



CIS Microsoft Intune for Windows 10 Benchmark

v3.0.1 - 03-01-2024

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 |
| Table of Contents..... | 2 |
| Overview..... | 22 |
| Intended Audience..... | 22 |
| Consensus Guidance | 23 |
| Typographical Conventions..... | 24 |
| Recommendation Definitions..... | 25 |
| Title | 25 |
| Assessment Status..... | 25 |
| Automated | 25 |
| Manual..... | 25 |
| Profile | 25 |
| Description..... | 25 |
| Rationale Statement | 25 |
| Impact Statement..... | 26 |
| Audit Procedure..... | 26 |
| Remediation Procedure..... | 26 |
| Default Value..... | 26 |
| References | 26 |
| CIS Critical Security Controls® (CIS Controls®)..... | 26 |
| Additional Information..... | 26 |
| Profile Definitions..... | 27 |
| Acknowledgements | 28 |
| Recommendations | 29 |
| 1 Above Lock | 29 |
| 1.1 (L1) Ensure 'Allow Cortana Above Lock' is set to 'Block' (Automated)..... | 30 |
| 2 Accounts | 32 |
| 3 Administrative Templates | 32 |
| 3.1 Control Panel..... | 32 |
| 3.1.1 Add or Remove Programs..... | 32 |
| 3.1.2 Display..... | 32 |
| 3.1.3 Personalization..... | 32 |
| 3.1.3.1 (L1) Ensure 'Enable screen saver (User)' is set to 'Enabled' (Automated)..... | 33 |
| 3.1.3.2 (L1) Ensure 'Prevent enabling lock screen camera' is set to 'Enabled' (Automated) ... | 35 |
| 3.1.3.3 (L1) Ensure 'Prevent enabling lock screen slide show' is set to 'Enabled' (Automated) | |
| | 37 |

| | |
|---|-----------|
| 3.1.4 Printers | 39 |
| 3.1.5 Programs..... | 39 |
| 3.1.6 Regional and Language Options | 39 |
| 3.1.6.1 Handwriting personalization | 39 |
| 3.1.7 User Account | 39 |
| 3.2 Desktop | 39 |
| 3.3 LAPS (legacy)..... | 39 |
| 3.4 MS Security Guide | 39 |
| 3.4.1 (L1) Ensure 'Apply UAC restrictions to local accounts on network logons' is set to 'Enabled' (Automated)..... | 40 |
| 3.4.2 (L1) Ensure 'Configure SMB v1 client driver' is set to 'Enabled: Disable driver (recommended)' (Automated)..... | 42 |
| 3.4.3 (L1) Ensure 'Configure SMB v1 server' is set to 'Disabled' (Automated) | 44 |
| 3.4.4 (L1) Ensure 'Enable Structured Exception Handling Overwrite Protection (SEHOP)' is set to 'Enabled' (Automated)..... | 46 |
| 3.4.5 (L1) Ensure 'WDigest Authentication' is set to 'Disabled' (Automated) | 48 |
| 3.5 MSS (Legacy) | 50 |
| 3.5.1 (L1) Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled' (Automated) | 51 |
| 3.5.2 (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)..... | 53 |
| 3.5.3 (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) | 55 |
| 3.5.4 (L2) Ensure 'MSS: (DisableSavePassword) Prevent the dial-up password from being saved (recommended)' is set to 'Enabled' (Automated) | 57 |
| 3.5.5 (L1) Ensure 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' is set to 'Disabled' (Automated) | 59 |
| 3.5.6 (L2) Ensure 'MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds' is set to 'Enabled: 300,000 or 5 minutes (recommended)' (Automated) | 61 |
| 3.5.7 (L1) Ensure 'MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers' is set to 'Enabled' (Automated) | 63 |
| 3.5.8 (L2) Ensure 'MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)' is set to 'Disabled' (Automated) | 65 |
| 3.5.9 (L1) Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' is set to 'Enabled' (Automated) | 67 |
| 3.5.10 (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) | 69 |
| 3.5.11 (L2) Ensure 'MSS: (TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted' is set to 'Enabled: 3' (Automated) | 71 |
| 3.5.12 (L2) Ensure 'MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted' is set to 'Enabled: 3' (Automated) | 73 |
| 3.5.13 (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)..... | 75 |
| 3.6 Network | 77 |
| 3.6.1 Background Intelligent Transfer Service (BITS) | 77 |
| 3.6.2 BranchCache | 77 |
| 3.6.3 DirectAccess Client Experience Settings | 77 |
| 3.6.4 DNS Client..... | 77 |
| 3.6.4.1 (L1) Ensure 'Turn off multicast name resolution' is set to 'Enabled' (Automated) | 78 |
| 3.6.5 Hotspot Authentication | 80 |
| 3.6.6 Lanman Server | 80 |
| 3.6.7 Lanman Workstation..... | 80 |
| 3.6.8 Link-Layer Topology Discovery..... | 80 |

