103 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.

18.9.103.1 (L2) Ensure 'Allow Remote Shell Access' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

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 workstation.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy object is backed by the following registry location:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WinRM\Service\WinRS:AllowRemoteShellAccess

Remediation:

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

Computer Configuration\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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>		●	●

18.9.104 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 Release 21H2 Administrative Templates (or newer).

18.9.104.1 (L1) Ensure 'Allow clipboard sharing with Windows Sandbox' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting enables or disables clipboard sharing with the Windows sandbox.

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

Note: The Windows Sandbox feature was first introduced in Windows 10 R1903, and allows a temporary "clean install" virtual instance of Windows to be run inside the host, for the ostensible purpose of testing applications without making changes to the host.

Rationale:

Disabling copy and paste decreases the attack surface exposed by the Windows Sandbox and possible exposure of untrusted applications to the internal network.

Impact:

The copy and paste function to/from the Windows Sandbox will be disabled. Therefore, files will not be able to be moved to/from the Windows Sandbox via the clipboard.

Audit:

Navigate to the UI 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\Policies\Microsoft\Windows\Sandbox:AllowClipboardRedirection

Remediation:

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

Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Sandbox\Allow clipboard sharing with Windows Sandbox
--

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WindowsSandbox.admx/adml` that is included with the Microsoft Windows 10 Release 21H2 Administrative Templates (or newer).

Default Value:

Enabled. (Copy and paste between the host and Windows Sandbox are permitted.)

References:

1. <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-sandbox/windows-sandbox-configure-using-wsb-file>

18.9.104.2 (L1) Ensure 'Allow networking in Windows Sandbox' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting enables or disables networking in the Windows Sandbox. Networking is achieved by creating a virtual switch on the host, and connecting the Windows Sandbox to it via a virtual Network Interface Card (NIC).

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

Note: The Windows Sandbox feature was first introduced in Windows 10 R1903, and allows a temporary "clean install" virtual instance of Windows to be run inside the host, for the ostensible purpose of testing applications without making changes to the host.

Rationale:

Disabling network access decreases the attack surface exposed by the Windows Sandbox and exposure of untrusted applications to the internal network.

Note: Per Microsoft, enabling networking in the Windows Sandbox can expose untrusted applications to the internal network.

Impact:

Network access to/from the Windows Sandbox will be disabled. Therefore, files will not be able to be moved to/from the Windows Sandbox via the 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\Policies\Microsoft\Windows\Sandbox:AllowNetworking
```

Remediation:

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

Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Sandbox\Allow networking in Windows Sandbox

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WindowsSandbox.admx/adml` that is included with the Microsoft Windows 10 Release 21H2 Administrative Templates (or newer).

Default Value:

Enabled. (Networking in the Windows Sandbox is enabled.)

References:

1. <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-sandbox/windows-sandbox-configure-using-wsb-file>

18.9.105 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 Release 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 Release 1809 & Server 2019 Administrative Templates.

18.9.105.1 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 Release 1803 Administrative Templates (or newer).

18.9.105.2 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 Release 1709 Administrative Templates (or newer).

18.9.105.2.1 (L1) Ensure 'Prevent users from modifying settings' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

`HKEY_LOCAL_MACHINE\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 Release 1709 Administrative Templates (or newer).

Default Value:

Disabled. (Local users are allowed to make changes in the Exploit protection settings area.)

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.	●	●	

18.9.106 Windows SideShow

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 `SideShow.admx/adml` that is only included with the Microsoft Windows Vista Administrative Templates through Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

18.9.107 Windows System Resource 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 `SystemResourceManager.admx/adml` that is only included with the Microsoft Windows Vista through Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

18.9.108 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.

18.9.108.1 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 Release 21H2 Administrative Templates (or newer).

18.9.108.1.1 (L1) Ensure 'No auto-restart with logged on users for scheduled automatic updates installations' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

HKEY_LOCAL_MACHINE\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.)

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.	●	●	●

18.9.108.2 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 Release 21H2 Administrative Templates (or newer).

18.9.108.2.1 (L1) Ensure 'Configure Automatic Updates' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 three 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 3rd-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 3rd-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:

HKEY_LOCAL_MACHINE\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.)

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.	●	●	●

18.9.108.2.2 (L1) Ensure 'Configure Automatic Updates: Scheduled install day' is set to '0 - Every day' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 the 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:

```
HKEY_LOCAL_MACHINE\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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>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.</p>	●	●	●
v7	<p>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.</p>	●	●	●

18.9.108.2.3 (L1) Ensure 'Remove access to "Pause updates" feature' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy removes access to "Pause updates" feature.

The recommended state for this setting is: Enabled.

Rationale:

In order to ensure security and system updates are applied, system administrators should control when updates are applied to systems.

Impact:

Users will not be able to select the "Pause updates" option in Windows Update to prevent updates from being installed 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:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate:SetDisablePauseUXAccess

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\Remove access to "Pause updates" feature

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 Release 1809 & Server 2019 Administrative Templates (or newer).

Default Value:

Disabled. (Users have access to the "Pause updates" feature.)

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.	●	●	●

18.9.108.3 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 Release 21H2 Administrative Templates (or newer).

18.9.108.4 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 Release 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 Release 1709 Administrative Templates. It was renamed (again) to *Manage updates offered from Windows Update* starting with the Microsoft Windows 11 Release 21H2 Administrative Templates.

18.9.108.4.1 (L1) Ensure 'Manage preview builds' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting manage which updates that are receive 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: <https://aka.ms/wipforbiz>

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 an attacker 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:

HKEY_LOCAL_MACHINE\SOFTWARE\ Policies\Microsoft\Windows\WindowsUpdate:ManagePreviewBuildsPolicyValue

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 Release 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>

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	●	●	●

18.9.108.4.2 (L1) Ensure 'Select when Preview Builds and Feature Updates are received' is set to 'Enabled: 180 or more days' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines when Preview Build or Feature Updates are received.

Defer Updates This enables devices to defer taking the next Feature Update available to your channel for up to 14 days for all the pre-release channels and up to 365 days for the Semi-Annual Channel. Or, if the device is updating from the Semi-Annual Channel, a version for the device to move to and/or stay on until the policy is updated or the device reaches end of service can be specified. Note: If you set both policies, the version specified will take precedence and the deferrals will not be in effect. Please see the Windows Release Information page for OS version information.

Pause Updates To prevent Feature Updates from being received on their scheduled time, you can temporarily pause Feature Updates. The pause will remain in effect for 35 days from the specified start date or until the field is cleared (Quality Updates will still be offered).

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 10 R1607, 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 Release 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](#)

Note #3: Prior to Windows 10 R1703, values above 180 days are not recognized by the OS. Starting with Windows 10 R1703, the maximum number of days you can defer is 365 days.

Rationale:

In a production environment, it is preferred to only use software and features that are publicly available, after they have gone through rigorous testing in beta.

Impact:

Feature Updates will be delayed until they are publicly released to general public by 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:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate:DeferFeatureUpdates  
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate:DeferFeatureUpdatesPeriodInDays
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to Enabled: 180 or more days:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update\Manage updates offered from Windows Update\Windows Update for Business>Select when Preview Builds and Feature 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 Release 1607 & Server 2016 Administrative Templates (or newer).

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Select when Feature Updates are received*, but it was renamed to *Select when Preview Builds and Feature Updates are received* starting with the Windows 10 Release 1709 Administrative Templates.

Default Value:

Disabled. (Feature Update cadence will not be enforced by Group Policy.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>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.</p>		●	●
v8	<p>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.</p>	●	●	●
v7	<p>2.4 Track Software Inventory Information The software inventory system should track the name, version, publisher, and install date for all software, including operating systems authorized by the organization.</p>		●	●

18.9.108.4.3 (L1) Ensure 'Select when Quality Updates are received' is set to 'Enabled: 0 days' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting 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 10 R1607, 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 Release 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:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate:DeferQualityUpdates  
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate:DeferQualityUpdatesPeriodInDays
```

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\Windows Update for Business>Select when Quality Updates are received
```

Note: This Group Policy path does not exist by default. An updated Group Policy template (WindowsUpdate.admx/adml) is required - it is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

Default Value:

Enabled: 0 days. (Install new Quality Updates as soon as they are available.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>7.3 Perform Automated Operating System Patch Management</u> Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v7	<u>3.4 Deploy Automated Operating System Patch Management Tools</u> 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.	●	●	●

19 Administrative Templates (User)

This section contains user-based recommendations from Group Policy Administrative Templates (ADMX).

19.1 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.

19.1.1 Add or Remove Programs

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 `AddRemovePrograms.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.1.2 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 `ControlPanelDisplay.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.1.3 Personalization (formerly Desktop Themes)

This section contains recommendations for personalization settings.

This Group Policy section is provided by the Group Policy template `ControlPanelDisplay.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note: This section was initially named *Desktop Themes* but was renamed by Microsoft to *Personalization* starting with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates.

19.1.3.1 (L1) Ensure 'Enable screen saver' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting enables/disables the use of desktop screen savers.

The recommended state for this setting is: Enabled.

Rationale:

If a user forgets to lock their computer when they walk away, it is possible that a passerby will hijack it. Configuring a timed screen saver with password lock will help to protect against these hijacks.

Impact:

A screen saver runs, provided that the following two conditions hold: First, a valid screen saver on the client is specified through the recommendation *Force specific screen saver* or through Control Panel on the client computer. Second, the recommendation *Screen saver timeout* setting is set to a nonzero value through the setting or through Control Panel.

Audit:

Navigate to the UI 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_USERS\[USER SID]\Software\Policies\Microsoft\Windows\Control Panel\Desktop:ScreenSaveActive

Remediation:

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

User Configuration\Policies\Administrative Templates\Control Panel\Personalization\Enable screen saver

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 7 & Server 2008 R2 Administrative Templates (or newer).

Default Value:

Enabling/disabling the screen saver is managed locally by the user.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.3 Configure Automatic Session Locking on Enterprise Assets</u> 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	<u>16.11 Lock Workstation Sessions After Inactivity</u> Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

19.1.3.2 (L1) Ensure 'Password protect the screen saver' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting determines whether screen savers used on the computer are password protected.

The recommended state for this setting is: Enabled.

Rationale:

If a user forgets to lock their computer when they walk away, it is possible that a passerby will hijack it. Configuring a timed screen saver with password lock will help to protect against these hijacks.