| | |
|--|------------|
| 3.6.8.1 (L2) Ensure 'Turn on Mapper I/O (LLTDIO) driver' is set to 'Disabled' (Automated) | 81 |
| 3.6.8.2 (L2) Ensure 'Turn on Responder (RSPNDR) driver' is set to 'Disabled' (Automated) .. | 83 |
| 3.6.9 Network Connections | 85 |
| 3.6.9.1 (L1) Ensure 'Prohibit installation and configuration of Network Bridge on your DNS domain network' is set to 'Enabled' (Automated) | 86 |
| 3.6.9.2 (L1) Ensure 'Prohibit use of Internet Connection Sharing on your DNS domain network' is set to 'Enabled' (Automated) | 88 |
| 3.6.9.3 (L1) Ensure 'Require domain users to elevate when setting a network's location' is set to 'Enabled' (Automated)..... | 90 |
| 3.6.10 Network Connectivity Status Indicator | 92 |
| 3.6.11 Network Provider..... | 92 |
| 3.6.11.1 (L1) Ensure 'Hardened UNC Paths' is set to 'Enabled, with "Require Mutual Authentication" and "Require Integrity" set for all NETLOGON and SYSVOL shares' (Automated) | 93 |
| 3.6.12 Offline Files..... | 95 |
| 3.6.13 QoS Packet Scheduler | 95 |
| 3.6.14 SNMP | 95 |
| 3.6.15 SSL Configuration Settings | 95 |
| 3.6.16 TCPIP Settings..... | 95 |
| 3.6.17 Windows Connect Now | 95 |
| 3.6.17.1 (L2) Ensure 'Configuration of wireless settings using Windows Connect Now' is set to 'Disabled' (Automated)..... | 96 |
| 3.6.17.2 (L2) Ensure 'Prohibit access of the Windows Connect Now wizards' is set to 'Enabled' (Automated) | 98 |
| 3.6.18 Windows Connection Manager..... | 100 |
| 3.6.18.1 (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)..... | 101 |
| 3.6.18.2 (L1) Ensure 'Prohibit connection to non-domain networks when connected to domain authenticated network' is set to 'Enabled' (Automated) | 103 |
| 3.6.19 Wireless Display..... | 105 |
| 3.6.19.1 (L1) Ensure 'Require PIN pairing' is set to 'Enabled' (Automated) | 106 |
| 3.7 Printers | 108 |
| 3.7.1 (L1) Ensure 'Allow Print Spooler to accept client connections' is set to 'Disabled' (Automated) | 109 |
| 3.7.2 (L1) Ensure 'Point and Print Restrictions: When installing drivers for a new connection' is set to 'Enabled: Show warning and elevation prompt' (Automated) | 111 |
| 3.7.3 (L1) Ensure 'Point and Print Restrictions: When updating drivers for an existing connection' is set to 'Enabled: Show warning and elevation prompt' (Automated) | 113 |
| 3.8 Shared Folders | 115 |
| 3.9 Start Menu and Taskbar | 115 |
| 3.9.1 Notifications..... | 115 |
| 3.9.1.1 (L1) Ensure 'Turn off toast notifications on the lock screen (User)' is set to 'Enabled' (Automated) | 116 |
| 3.10 System | 118 |
| 3.10.1 Access-Denied Assistance | 118 |
| 3.10.2 App-V | 118 |
| 3.10.3 Application Compatibility Settings..... | 118 |
| 3.10.4 Audit Process Creation | 118 |
| 3.10.4.1 (L1) Ensure 'Include command line in process creation events' is set to 'Enabled' (Automated) | 119 |
| 3.10.5 Credentials Delegation | 121 |
| 3.10.5.1 (L1) Ensure 'Encryption Oracle Remediation' is set to 'Enabled: Force Updated Clients' (Automated) | 122 |
| 3.10.5.2 (L1) Ensure 'Remote host allows delegation of non-exportable credentials' is set to 'Enabled' (Automated)..... | 124 |
| 3.10.6 Ctrl+Alt+Del Options | 126 |