Impact:

All screen savers are password protected. The "Password protected" checkbox on the Screen Saver dialog in the Personalization or Display Control Panel will be disabled, preventing users from changing the password protection 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:

```
HKEY_USERS\[USER SID]\Software\Policies\Microsoft\Windows\Control  
Panel\Desktop:ScreenSaverIsSecure
```

Remediation:

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

```
User Configuration\Policies\Administrative Templates\Control  
Panel\Personalization\Password protect the screen saver
```

Note: This Group Policy path is provided by the Group Policy template ControlPanelDisplay.admx/adml that is included with all versions of the Microsoft Windows Administrative Templates.

Default Value:

Whether or not to password protect each screen saver is managed locally by the user.

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.	●	●	●

19.1.3.3 (L1) Ensure 'Screen saver timeout' is set to 'Enabled: 900 seconds or fewer, but not 0' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting specifies how much user idle time must elapse before the screen saver is launched.

The recommended state for this setting is: Enabled: 900 seconds or fewer, but not 0.

Note: This setting has no effect under the following circumstances:

- The wait time is set to zero.
- The "Enable Screen Saver" setting is disabled.
- A valid screen existing saver is not selected manually or via the "Screen saver executable name" setting

Rationale:

If a user forgets to lock their computer when they walk away, it is possible that a passerby will hijack it. Configuring a timed screen saver with password lock will help to protect against these hijacks.

Impact:

The screen saver will automatically activate when the computer has been left unattended for the amount of time specified, and the users will not be able to change the timeout value.

Audit:

Navigate to the UI 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_USERS\ [USER SID]\Software\Policies\Microsoft\Windows\Control Panel\Desktop:ScreenSaveTimeOut

Remediation:

To establish the recommended configuration via GP, set the following UI path to Enabled:
900 or fewer, but not 0:

User Configuration\Policies\Administrative Templates\Control Panel\Personalization\Screen saver timeout

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 7 & Server 2008 R2 Administrative Templates (or newer).

Default Value:

15 minutes. (May subsequently be reconfigured locally by the user.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.3 Configure Automatic Session Locking on Enterprise Assets</u> 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	<u>16.11 Lock Workstation Sessions After Inactivity</u> Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

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 (L1) Ensure 'Turn off toast notifications on the lock screen' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

```
HKEY_USERS\ [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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
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 Release 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 (L2) Ensure 'Turn off Help Experience Improvement Program' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

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:

HKEY_USERS\ [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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

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 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.

19.7.2 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).

19.7.3 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.

19.7.4 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.

19.7.4.1 (L1) Ensure 'Do not preserve zone information in file attachments' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

```
HKEY_USERS\[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.)

19.7.4.2 (L1) Ensure 'Notify antivirus programs when opening attachments' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

```
HKEY_USERS\ [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.)

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.		●	●

19.7.5 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.

19.7.6 Backup

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 `UserDataBackup.admx/adml` that is included only with the Microsoft Windows Vista through Windows 8.0 & Server 2012 (non-R2) Administrative Templates, as well as the Microsoft Windows 10 RTM (Release 1507) and Windows 10 Release 1511 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 Release 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 Release 1607 & Server 2016 Administrative Templates (or newer).

19.7.8.1 (L1) Ensure 'Configure Windows spotlight on lock screen' is set to Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

```
HKEY_USERS\ [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 Release 1607 & Server 2016 Administrative Templates (or newer).

Default Value:

Enabled. (Windows Spotlight is set as the lock screen provider.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

19.7.8.2 (L1) Ensure 'Do not suggest third-party content in Windows spotlight' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

```
HKEY_USERS\[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 Release 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.)

19.7.8.3 (L2) Ensure 'Do not use diagnostic data for tailored experiences' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

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:

```
HKEY_USERS\[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 Release 1703 Administrative Templates (or newer).

Default Value:

Disabled. (Microsoft will use diagnostic data to provide personalized recommendations, tips and offers.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> 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 (L2) Ensure 'Turn off all Windows spotlight features' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This policy setting determines whether the all Windows Spotlight features are turned on/off (together).

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:

```
HKEY_USERS\[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 Release 1607 & Server 2016 Administrative Templates (or newer).

Default Value:

Disabled. (Windows Spotlight features are allowed.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> 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 (L1) Ensure 'Turn off Spotlight collection on Desktop' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

```
HKEY_USERS\[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 10 Release 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>

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 Release 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 Release 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 Import Video

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 `CaptureWizard.admx/adml` that is only included with the Microsoft Windows Vista and Windows Server 2008 (non-R2) Administrative Templates.

19.7.19 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.

19.7.20 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.

19.7.21 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).

19.7.22 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 (Release 1507) Administrative Templates (or newer).

19.7.23 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.

19.7.24 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 Release 1607 & Server 2016 Administrative Templates (or newer).

19.7.25 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.

19.7.26 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.

19.7.27 Network Projector

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 `NetworkProjection.admx/adml` that is only included with the Microsoft Windows Vista through the Windows 8.1 Update & Server 2012 R2 Update Administrative Templates.

19.7.28 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.

19.7.28.1 (L1) Ensure 'Prevent users from sharing files within their profile.' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

```
HKEY_USERS\ [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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
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.	●	●	●

19.7.29 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 Release 1809 and Server 2019 Administrative Templates (or newer).

19.7.30 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.

19.7.31 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.

19.7.32 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.

19.7.33 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).

19.7.34 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.

19.7.35 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 Release 1511 Administrative Templates (or newer).

19.7.36 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.

19.7.37 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.

19.7.38 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 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 Release 1703 Administrative Templates (or newer).

19.7.41 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.

19.7.42 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 (Release 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 Release 1607 & Server 2016 Administrative Templates.

19.7.43 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.

19.7.43.1 (L1) Ensure 'Always install with elevated privileges' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

HKEY_USERS\ [USER SID]\Software\Policies\Microsoft\Windows\Installer:AlwaysInstallElevated

Remediation:

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

User 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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts</p> <p>Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.</p>	●	●	●
v7	<p>4.3 Ensure the Use of Dedicated Administrative Accounts</p> <p>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.</p>	●	●	●

19.7.44 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.

19.7.45 Windows Mail

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 `WindowsMail.admx/adml` that is only included with the Microsoft Windows Vista through Windows 10 Release 1703 Administrative Templates.

19.7.46 Windows Media 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 `MediaCenter.admx/adml` that is only included with the Microsoft Windows Vista through Windows 10 Release 1511 Administrative Templates.

19.7.47 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.

19.7.47.1 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.

19.7.47.2 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.

19.7.47.2.1 (L2) Ensure 'Prevent Codec Download' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

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:

HKEY_USERS\ [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.

Appendix: Recommendation Summary Table

Control		Set Correctly	
		Yes	No
1	Account Policies		
1.1	Password Policy		
1.1.1	(L1) Ensure 'Enforce password history' is set to '24 or more password(s)' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2	(L1) Ensure 'Maximum password age' is set to '365 or fewer days, but not 0' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.3	(L1) Ensure 'Minimum password age' is set to '1 or more day(s)' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.4	(L1) Ensure 'Minimum password length' is set to '14 or more character(s)' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.5	(L1) Ensure 'Password must meet complexity requirements' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.6	(L1) Ensure 'Relax minimum password length limits' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.7	(L1) Ensure 'Store passwords using reversible encryption' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.2	Account Lockout Policy		
1.2.1	(L1) Ensure 'Account lockout duration' is set to '15 or more minute(s)' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.2.2	(L1) Ensure 'Account lockout threshold' is set to '5 or fewer invalid logon attempt(s), but not 0' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.2.3	(L1) Ensure 'Reset account lockout counter after' is set to '15 or more minute(s)' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2	Local Policies		
2.1	Audit Policy		
2.2	User Rights Assignment		
2.2.1	(L1) Ensure 'Access Credential Manager as a trusted caller' is set to 'No One' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.2	(L1) Ensure 'Access this computer from the network' is set to 'Administrators, Remote Desktop Users' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.3	(L1) Ensure 'Act as part of the operating system' is set to 'No One' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.4	(L1) Ensure 'Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

Control		Set Correctly	
		Yes	No
2.2.5	(L1) Ensure 'Allow log on locally' is set to 'Administrators, Users' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.6	(L1) Ensure 'Allow log on through Remote Desktop Services' is set to 'Administrators, Remote Desktop Users' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.7	(L1) Ensure 'Back up files and directories' is set to 'Administrators' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.8	(L1) Ensure 'Change the system time' is set to 'Administrators, LOCAL SERVICE' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.9	(L1) Ensure 'Change the time zone' is set to 'Administrators, LOCAL SERVICE, Users' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.10	(L1) Ensure 'Create a pagefile' is set to 'Administrators' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.11	(L1) Ensure 'Create a token object' is set to 'No One' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.12	(L1) Ensure 'Create global objects' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.13	(L1) Ensure 'Create permanent shared objects' is set to 'No One' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.14	(L1) Configure 'Create symbolic links' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.15	(L1) Ensure 'Debug programs' is set to 'Administrators' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.16	(L1) Ensure 'Deny access to this computer from the network' to include 'Guests, Local account' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.17	(L1) Ensure 'Deny log on as a batch job' to include 'Guests' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.18	(L1) Ensure 'Deny log on as a service' to include 'Guests' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.19	(L1) Ensure 'Deny log on locally' to include 'Guests' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.20	(L1) Ensure 'Deny log on through Remote Desktop Services' to include 'Guests, Local account' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.21	(L1) Ensure 'Enable computer and user accounts to be trusted for delegation' is set to 'No One' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.22	(L1) Ensure 'Force shutdown from a remote system' is set to 'Administrators' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.23	(L1) Ensure 'Generate security audits' is set to 'LOCAL SERVICE, NETWORK SERVICE' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

Control		Set Correctly	
		Yes	No
2.2.24	(L1) Ensure 'Impersonate a client after authentication' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.25	(L1) Ensure 'Increase scheduling priority' is set to 'Administrators, Window Manager\Window Manager Group' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.26	(L1) Ensure 'Load and unload device drivers' is set to 'Administrators' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.27	(L1) Ensure 'Lock pages in memory' is set to 'No One' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.28	(L2) Ensure 'Log on as a batch job' is set to 'Administrators' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.29	(L2) Configure 'Log on as a service' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.30	(L1) Ensure 'Manage auditing and security log' is set to 'Administrators' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.31	(L1) Ensure 'Modify an object label' is set to 'No One' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.32	(L1) Ensure 'Modify firmware environment values' is set to 'Administrators' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.33	(L1) Ensure 'Perform volume maintenance tasks' is set to 'Administrators' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.34	(L1) Ensure 'Profile single process' is set to 'Administrators' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.35	(L1) Ensure 'Profile system performance' is set to 'Administrators, NT SERVICE\WdiServiceHost' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.36	(L1) Ensure 'Replace a process level token' is set to 'LOCAL SERVICE, NETWORK SERVICE' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.37	(L1) Ensure 'Restore files and directories' is set to 'Administrators' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.38	(L1) Ensure 'Shut down the system' is set to 'Administrators, Users' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.39	(L1) Ensure 'Take ownership of files or other objects' is set to 'Administrators' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3	Security Options		
2.3.1	Accounts		
2.3.1.1	(L1) Ensure 'Accounts: Administrator account status' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.2	(L1) Ensure 'Accounts: Block Microsoft accounts' is set to 'Users can't add or log on with Microsoft accounts' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

Control		Set Correctly	
		Yes	No
2.3.1.3	(L1) Ensure 'Accounts: Guest account status' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.4	(L1) Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.5	(L1) Configure 'Accounts: Rename administrator account' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1.6	(L1) Configure 'Accounts: Rename guest account' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2	Audit		
2.3.2.1	(L1) Ensure 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2.2	(L1) Ensure 'Audit: Shut down system immediately if unable to log security audits' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3	DCOM		
2.3.4	Devices		
2.3.4.1	(L1) Ensure 'Devices: Allowed to format and eject removable media' is set to 'Administrators and Interactive Users' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.4.2	(L2) Ensure 'Devices: Prevent users from installing printer drivers' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.5	Domain controller		
2.3.6	Domain member		
2.3.6.1	(L1) Ensure 'Domain member: Digitally encrypt or sign secure channel data (always)' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.6.2	(L1) Ensure 'Domain member: Digitally encrypt secure channel data (when possible)' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.6.3	(L1) Ensure 'Domain member: Digitally sign secure channel data (when possible)' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.6.4	(L1) Ensure 'Domain member: Disable machine account password changes' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.6.5	(L1) Ensure 'Domain member: Maximum machine account password age' is set to '30 or fewer days, but not 0' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.6.6	(L1) Ensure 'Domain member: Require strong (Windows 2000 or later) session key' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.7	Interactive logon		

Control		Set Correctly	
		Yes	No
2.3.7.1	(L1) Ensure 'Interactive logon: Do not require CTRL+ALT+DEL' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.7.2	(L1) Ensure 'Interactive logon: Don't display last signed-in' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.7.3	(BL) Ensure 'Interactive logon: Machine account lockout threshold' is set to '10 or fewer invalid logon attempts, but not 0' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.7.4	(L1) Ensure 'Interactive logon: Machine inactivity limit' is set to '900 or fewer second(s), but not 0' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.7.5	(L1) Configure 'Interactive logon: Message text for users attempting to log on' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.7.6	(L1) Configure 'Interactive logon: Message title for users attempting to log on' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.7.7	(L2) Ensure 'Interactive logon: Number of previous logons to cache (in case domain controller is not available)' is set to '4 or fewer logon(s)' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.7.8	(L1) Ensure 'Interactive logon: Prompt user to change password before expiration' is set to 'between 5 and 14 days' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.7.9	(L1) Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or higher (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.8	Microsoft network client		
2.3.8.1	(L1) Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.8.2	(L1) Ensure 'Microsoft network client: Digitally sign communications (if server agrees)' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.8.3	(L1) Ensure 'Microsoft network client: Send unencrypted password to third-party SMB servers' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.9	Microsoft network server		
2.3.9.1	(L1) Ensure 'Microsoft network server: Amount of idle time required before suspending session' is set to '15 or fewer minute(s)' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.9.2	(L1) Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.9.3	(L1) Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.9.4	(L1) Ensure 'Microsoft network server: Disconnect clients when logon hours expire' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

Control		Set Correctly	
		Yes	No
2.3.9.5	(L1) Ensure 'Microsoft network server: Server SPN target name validation level' is set to 'Accept if provided by client' or higher (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.10	Network access		
2.3.10.1	(L1) Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.10.2	(L1) Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.10.3	(L1) Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.10.4	(L1) Ensure 'Network access: Do not allow storage of passwords and credentials for network authentication' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.10.5	(L1) Ensure 'Network access: Let Everyone permissions apply to anonymous users' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.10.6	(L1) Ensure 'Network access: Named Pipes that can be accessed anonymously' is set to 'None' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.10.7	(L1) Ensure 'Network access: Remotely accessible registry paths' is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.10.8	(L1) Ensure 'Network access: Remotely accessible registry paths and sub-paths' is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.10.9	(L1) Ensure 'Network access: Restrict anonymous access to Named Pipes and Shares' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.10.10	(L1) Ensure 'Network access: Restrict clients allowed to make remote calls to SAM' is set to 'Administrators: Remote Access: Allow' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.10.11	(L1) Ensure 'Network access: Shares that can be accessed anonymously' is set to 'None' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.10.12	(L1) Ensure 'Network access: Sharing and security model for local accounts' is set to 'Classic - local users authenticate as themselves' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.11	Network security		
2.3.11.1	(L1) Ensure 'Network security: Allow Local System to use computer identity for NTLM' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.11.2	(L1) Ensure 'Network security: Allow LocalSystem NULL session fallback' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.11.3	(L1) Ensure 'Network Security: Allow PKU2U authentication requests to this computer to use online identities' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

Control		Set Correctly	
		Yes	No
2.3.11.4	(L1) Ensure 'Network security: Configure encryption types allowed for Kerberos' is set to 'AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.11.5	(L1) Ensure 'Network security: Do not store LAN Manager hash value on next password change' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.11.6	(L1) Ensure 'Network security: Force logoff when logon hours expire' is set to 'Enabled' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.11.7	(L1) Ensure 'Network security: LAN Manager authentication level' is set to 'Send NTLMv2 response only. Refuse LM & NTLM' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.11.8	(L1) Ensure 'Network security: LDAP client signing requirements' is set to 'Negotiate signing' or higher (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.11.9	(L1) 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)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.11.10	(L1) 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)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.12	Recovery console		
2.3.13	Shutdown		
2.3.14	System cryptography		
2.3.14.1	(L2) Ensure 'System cryptography: Force strong key protection for user keys stored on the computer' is set to 'User is prompted when the key is first used' or higher (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.15	System objects		
2.3.15.1	(L1) Ensure 'System objects: Require case insensitivity for non-Windows subsystems' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.15.2	(L1) Ensure 'System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.16	System settings		
2.3.17	User Account Control		
2.3.17.1	(L1) Ensure 'User Account Control: Admin Approval Mode for the Built-in Administrator account' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

Control		Set Correctly	
		Yes	No
2.3.17.2	(L1) 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' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.17.3	(L1) Ensure 'User Account Control: Behavior of the elevation prompt for standard users' is set to 'Automatically deny elevation requests' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.17.4	(L1) Ensure 'User Account Control: Detect application installations and prompt for elevation' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.17.5	(L1) Ensure 'User Account Control: Only elevate UIAccess applications that are installed in secure locations' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.17.6	(L1) Ensure 'User Account Control: Run all administrators in Admin Approval Mode' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.17.7	(L1) Ensure 'User Account Control: Switch to the secure desktop when prompting for elevation' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.17.8	(L1) Ensure 'User Account Control: Virtualize file and registry write failures to per-user locations' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3	Event Log		
4	Restricted Groups		
5	System Services		
5.1	(L2) Ensure 'Bluetooth Audio Gateway Service (BTAGService)' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2	(L2) Ensure 'Bluetooth Support Service (bthserv)' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3	(L1) Ensure 'Computer Browser (Browser)' is set to 'Disabled' or 'Not Installed' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4	(L2) Ensure 'Downloaded Maps Manager (MapsBroker)' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.5	(L2) Ensure 'Geolocation Service (lfsvc)' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.6	(L1) Ensure 'IIS Admin Service (IISADMIN)' is set to 'Disabled' or 'Not Installed' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.7	(L1) Ensure 'Infrared monitor service (irmon)' is set to 'Disabled' or 'Not Installed' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.8	(L1) Ensure 'Internet Connection Sharing (ICS) (SharedAccess)' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

Control		Set Correctly	
		Yes	No
5.9	(L2) Ensure 'Link-Layer Topology Discovery Mapper (lltdsvc)' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.10	(L1) Ensure 'LxssManager (LxssManager)' is set to 'Disabled' or 'Not Installed' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.11	(L1) Ensure 'Microsoft FTP Service (FTPSVC)' is set to 'Disabled' or 'Not Installed' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.12	(L2) Ensure 'Microsoft iSCSI Initiator Service (MSiSCSI)' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.13	(L1) Ensure 'OpenSSH SSH Server (sshd)' is set to 'Disabled' or 'Not Installed' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.14	(L2) Ensure 'Peer Name Resolution Protocol (PNRPsrv)' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.15	(L2) Ensure 'Peer Networking Grouping (p2psvc)' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.16	(L2) Ensure 'Peer Networking Identity Manager (p2pimsvc)' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.17	(L2) Ensure 'PNRP Machine Name Publication Service (PNRPAutoReg)' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.18	(L2) Ensure 'Print Spooler (Spooler)' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.19	(L2) Ensure 'Problem Reports and Solutions Control Panel Support (wercplsupport)' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.20	(L2) Ensure 'Remote Access Auto Connection Manager (RasAuto)' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.21	(L2) Ensure 'Remote Desktop Configuration (SessionEnv)' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.22	(L2) Ensure 'Remote Desktop Services (TermService)' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.23	(L2) Ensure 'Remote Desktop Services UserMode Port Redirector (UmRdpService)' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.24	(L1) Ensure 'Remote Procedure Call (RPC) Locator (RpcLocator)' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.25	(L2) Ensure 'Remote Registry (RemoteRegistry)' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.26	(L1) Ensure 'Routing and Remote Access (RemoteAccess)' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.27	(L2) Ensure 'Server (LanmanServer)' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.28	(L1) Ensure 'Simple TCP/IP Services (simptcp)' is set to 'Disabled' or 'Not Installed' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

Control		Set Correctly	
		Yes	No
5.29	(L2) Ensure 'SNMP Service (SNMP)' is set to 'Disabled' or 'Not Installed' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.30	(L1) Ensure 'Special Administration Console Helper (sacsrv)' is set to 'Disabled' or 'Not Installed' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.31	(L1) Ensure 'SSDP Discovery (SSDPSRV)' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.32	(L1) Ensure 'UPnP Device Host (upnphost)' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.33	(L1) Ensure 'Web Management Service (WMSvc)' is set to 'Disabled' or 'Not Installed' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.34	(L2) Ensure 'Windows Error Reporting Service (WerSvc)' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.35	(L2) Ensure 'Windows Event Collector (Webservice)' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.36	(L1) Ensure 'Windows Media Player Network Sharing Service (WMPNetworkSvc)' is set to 'Disabled' or 'Not Installed' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.37	(L1) Ensure 'Windows Mobile Hotspot Service (icssvc)' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.38	(L2) Ensure 'Windows Push Notifications System Service (WpnService)' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.39	(L2) Ensure 'Windows PushToInstall Service (PushToInstall)' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.40	(L2) Ensure 'Windows Remote Management (WS-Management) (WinRM)' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.41	(L1) Ensure 'World Wide Web Publishing Service (W3SVC)' is set to 'Disabled' or 'Not Installed' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.42	(L1) Ensure 'Xbox Accessory Management Service (XboxGipSvc)' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.43	(L1) Ensure 'Xbox Live Auth Manager (XblAuthManager)' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.44	(L1) Ensure 'Xbox Live Game Save (XblGameSave)' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.45	(L1) Ensure 'Xbox Live Networking Service (XboxNetApiSvc)' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
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		

Control		Set Correctly	
		Yes	No
9.1.1	(L1) Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
9.1.2	(L1) Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
9.1.3	(L1) Ensure 'Windows Firewall: Domain: Outbound connections' is set to 'Allow (default)' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
9.1.4	(L1) Ensure 'Windows Firewall: Domain: Settings: Display a notification' is set to 'No' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
9.1.5	(L1) Ensure 'Windows Firewall: Domain: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\domainfw.log' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
9.1.6	(L1) Ensure 'Windows Firewall: Domain: Logging: Size limit (KB)' is set to '16,384 KB or greater' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
9.1.7	(L1) Ensure 'Windows Firewall: Domain: Logging: Log dropped packets' is set to 'Yes' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
9.1.8	(L1) Ensure 'Windows Firewall: Domain: Logging: Log successful connections' is set to 'Yes' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
9.2	Private Profile		
9.2.1	(L1) Ensure 'Windows Firewall: Private: Firewall state' is set to 'On (recommended)' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
9.2.2	(L1) Ensure 'Windows Firewall: Private: Inbound connections' is set to 'Block (default)' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
9.2.3	(L1) Ensure 'Windows Firewall: Private: Outbound connections' is set to 'Allow (default)' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
9.2.4	(L1) Ensure 'Windows Firewall: Private: Settings: Display a notification' is set to 'No' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
9.2.5	(L1) Ensure 'Windows Firewall: Private: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\privatefw.log' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
9.2.6	(L1) Ensure 'Windows Firewall: Private: Logging: Size limit (KB)' is set to '16,384 KB or greater' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
9.2.7	(L1) Ensure 'Windows Firewall: Private: Logging: Log dropped packets' is set to 'Yes' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
9.2.8	(L1) Ensure 'Windows Firewall: Private: Logging: Log successful connections' is set to 'Yes' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
9.3	Public Profile		
9.3.1	(L1) Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

Control		Set Correctly	
		Yes	No
9.3.2	(L1) Ensure 'Windows Firewall: Public: Inbound connections' is set to 'Block (default)' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
9.3.3	(L1) Ensure 'Windows Firewall: Public: Outbound connections' is set to 'Allow (default)' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
9.3.4	(L1) Ensure 'Windows Firewall: Public: Settings: Display a notification' is set to 'No' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
9.3.5	(L1) Ensure 'Windows Firewall: Public: Settings: Apply local firewall rules' is set to 'No' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
9.3.6	(L1) Ensure 'Windows Firewall: Public: Settings: Apply local connection security rules' is set to 'No' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
9.3.7	(L1) Ensure 'Windows Firewall: Public: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\publicfw.log' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
9.3.8	(L1) Ensure 'Windows Firewall: Public: Logging: Size limit (KB)' is set to '16,384 KB or greater' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
9.3.9	(L1) Ensure 'Windows Firewall: Public: Logging: Log dropped packets' is set to 'Yes' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
9.3.10	(L1) Ensure 'Windows Firewall: Public: Logging: Log successful connections' is set to 'Yes' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
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	(L1) Ensure 'Audit Credential Validation' is set to 'Success and Failure' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
17.2	Account Management		
17.2.1	(L1) Ensure 'Audit Application Group Management' is set to 'Success and Failure' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
17.2.2	(L1) Ensure 'Audit Security Group Management' is set to include 'Success' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
17.2.3	(L1) Ensure 'Audit User Account Management' is set to 'Success and Failure' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
17.3	Detailed Tracking		
17.3.1	(L1) Ensure 'Audit PNP Activity' is set to include 'Success' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

Control		Set Correctly	
		Yes	No
17.3.2	(L1) Ensure 'Audit Process Creation' is set to include 'Success' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
17.4	DS Access		
17.5	Logon/Logoff		
17.5.1	(L1) Ensure 'Audit Account Lockout' is set to include 'Failure' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
17.5.2	(L1) Ensure 'Audit Group Membership' is set to include 'Success' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
17.5.3	(L1) Ensure 'Audit Logoff' is set to include 'Success' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
17.5.4	(L1) Ensure 'Audit Logon' is set to 'Success and Failure' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
17.5.5	(L1) Ensure 'Audit Other Logon/Logoff Events' is set to 'Success and Failure' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
17.5.6	(L1) Ensure 'Audit Special Logon' is set to include 'Success' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
17.6	Object Access		
17.6.1	(L1) Ensure 'Audit Detailed File Share' is set to include 'Failure' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
17.6.2	(L1) Ensure 'Audit File Share' is set to 'Success and Failure' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
17.6.3	(L1) Ensure 'Audit Other Object Access Events' is set to 'Success and Failure' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
17.6.4	(L1) Ensure 'Audit Removable Storage' is set to 'Success and Failure' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
17.7	Policy Change		
17.7.1	(L1) Ensure 'Audit Audit Policy Change' is set to include 'Success' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
17.7.2	(L1) Ensure 'Audit Authentication Policy Change' is set to include 'Success' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
17.7.3	(L1) Ensure 'Audit Authorization Policy Change' is set to include 'Success' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
17.7.4	(L1) Ensure 'Audit MPSSVC Rule-Level Policy Change' is set to 'Success and Failure' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
17.7.5	(L1) Ensure 'Audit Other Policy Change Events' is set to include 'Failure' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
17.8	Privilege Use		
17.8.1	(L1) Ensure 'Audit Sensitive Privilege Use' is set to 'Success and Failure' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
17.9	System		

Control		Set Correctly	
		Yes	No
17.9.1	(L1) Ensure 'Audit IPsec Driver' is set to 'Success and Failure' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
17.9.2	(L1) Ensure 'Audit Other System Events' is set to 'Success and Failure' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
17.9.3	(L1) Ensure 'Audit Security State Change' is set to include 'Success' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
17.9.4	(L1) Ensure 'Audit Security System Extension' is set to include 'Success' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
17.9.5	(L1) Ensure 'Audit System Integrity' is set to 'Success and Failure' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18	Administrative Templates (Computer)		
18.1	Control Panel		
18.1.1	Personalization		
18.1.1.1	(L1) Ensure 'Prevent enabling lock screen camera' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.1.1.2	(L1) Ensure 'Prevent enabling lock screen slide show' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.1.2	Regional and Language Options		
18.1.2.1	Handwriting personalization		
18.1.2.2	(L1) Ensure 'Allow users to enable online speech recognition services' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.1.3	(L2) Ensure 'Allow Online Tips' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.2	LAPS		
18.2.1	(L1) Ensure LAPS AdmPwd GPO Extension / CSE is installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.2.2	(L1) Ensure 'Do not allow password expiration time longer than required by policy' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.2.3	(L1) Ensure 'Enable Local Admin Password Management' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.2.4	(L1) Ensure 'Password Settings: Password Complexity' is set to 'Enabled: Large letters + small letters + numbers + special characters' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.2.5	(L1) Ensure 'Password Settings: Password Length' is set to 'Enabled: 15 or more' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.2.6	(L1) Ensure 'Password Settings: Password Age (Days)' is set to 'Enabled: 30 or fewer' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.3	MS Security Guide		
18.3.1	(L1) Ensure 'Apply UAC restrictions to local accounts on network logons' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

Control		Set Correctly	
		Yes	No
18.3.2	(L1) Ensure 'Configure SMB v1 client driver' is set to 'Enabled: Disable driver (recommended)' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.3.3	(L1) Ensure 'Configure SMB v1 server' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.3.4	(L1) Ensure 'Enable Structured Exception Handling Overwrite Protection (SEHOP)' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.3.5	(L1) Ensure 'Limits print driver installation to Administrators' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.3.6	(L1) Ensure 'NetBT NodeType configuration' is set to 'Enabled: P-node (recommended)' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.3.7	(L1) Ensure 'WDigest Authentication' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.4	MSS (Legacy)		
18.4.1	(L1) Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.4.2	(L1) Ensure 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.4.3	(L1) Ensure 'MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.4.4	(L2) Ensure 'MSS: (DisableSavePassword) Prevent the dial-up password from being saved' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.4.5	(L1) Ensure 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.4.6	(L2) Ensure 'MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds' is set to 'Enabled: 300,000 or 5 minutes (recommended)' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.4.7	(L1) Ensure 'MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.4.8	(L2) Ensure 'MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

Control		Set Correctly	
		Yes	No
18.4.9	(L1) Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.4.10	(L1) Ensure 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)' is set to 'Enabled: 5 or fewer seconds' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.4.11	(L2) Ensure 'MSS: (TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted' is set to 'Enabled: 3' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.4.12	(L2) Ensure 'MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted' is set to 'Enabled: 3' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.4.13	(L1) 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)	<input type="checkbox"/>	<input type="checkbox"/>
18.5	Network		
18.5.1	Background Intelligent Transfer Service (BITS)		
18.5.2	BranchCache		
18.5.3	DirectAccess Client Experience Settings		
18.5.4	DNS Client		
18.5.4.1	(L1) Ensure 'Configure DNS over HTTPS (DoH) name resolution' is set to 'Enabled: Allow DoH' or higher (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.5.4.2	(L1) Ensure 'Turn off multicast name resolution' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.5.5	Fonts		
18.5.5.1	(L2) Ensure 'Enable Font Providers' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.5.6	Hotspot Authentication		
18.5.7	Lanman Server		
18.5.8	Lanman Workstation		
18.5.8.1	(L1) Ensure 'Enable insecure guest logons' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.5.9	Link-Layer Topology Discovery		
18.5.9.1	(L2) Ensure 'Turn on Mapper I/O (LLTDIO) driver' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.5.9.2	(L2) Ensure 'Turn on Responder (RSPNDR) driver' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.5.10	Microsoft Peer-to-Peer Networking Services		
18.5.10.1	Peer Name Resolution Protocol		

Control		Set Correctly	
		Yes	No
18.5.10.2	(L2) Ensure 'Turn off Microsoft Peer-to-Peer Networking Services' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.5.11	Network Connections		
18.5.11.1	Windows Defender Firewall (formerly Windows Firewall)		
18.5.11.2	(L1) Ensure 'Prohibit installation and configuration of Network Bridge on your DNS domain network' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.5.11.3	(L1) Ensure 'Prohibit use of Internet Connection Sharing on your DNS domain network' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.5.11.4	(L1) Ensure 'Require domain users to elevate when setting a network's location' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.5.12	Network Connectivity Status Indicator		
18.5.13	Network Isolation		
18.5.14	Network Provider		
18.5.14.1	(L1) Ensure 'Hardened UNC Paths' is set to 'Enabled, with "Require Mutual Authentication" and "Require Integrity" set for all NETLOGON and SYSVOL shares' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.5.15	Offline Files		
18.5.16	QoS Packet Scheduler		
18.5.17	SNMP		
18.5.18	SSL Configuration Settings		
18.5.19	TCPIP Settings		
18.5.19.1	IPv6 Transition Technologies		
18.5.19.2	Parameters		
18.5.19.2.1	(L2) Disable IPv6 (Ensure TCPIP6 Parameter 'DisabledComponents' is set to '0xff (255)' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.5.20	Windows Connect Now		
18.5.20.1	(L2) Ensure 'Configuration of wireless settings using Windows Connect Now' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.5.20.2	(L2) Ensure 'Prohibit access of the Windows Connect Now wizards' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.5.21	Windows Connection Manager		
18.5.21.1	(L1) 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)	<input type="checkbox"/>	<input type="checkbox"/>
18.5.21.2	(L1) Ensure 'Prohibit connection to non-domain networks when connected to domain authenticated network' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.5.22	Wireless Display		
18.5.23	WLAN Service		

Control		Set Correctly	
		Yes	No
18.5.23.1	WLAN Media Cost		
18.5.23.2	WLAN Settings		
18.5.23.2.1	(L1) Ensure 'Allow Windows to automatically connect to suggested open hotspots, to networks shared by contacts, and to hotspots offering paid services' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.6	Printers		
18.6.1	(L1) Ensure 'Allow Print Spooler to accept client connections' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.6.2	(L1) Ensure 'Point and Print Restrictions: When installing drivers for a new connection' is set to 'Enabled: Show warning and elevation prompt' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.6.3	(L1) Ensure 'Point and Print Restrictions: When updating drivers for an existing connection' is set to 'Enabled: Show warning and elevation prompt' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.7	Start Menu and Taskbar		
18.7.1	Notifications		
18.7.1.1	(L2) Ensure 'Turn off notifications network usage' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.8	System		
18.8.1	Access-Denied Assistance		
18.8.2	App-V		
18.8.3	Audit Process Creation		
18.8.3.1	(L1) Ensure 'Include command line in process creation events' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.8.4	Credentials Delegation		
18.8.4.1	(L1) Ensure 'Encryption Oracle Remediation' is set to 'Enabled: Force Updated Clients' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.8.4.2	(L1) Ensure 'Remote host allows delegation of non-exportable credentials' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.8.5	Device Guard		
18.8.5.1	(NG) Ensure 'Turn On Virtualization Based Security' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.8.5.2	(NG) Ensure 'Turn On Virtualization Based Security: Select Platform Security Level' is set to 'Secure Boot and DMA Protection' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.8.5.3	(NG) Ensure 'Turn On Virtualization Based Security: Virtualization Based Protection of Code Integrity' is set to 'Enabled with UEFI lock' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

Control		Set Correctly	
		Yes	No
18.8.5.4	(NG) Ensure 'Turn On Virtualization Based Security: Require UEFI Memory Attributes Table' is set to 'True (checked)' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.8.5.5	(NG) Ensure 'Turn On Virtualization Based Security: Credential Guard Configuration' is set to 'Enabled with UEFI lock' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.8.5.6	(NG) Ensure 'Turn On Virtualization Based Security: Secure Launch Configuration' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.8.6	Device Health Attestation Service		
18.8.7	Device Installation		
18.8.7.1	Device Installation Restrictions		
18.8.7.1.1	(BL) Ensure 'Prevent installation of devices that match any of these device IDs' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.8.7.1.2	(BL) Ensure 'Prevent installation of devices that match any of these device IDs: Prevent installation of devices that match any of these device IDs' is set to 'PCI\CC_0C0A' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.8.7.1.3	(BL) Ensure 'Prevent installation of devices that match any of these device IDs: Also apply to matching devices that are already installed.' is set to 'True' (checked) (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.8.7.1.4	(BL) Ensure 'Prevent installation of devices using drivers that match these device setup classes' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.8.7.1.5	(BL) Ensure 'Prevent installation of devices using drivers that match these device setup classes: Prevent installation of devices using drivers for these device setup' is set to 'IEEE 1394 device setup classes' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.8.7.1.6	(BL) Ensure 'Prevent installation of devices using drivers that match these device setup classes: Also apply to matching devices that are already installed.' is set to 'True' (checked) (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.8.7.2	(L1) Ensure 'Prevent device metadata retrieval from the Internet' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.8.8	Device Redirection		
18.8.9	Disk NV Cache		
18.8.10	Disk Quotas		
18.8.11	Display		
18.8.12	Distributed COM		
18.8.13	Driver Installation		
18.8.14	Early Launch Antimalware		

Control		Set Correctly	
		Yes	No
18.8.14.1	(L1) Ensure 'Boot-Start Driver Initialization Policy' is set to 'Enabled: Good, unknown and bad but critical' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.8.15	Enhanced Storage Access		
18.8.16	File Classification Infrastructure		
18.8.17	File Share Shadow Copy Agent		
18.8.18	File Share Shadow Copy Provider		
18.8.19	Filesystem (formerly NTFS Filesystem)		
18.8.20	Folder Redirection		
18.8.21	Group Policy		
18.8.21.1	Logging and tracing		
18.8.21.2	(L1) Ensure 'Configure registry policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.8.21.3	(L1) Ensure 'Configure registry policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.8.21.4	(L1) Ensure 'Continue experiences on this device' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.8.21.5	(L1) Ensure 'Turn off background refresh of Group Policy' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.8.22	Internet Communication Management		
18.8.22.1	Internet Communication settings		
18.8.22.1.1	(L2) Ensure 'Turn off access to the Store' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.8.22.1.2	(L1) Ensure 'Turn off downloading of print drivers over HTTP' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.8.22.1.3	(L2) Ensure 'Turn off handwriting personalization data sharing' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.8.22.1.4	(L2) Ensure 'Turn off handwriting recognition error reporting' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.8.22.1.5	(L2) Ensure 'Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.8.22.1.6	(L1) Ensure 'Turn off Internet download for Web publishing and online ordering wizards' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.8.22.1.7	(L2) Ensure 'Turn off printing over HTTP' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.8.22.1.8	(L2) Ensure 'Turn off Registration if URL connection is referring to Microsoft.com' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.8.22.1.9	(L2) Ensure 'Turn off Search Companion content file updates' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

Control		Set Correctly	
		Yes	No
18.8.22.1.10	(L2) Ensure 'Turn off the "Order Prints" picture task' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.8.22.1.11	(L2) Ensure 'Turn off the "Publish to Web" task for files and folders' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.8.22.1.12	(L2) Ensure 'Turn off the Windows Messenger Customer Experience Improvement Program' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.8.22.1.13	(L2) Ensure 'Turn off Windows Customer Experience Improvement Program' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.8.22.1.14	(L2) Ensure 'Turn off Windows Error Reporting' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.8.23	iSCSI		
18.8.24	KDC		
18.8.25	Kerberos		
18.8.25.1	(L2) Ensure 'Support device authentication using certificate' is set to 'Enabled: Automatic' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.8.26	Kernel DMA Protection		
18.8.26.1	(BL) Ensure 'Enumeration policy for external devices incompatible with Kernel DMA Protection' is set to 'Enabled: Block All' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.8.27	Locale Services		
18.8.27.1	(L2) Ensure 'Disallow copying of user input methods to the system account for sign-in' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.8.28	Logon		
18.8.28.1	(L1) Ensure 'Block user from showing account details on sign-in' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.8.28.2	(L1) Ensure 'Do not display network selection UI' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.8.28.3	(L1) Ensure 'Do not enumerate connected users on domain-joined computers' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.8.28.4	(L1) Ensure 'Enumerate local users on domain-joined computers' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.8.28.5	(L1) Ensure 'Turn off app notifications on the lock screen' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.8.28.6	(L1) Ensure 'Turn off picture password sign-in' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.8.28.7	(L1) Ensure 'Turn on convenience PIN sign-in' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.8.29	Mitigation Options		
18.8.30	Net Logon		
18.8.31	OS Policies		

Control		Set Correctly	
		Yes	No
18.8.31.1	(L2) Ensure 'Allow Clipboard synchronization across devices' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.8.31.2	(L2) Ensure 'Allow upload of User Activities' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.8.32	Performance Control Panel		
18.8.33	PIN Complexity		
18.8.34	Power Management		
18.8.34.1	Button Settings		
18.8.34.2	Energy Saver Settings		
18.8.34.3	Hard Disk Settings		
18.8.34.4	Notification Settings		
18.8.34.5	Power Throttling Settings		
18.8.34.6	Sleep Settings		
18.8.34.6.1	(L1) Ensure 'Allow network connectivity during connected-standby (on battery)' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.8.34.6.2	(L1) Ensure 'Allow network connectivity during connected-standby (plugged in)' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.8.34.6.3	(BL) Ensure 'Allow standby states (S1-S3) when sleeping (on battery)' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.8.34.6.4	(BL) Ensure 'Allow standby states (S1-S3) when sleeping (plugged in)' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.8.34.6.5	(L1) Ensure 'Require a password when a computer wakes (on battery)' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.8.34.6.6	(L1) Ensure 'Require a password when a computer wakes (plugged in)' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.8.35	Recovery		
18.8.36	Remote Assistance		
18.8.36.1	(L1) Ensure 'Configure Offer Remote Assistance' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.8.36.2	(L1) Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.8.37	Remote Procedure Call		
18.8.37.1	(L1) Ensure 'Enable RPC Endpoint Mapper Client Authentication' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.8.37.2	(L1) Ensure 'Restrict Unauthenticated RPC clients' is set to 'Enabled: Authenticated' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.8.38	Removable Storage Access		
18.8.39	Scripts		
18.8.40	Security Account Manager		
18.8.41	Server Manager		

Control		Set Correctly	
		Yes	No
18.8.42	Service Control Manager Settings		
18.8.43	Shutdown		
18.8.44	Shutdown Options		
18.8.45	Storage Health		
18.8.46	Storage Sense		
18.8.47	System Restore		
18.8.48	Troubleshooting and Diagnostics		
18.8.48.1	Application Compatibility Diagnostics		
18.8.48.2	Corrupted File Recovery		
18.8.48.3	Disk Diagnostic		
18.8.48.4	Fault Tolerant Heap		
18.8.48.5	Microsoft Support Diagnostic Tool		
18.8.48.5.1	(L2) Ensure 'Microsoft Support Diagnostic Tool: Turn on MSDT interactive communication with support provider' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.8.48.6	MSI Corrupted File Recovery		
18.8.48.7	Scheduled Maintenance		
18.8.48.8	Scripted Diagnostics		
18.8.48.9	Windows Boot Performance Diagnostics		
18.8.48.10	Windows Memory Leak Diagnosis		
18.8.48.11	Windows Performance PerfTrack		
18.8.48.11.1	(L2) Ensure 'Enable/Disable PerfTrack' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.8.49	Trusted Platform Module Services		
18.8.50	User Profiles		
18.8.50.1	(L2) Ensure 'Turn off the advertising ID' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.8.51	Windows File Protection		
18.8.52	Windows HotStart		
18.8.53	Windows Time Service		
18.8.53.1	Time Providers		
18.8.53.1.1	(L2) Ensure 'Enable Windows NTP Client' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.8.53.1.2	(L2) Ensure 'Enable Windows NTP Server' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9	Windows Components		
18.9.1	Active Directory Federation Services		
18.9.2	ActiveX Installer Service		
18.9.3	Add features to Windows 8 / 8.1 / 10 (formerly Windows Anytime Upgrade)		

Control		Set Correctly	
		Yes	No
18.9.4	App Package Deployment		
18.9.4.1	(L2) Ensure 'Allow a Windows app to share application data between users' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.4.2	(L1) Ensure 'Prevent non-admin users from installing packaged Windows apps' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.5	App Privacy		
18.9.5.1	(L1) Ensure 'Let Windows apps activate with voice while the system is locked' is set to 'Enabled: Force Deny' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.6	App runtime		
18.9.6.1	(L1) Ensure 'Allow Microsoft accounts to be optional' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.6.2	(L2) Ensure 'Block launching Universal Windows apps with Windows Runtime API access from hosted content.' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.7	Application Compatibility		
18.9.8	AutoPlay Policies		
18.9.8.1	(L1) Ensure 'Disallow Autoplay for non-volume devices' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.8.2	(L1) Ensure 'Set the default behavior for AutoRun' is set to 'Enabled: Do not execute any autorun commands' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.8.3	(L1) Ensure 'Turn off Autoplay' is set to 'Enabled: All drives' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.9	Backup		
18.9.10	Biometrics		
18.9.10.1	Facial Features		
18.9.10.1.1	(L1) Ensure 'Configure enhanced anti-spoofing' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.11	BitLocker Drive Encryption		
18.9.11.1	Fixed Data Drives		
18.9.11.1.1	(BL) Ensure 'Allow access to BitLocker-protected fixed data drives from earlier versions of Windows' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.11.1.2	(BL) Ensure 'Choose how BitLocker-protected fixed drives can be recovered' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.11.1.3	(BL) Ensure 'Choose how BitLocker-protected fixed drives can be recovered: Allow data recovery agent' is set to 'Enabled: True' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

Control		Set Correctly	
		Yes	No
18.9.11.1.4	(BL) Ensure 'Choose how BitLocker-protected fixed drives can be recovered: Recovery Password' is set to 'Enabled: Allow 48-digit recovery password' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.11.1.5	(BL) Ensure 'Choose how BitLocker-protected fixed drives can be recovered: Recovery Key' is set to 'Enabled: Allow 256-bit recovery key' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.11.1.6	(BL) Ensure 'Choose how BitLocker-protected fixed drives can be recovered: Omit recovery options from the BitLocker setup wizard' is set to 'Enabled: True' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.11.1.7	(BL) Ensure 'Choose how BitLocker-protected fixed drives can be recovered: Save BitLocker recovery information to AD DS for fixed data drives' is set to 'Enabled: False' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.11.1.8	(BL) Ensure 'Choose how BitLocker-protected fixed drives can be recovered: Configure storage of BitLocker recovery information to AD DS' is set to 'Enabled: Backup recovery passwords and key packages' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.11.1.9	(BL) Ensure 'Choose how BitLocker-protected fixed drives can be recovered: Do not enable BitLocker until recovery information is stored to AD DS for fixed data drives' is set to 'Enabled: False' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.11.1.10	(BL) Ensure 'Configure use of hardware-based encryption for fixed data drives' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.11.1.11	(BL) Ensure 'Configure use of passwords for fixed data drives' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.11.1.12	(BL) Ensure 'Configure use of smart cards on fixed data drives' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.11.1.13	(BL) Ensure 'Configure use of smart cards on fixed data drives: Require use of smart cards on fixed data drives' is set to 'Enabled: True' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.11.2	Operating System Drives		
18.9.11.2.1	(BL) Ensure 'Allow enhanced PINs for startup' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.11.2.2	(BL) Ensure 'Allow Secure Boot for integrity validation' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.11.2.3	(BL) Ensure 'Choose how BitLocker-protected operating system drives can be recovered' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.11.2.4	(BL) Ensure 'Choose how BitLocker-protected operating system drives can be recovered: Allow data recovery agent' is set to 'Enabled: False' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

Control		Set Correctly	
		Yes	No
18.9.11.2.5	(BL) Ensure 'Choose how BitLocker-protected operating system drives can be recovered: Recovery Password' is set to 'Enabled: Require 48-digit recovery password' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.11.2.6	(BL) Ensure 'Choose how BitLocker-protected operating system drives can be recovered: Recovery Key' is set to 'Enabled: Do not allow 256-bit recovery key' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.11.2.7	(BL) Ensure 'Choose how BitLocker-protected operating system drives can be recovered: Omit recovery options from the BitLocker setup wizard' is set to 'Enabled: True' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.11.2.8	(BL) Ensure 'Choose how BitLocker-protected operating system drives can be recovered: Save BitLocker recovery information to AD DS for operating system drives' is set to 'Enabled: True' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.11.2.9	(BL) Ensure 'Choose how BitLocker-protected operating system drives can be recovered: Configure storage of BitLocker recovery information to AD DS:' is set to 'Enabled: Store recovery passwords and key packages' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.11.2.10	(BL) Ensure 'Choose how BitLocker-protected operating system drives can be recovered: Do not enable BitLocker until recovery information is stored to AD DS for operating system drives' is set to 'Enabled: True' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.11.2.11	(BL) Ensure 'Configure use of hardware-based encryption for operating system drives' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.11.2.12	(BL) Ensure 'Configure use of passwords for operating system drives' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.11.2.13	(BL) Ensure 'Require additional authentication at startup' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.11.2.14	(BL) Ensure 'Require additional authentication at startup: Allow BitLocker without a compatible TPM' is set to 'Enabled: False' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.11.3	Removable Data Drives		
18.9.11.3.1	(BL) Ensure 'Allow access to BitLocker-protected removable data drives from earlier versions of Windows' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.11.3.2	(BL) Ensure 'Choose how BitLocker-protected removable drives can be recovered' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.11.3.3	(BL) Ensure 'Choose how BitLocker-protected removable drives can be recovered: Allow data recovery agent' is set to 'Enabled: True' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

Control		Set Correctly	
		Yes	No
18.9.11.3.4	(BL) Ensure 'Choose how BitLocker-protected removable drives can be recovered: Recovery Password' is set to 'Enabled: Do not allow 48-digit recovery password' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.11.3.5	(BL) Ensure 'Choose how BitLocker-protected removable drives can be recovered: Recovery Key' is set to 'Enabled: Do not allow 256-bit recovery key' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.11.3.6	(BL) Ensure 'Choose how BitLocker-protected removable drives can be recovered: Omit recovery options from the BitLocker setup wizard' is set to 'Enabled: True' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.11.3.7	(BL) Ensure 'Choose how BitLocker-protected removable drives can be recovered: Save BitLocker recovery information to AD DS for removable data drives' is set to 'Enabled: False' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.11.3.8	(BL) Ensure 'Choose how BitLocker-protected removable drives can be recovered: Configure storage of BitLocker recovery information to AD DS:' is set to 'Enabled: Backup recovery passwords and key packages' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.11.3.9	(BL) Ensure 'Choose how BitLocker-protected removable drives can be recovered: Do not enable BitLocker until recovery information is stored to AD DS for removable data drives' is set to 'Enabled: False' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.11.3.10	(BL) Ensure 'Configure use of hardware-based encryption for removable data drives' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.11.3.11	(BL) Ensure 'Configure use of passwords for removable data drives' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.11.3.12	(BL) Ensure 'Configure use of smart cards on removable data drives' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.11.3.13	(BL) Ensure 'Configure use of smart cards on removable data drives: Require use of smart cards on removable data drives' is set to 'Enabled: True' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.11.3.14	(BL) Ensure 'Deny write access to removable drives not protected by BitLocker' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.11.3.15	(BL) Ensure 'Deny write access to removable drives not protected by BitLocker: Do not allow write access to devices configured in another organization' is set to 'Enabled: False' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.11.4	(BL) Ensure 'Disable new DMA devices when this computer is locked' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.12	Camera		

Control		Set Correctly	
		Yes	No
18.9.12.1	(L2) Ensure 'Allow Use of Camera' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.13	Chat		
18.9.14	Cloud Content		
18.9.14.1	(L1) Ensure 'Turn off cloud consumer account state content' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.14.2	(L2) Ensure 'Turn off cloud optimized content' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.14.3	(L1) Ensure 'Turn off Microsoft consumer experiences' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.15	Connect		
18.9.15.1	(L1) Ensure 'Require pin for pairing' is set to 'Enabled: First Time' OR 'Enabled: Always' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.16	Credential User Interface		
18.9.16.1	(L1) Ensure 'Do not display the password reveal button' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.16.2	(L1) Ensure 'Enumerate administrator accounts on elevation' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.16.3	(L1) Ensure 'Prevent the use of security questions for local accounts' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.17	Data Collection and Preview Builds		
18.9.17.1	(L1) Ensure 'Allow Diagnostic Data' is set to 'Enabled: Diagnostic data off (not recommended)' or 'Enabled: Send required diagnostic data' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.17.2	(L2) Ensure 'Configure Authenticated Proxy usage for the Connected User Experience and Telemetry service' is set to 'Enabled: Disable Authenticated Proxy usage' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.17.3	(L1) Ensure 'Disable OneSettings Downloads' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.17.4	(L1) Ensure 'Do not show feedback notifications' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.17.5	(L1) Ensure 'Enable OneSettings Auditing' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.17.6	(L1) Ensure 'Limit Diagnostic Log Collection' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.17.7	(L1) Ensure 'Limit Dump Collection' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.17.8	(L1) Ensure 'Toggle user control over Insider builds' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.18	Delivery Optimization		

Control		Set Correctly	
		Yes	No
18.9.18.1	(L1) Ensure 'Download Mode' is NOT set to 'Enabled: Internet' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.19	Desktop Gadgets		
18.9.20	Desktop Window Manager		
18.9.21	Device and Driver Compatibility		
18.9.22	Device Registration (formerly Workplace Join)		
18.9.23	Digital Locker		
18.9.24	Edge UI		
18.9.25	EMET		
18.9.26	Event Forwarding		
18.9.27	Event Log Service		
18.9.27.1	Application		
18.9.27.1.1	(L1) Ensure 'Application: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.27.1.2	(L1) Ensure 'Application: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.27.2	Security		
18.9.27.2.1	(L1) Ensure 'Security: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.27.2.2	(L1) Ensure 'Security: Specify the maximum log file size (KB)' is set to 'Enabled: 196,608 or greater' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.27.3	Setup		
18.9.27.3.1	(L1) Ensure 'Setup: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.27.3.2	(L1) Ensure 'Setup: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.27.4	System		
18.9.27.4.1	(L1) Ensure 'System: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.27.4.2	(L1) Ensure 'System: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.28	Event Logging		
18.9.29	Event Viewer		
18.9.30	Family Safety (formerly Parental Controls)		
18.9.31	File Explorer (formerly Windows Explorer)		
18.9.31.1	Previous Versions		

Control		Set Correctly	
		Yes	No
18.9.31.2	(L1) Ensure 'Turn off Data Execution Prevention for Explorer' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.31.3	(L1) Ensure 'Turn off heap termination on corruption' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.31.4	(L1) Ensure 'Turn off shell protocol protected mode' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.32	File History		
18.9.33	Find My Device		
18.9.34	Game Explorer		
18.9.35	Handwriting		
18.9.36	HomeGroup		
18.9.36.1	(L1) Ensure 'Prevent the computer from joining a homegroup' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.37	Human Presence		
18.9.38	Import Video		
18.9.39	Internet Explorer		
18.9.40	Internet Information Services		
18.9.41	Location and Sensors		
18.9.41.1	(L2) Ensure 'Turn off location' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.42	Maintenance Scheduler		
18.9.43	Maps		
18.9.44	MDM		
18.9.45	Messaging		
18.9.45.1	(L2) Ensure 'Allow Message Service Cloud Sync' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.46	Microsoft account		
18.9.46.1	(L1) Ensure 'Block all consumer Microsoft account user authentication' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.47	Microsoft Defender Antivirus (formerly Windows Defender and Windows Defender Antivirus)		
18.9.47.1	Client Interface		
18.9.47.2	Device Control		
18.9.47.3	Exclusions		
18.9.47.4	MAPS		
18.9.47.4.1	(L1) Ensure 'Configure local setting override for reporting to Microsoft MAPS' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.47.4.2	(L2) Ensure 'Join Microsoft MAPS' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

Control		Set Correctly	
		Yes	No
18.9.47.5	Microsoft Defender Exploit Guard (formerly Windows Defender Exploit Guard)		
18.9.47.5.1	Attack Surface Reduction		
18.9.47.5.1.1	(L1) Ensure 'Configure Attack Surface Reduction rules' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.47.5.1.2	(L1) Ensure 'Configure Attack Surface Reduction rules: Set the state for each ASR rule' is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.47.5.2	Controlled Folder Access		
18.9.47.5.3	Network Protection		
18.9.47.5.3.1	(L1) Ensure 'Prevent users and apps from accessing dangerous websites' is set to 'Enabled: Block' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.47.6	MpEngine		
18.9.47.6.1	(L2) Ensure 'Enable file hash computation feature' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.47.7	Network Inspection System		
18.9.47.8	Quarantine		
18.9.47.9	Real-time Protection		
18.9.47.9.1	(L1) Ensure 'Scan all downloaded files and attachments' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.47.9.2	(L1) Ensure 'Turn off real-time protection' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.47.9.3	(L1) Ensure 'Turn on behavior monitoring' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.47.9.4	(L1) Ensure 'Turn on script scanning' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.47.10	Remediation		
18.9.47.11	Reporting		
18.9.47.11.1	(L2) Ensure 'Configure Watson events' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.47.12	Scan		
18.9.47.12.1	(L1) Ensure 'Scan removable drives' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.47.12.2	(L1) Ensure 'Turn on e-mail scanning' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.47.13	Security Intelligence Updates (formerly Signature Updates)		
18.9.47.14	Threats		
18.9.47.15	(L1) Ensure 'Configure detection for potentially unwanted applications' is set to 'Enabled: Block' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.47.16	(L1) Ensure 'Turn off Microsoft Defender AntiVirus' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

Control		Set Correctly	
		Yes	No
18.9.48	Microsoft Defender Application Guard (formerly Windows Defender Application Guard)		
18.9.48.1	(NG) Ensure 'Allow auditing events in Microsoft Defender Application Guard' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.48.2	(NG) Ensure 'Allow camera and microphone access in Microsoft Defender Application Guard' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.48.3	(NG) Ensure 'Allow data persistence for Microsoft Defender Application Guard' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.48.4	(NG) Ensure 'Allow files to download and save to the host operating system from Microsoft Defender Application Guard' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.48.5	(NG) Ensure 'Configure Microsoft Defender Application Guard clipboard settings: Clipboard behavior setting' is set to 'Enabled: Enable clipboard operation from an isolated session to the host' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.48.6	(NG) Ensure 'Turn on Microsoft Defender Application Guard in Managed Mode' is set to 'Enabled: 1' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.49	Microsoft Defender Exploit Guard (formerly Windows Defender Exploit Guard)		
18.9.50	Microsoft Edge		
18.9.51	Microsoft FIDO Authentication		
18.9.52	Microsoft Secondary Authentication Factor		
18.9.53	Microsoft User Experience Virtualization		
18.9.54	NetMeeting		
18.9.55	Network Access Protection		
18.9.56	Network Projector		
18.9.57	News and interests		
18.9.57.1	(L2) Ensure 'Enable news and interests on the taskbar' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.58	OneDrive (formerly SkyDrive)		
18.9.58.1	(L1) Ensure 'Prevent the usage of OneDrive for file storage' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.59	Online Assistance		
18.9.60	OOBE		
18.9.61	Password Synchronization		
18.9.62	Portable Operating System		
18.9.63	Presentation Settings		
18.9.64	Push To Install		

Control		Set Correctly	
		Yes	No
18.9.64.1	(L2) Ensure 'Turn off Push To Install service' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.65	Remote Desktop Services (formerly Terminal Services)		
18.9.65.1	RD Licensing (formerly TS Licensing)		
18.9.65.2	Remote Desktop Connection Client		
18.9.65.2.1	RemoteFX USB Device Redirection		
18.9.65.2.2	(L1) Ensure 'Do not allow passwords to be saved' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.65.3	Remote Desktop Session Host (formerly Terminal Server)		
18.9.65.3.1	Application Compatibility		
18.9.65.3.2	Connections		
18.9.65.3.2.1	(L2) Ensure 'Allow users to connect remotely by using Remote Desktop Services' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.65.3.3	Device and Resource Redirection		
18.9.65.3.3.1	(L2) Ensure 'Allow UI Automation redirection' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.65.3.3.2	(L2) Ensure 'Do not allow COM port redirection' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.65.3.3.3	(L1) Ensure 'Do not allow drive redirection' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.65.3.3.4	(L2) Ensure 'Do not allow location redirection' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.65.3.3.5	(L2) Ensure 'Do not allow LPT port redirection' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.65.3.3.6	(L2) Ensure 'Do not allow supported Plug and Play device redirection' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.65.3.4	Licensing		
18.9.65.3.5	Printer Redirection		
18.9.65.3.6	Profiles		
18.9.65.3.7	RD Connection Broker (formerly TS Connection Broker)		
18.9.65.3.8	Remote Session Environment		
18.9.65.3.9	Security		
18.9.65.3.9.1	(L1) Ensure 'Always prompt for password upon connection' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.65.3.9.2	(L1) Ensure 'Require secure RPC communication' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.65.3.9.3	(L1) Ensure 'Require use of specific security layer for remote (RDP) connections' is set to 'Enabled: SSL' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

Control		Set Correctly	
		Yes	No
18.9.65.3.9.4	(L1) Ensure 'Require user authentication for remote connections by using Network Level Authentication' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.65.3.9.5	(L1) Ensure 'Set client connection encryption level' is set to 'Enabled: High Level' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.65.3.10	Session Time Limits		
18.9.65.3.10.1	(L2) 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)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.65.3.10.2	(L2) Ensure 'Set time limit for disconnected sessions' is set to 'Enabled: 1 minute' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.65.3.11	Temporary folders		
18.9.65.3.11.1	(L1) Ensure 'Do not delete temp folders upon exit' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.66	RSS Feeds		
18.9.66.1	(L1) Ensure 'Prevent downloading of enclosures' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.67	Search		
18.9.67.1	OCR		
18.9.67.2	(L2) Ensure 'Allow Cloud Search' is set to 'Enabled: Disable Cloud Search' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.67.3	(L1) Ensure 'Allow Cortana' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.67.4	(L1) Ensure 'Allow Cortana above lock screen' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.67.5	(L1) Ensure 'Allow indexing of encrypted files' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.67.6	(L1) Ensure 'Allow search and Cortana to use location' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.68	Security Center		
18.9.69	Server for NIS		
18.9.70	Shutdown Options		
18.9.71	Smart Card		
18.9.72	Software Protection Platform		
18.9.72.1	(L2) Ensure 'Turn off KMS Client Online AVS Validation' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.73	Sound Recorder		
18.9.74	Speech		
18.9.75	Store		
18.9.75.1	(L2) Ensure 'Disable all apps from Microsoft Store' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

Control		Set Correctly	
		Yes	No
18.9.75.2	(L1) Ensure 'Only display the private store within the Microsoft Store' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.75.3	(L1) Ensure 'Turn off Automatic Download and Install of updates' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.75.4	(L1) Ensure 'Turn off the offer to update to the latest version of Windows' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.75.5	(L2) Ensure 'Turn off the Store application' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.76	Sync your settings		
18.9.77	Tablet PC		
18.9.78	Task Scheduler		
18.9.79	Tenant Restrictions		
18.9.80	Text Input		
18.9.81	Widgets		
18.9.81.1	(L1) Ensure 'Allow widgets' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.82	Windows Calendar		
18.9.83	Windows Color System		
18.9.84	Windows Customer Experience Improvement Program		
18.9.85	Windows Defender SmartScreen		
18.9.85.1	Explorer		
18.9.85.1.1	(L1) Ensure 'Configure Windows Defender SmartScreen' is set to 'Enabled: Warn and prevent bypass' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.85.2	Microsoft Edge		
18.9.85.2.1	(L1) Ensure 'Configure Windows Defender SmartScreen' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.85.2.2	(L1) Ensure 'Prevent bypassing Windows Defender SmartScreen prompts for sites' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.86	Windows Error Reporting		
18.9.87	Windows Game Recording and Broadcasting		
18.9.87.1	(L1) Ensure 'Enables or disables Windows Game Recording and Broadcasting' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.88	Windows Hello for Business (formerly Microsoft Passport for Work)		
18.9.89	Windows Ink Workspace		
18.9.89.1	(L2) Ensure 'Allow suggested apps in Windows Ink Workspace' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.89.2	(L1) Ensure 'Allow Windows Ink Workspace' is set to 'Enabled: On, but disallow access above lock' OR 'Disabled' but not 'Enabled: On' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

Control		Set Correctly	
		Yes	No
18.9.90	Windows Installer		
18.9.90.1	(L1) Ensure 'Allow user control over installs' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.90.2	(L1) Ensure 'Always install with elevated privileges' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.90.3	(L2) Ensure 'Prevent Internet Explorer security prompt for Windows Installer scripts' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.91	Windows Logon Options		
18.9.91.1	(L1) Ensure 'Sign-in and lock last interactive user automatically after a restart' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.92	Windows Mail		
18.9.93	Windows Media Center		
18.9.94	Windows Media Digital Rights Management		
18.9.95	Windows Media Player		
18.9.96	Windows Meeting Space		
18.9.97	Windows Messenger		
18.9.98	Windows Mobility Center		
18.9.99	Windows Movie Maker		
18.9.100	Windows PowerShell		
18.9.100.1	(L1) Ensure 'Turn on PowerShell Script Block Logging' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.100.2	(L1) Ensure 'Turn on PowerShell Transcription' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.101	Windows Reliability Analysis		
18.9.102	Windows Remote Management (WinRM)		
18.9.102.1	WinRM Client		
18.9.102.1.1	(L1) Ensure 'Allow Basic authentication' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.102.1.2	(L1) Ensure 'Allow unencrypted traffic' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.102.1.3	(L1) Ensure 'Disallow Digest authentication' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.102.2	WinRM Service		
18.9.102.2.1	(L1) Ensure 'Allow Basic authentication' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.102.2.2	(L2) Ensure 'Allow remote server management through WinRM' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.102.2.3	(L1) Ensure 'Allow unencrypted traffic' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

Control		Set Correctly	
		Yes	No
18.9.102.2.4	(L1) Ensure 'Disallow WinRM from storing RunAs credentials' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.103	Windows Remote Shell		
18.9.103.1	(L2) Ensure 'Allow Remote Shell Access' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.104	Windows Sandbox		
18.9.104.1	(L1) Ensure 'Allow clipboard sharing with Windows Sandbox' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.104.2	(L1) Ensure 'Allow networking in Windows Sandbox' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.105	Windows Security (formerly Windows Defender Security Center)		
18.9.105.1	Account protection		
18.9.105.2	App and browser protection		
18.9.105.2.1	(L1) Ensure 'Prevent users from modifying settings' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.106	Windows SideShow		
18.9.107	Windows System Resource Manager		
18.9.108	Windows Update		
18.9.108.1	Legacy Policies		
18.9.108.1.1	(L1) Ensure 'No auto-restart with logged on users for scheduled automatic updates installations' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.108.2	Manage end user experience		
18.9.108.2.1	(L1) Ensure 'Configure Automatic Updates' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.108.2.2	(L1) Ensure 'Configure Automatic Updates: Scheduled install day' is set to '0 - Every day' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.108.2.3	(L1) Ensure 'Remove access to "Pause updates" feature' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.108.3	Manage updates offered from Windows Server Update Service		
18.9.108.4	Manage updates offered from Windows Update (formerly Defer Windows Updates and Windows Update for Business)		
18.9.108.4.1	(L1) Ensure 'Manage preview builds' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.108.4.2	(L1) Ensure 'Select when Preview Builds and Feature Updates are received' is set to 'Enabled: 180 or more days' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18.9.108.4.3	(L1) Ensure 'Select when Quality Updates are received' is set to 'Enabled: 0 days' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
19	Administrative Templates (User)		

Control		Set Correctly	
		Yes	No
19.1	Control Panel		
19.1.1	Add or Remove Programs		
19.1.2	Display		
19.1.3	Personalization (formerly Desktop Themes)		
19.1.3.1	(L1) Ensure 'Enable screen saver' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
19.1.3.2	(L1) Ensure 'Password protect the screen saver' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
19.1.3.3	(L1) Ensure 'Screen saver timeout' is set to 'Enabled: 900 seconds or fewer, but not 0' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
19.2	Desktop		
19.3	Network		
19.4	Shared Folders		
19.5	Start Menu and Taskbar		
19.5.1	Notifications		
19.5.1.1	(L1) Ensure 'Turn off toast notifications on the lock screen' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
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	(L2) Ensure 'Turn off Help Experience Improvement Program' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
19.7	Windows Components		
19.7.1	Add features to Windows 8 / 8.1 / 10 (formerly Windows Anytime Upgrade)		
19.7.2	App runtime		
19.7.3	Application Compatibility		
19.7.4	Attachment Manager		
19.7.4.1	(L1) Ensure 'Do not preserve zone information in file attachments' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
19.7.4.2	(L1) Ensure 'Notify antivirus programs when opening attachments' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
19.7.5	AutoPlay Policies		
19.7.6	Backup		
19.7.7	Calculator		

Control		Set Correctly	
		Yes	No
19.7.8	Cloud Content		
19.7.8.1	(L1) Ensure 'Configure Windows spotlight on lock screen' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
19.7.8.2	(L1) Ensure 'Do not suggest third-party content in Windows spotlight' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
19.7.8.3	(L2) Ensure 'Do not use diagnostic data for tailored experiences' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
19.7.8.4	(L2) Ensure 'Turn off all Windows spotlight features' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
19.7.8.5	(L1) Ensure 'Turn off Spotlight collection on Desktop' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
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		
19.7.17	IME		
19.7.18	Import Video		
19.7.19	Instant Search		
19.7.20	Internet Explorer		
19.7.21	Location and Sensors		
19.7.22	Microsoft Edge		
19.7.23	Microsoft Management Console		
19.7.24	Microsoft User Experience Virtualization		
19.7.25	Multitasking		
19.7.26	NetMeeting		
19.7.27	Network Projector		
19.7.28	Network Sharing		
19.7.28.1	(L1) Ensure 'Prevent users from sharing files within their profile.' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
19.7.29	OOBE		
19.7.30	Presentation Settings		
19.7.31	Remote Desktop Services (formerly Terminal Services)		
19.7.32	RSS Feeds		
19.7.33	Search		
19.7.34	Sound Recorder		
19.7.35	Store		

Control		Set Correctly	
		Yes	No
19.7.36	Tablet PC		
19.7.37	Task Scheduler		
19.7.38	Windows Calendar		
19.7.39	Windows Color System		
19.7.40	Windows Defender SmartScreen		
19.7.41	Windows Error Reporting		
19.7.42	Windows Hello for Business (formerly Microsoft Passport for Work)		
19.7.43	Windows Installer		
19.7.43.1	(L1) Ensure 'Always install with elevated privileges' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
19.7.44	Windows Logon Options		
19.7.45	Windows Mail		
19.7.46	Windows Media Center		
19.7.47	Windows Media Player		
19.7.47.1	Networking		
19.7.47.2	Playback		
19.7.47.2.1	(L2) Ensure 'Prevent Codec Download' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: Change History

Date	Version	Changes for this version
02/14/2022	1.0.0	Initial Public Release