| | |
|---|------------|
| 3.10.7 Device Guard | 126 |
| 3.10.8 Device Health Attestation Service | 126 |
| 3.10.9 Device Installation..... | 126 |
| 3.10.9.1 Device Installation Restrictions | 126 |
| 3.10.9.1.1 (BL) Ensure 'Prevent installation of devices that match any of these device IDs' is set to 'Enabled' (Automated)..... | 127 |
| 3.10.9.1.2 (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) | 129 |
| 3.10.9.1.3 (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) | 131 |
| 3.10.9.1.4 (BL) Ensure 'Prevent installation of devices using drivers that match these device setup classes' is set to 'Enabled' (Automated) | 133 |
| 3.10.9.1.5 (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) | 135 |
| 3.10.9.1.6 (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) | 137 |
| 3.10.9.2 (L1) Ensure 'Prevent device metadata retrieval from the Internet' is set to 'Enabled' (Automated) | 140 |
| 3.10.10 Disk NV Cache | 142 |
| 3.10.11 Disk Quotas | 142 |
| 3.10.12 Driver Installation | 142 |
| 3.10.13 Early Launch Antimalware | 142 |
| 3.10.13.1 (L1) Ensure 'Boot-Start Driver Initialization Policy' is set to 'Enabled: Good, unknown and bad but critical' (Automated) | 143 |
| 3.10.14 Enhanced Storage Access | 145 |
| 3.10.15 File Classification Infrastructure | 145 |
| 3.10.16 File Share Shadow Copy Provider | 145 |
| 3.10.17 Filesystem..... | 145 |
| 3.10.18 Folder Redirection | 145 |
| 3.10.19 Group Policy | 145 |
| 3.10.19.1 (L1) Ensure 'Configure registry policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE' (Automated) | 146 |
| 3.10.19.2 (L1) Ensure 'Configure registry policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE' (Automated) | 148 |
| 3.10.19.3 (L1) Ensure 'Configure security policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE' (Automated) | 150 |
| 3.10.19.4 (L1) Ensure 'Configure security policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE' (Automated) | 152 |
| 3.10.19.5 (L1) Ensure 'Continue experiences on this device' is set to 'Disabled' (Automated) | 154 |
| 3.10.19.6 (L1) Ensure 'Turn off background refresh of Group Policy' is set to 'Disabled' (Automated) | 156 |
| 3.10.20 Internet Communication Management..... | 158 |
| 3.10.20.1 Internet Communication settings | 158 |
| 3.10.20.1.1 (L2) Ensure 'Turn off access to the Store' is set to 'Enabled' (Automated) | 159 |
| 3.10.20.1.2 (L1) Ensure 'Turn off downloading of print drivers over HTTP' is set to 'Enabled' (Automated) | 161 |
| 3.10.20.1.3 (L2) Ensure 'Turn off Help Experience Improvement Program (User)' is set to 'Enabled' (Automated)..... | 163 |
| 3.10.20.1.4 (L2) Ensure 'Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com' is set to 'Enabled' (Automated) | 165 |

| | |
|---|------------|
| 3.10.20.1.5 (L1) Ensure 'Turn off Internet download for Web publishing and online ordering wizards' is set to 'Enabled' (Automated) | 167 |
| 3.10.20.1.6 (L2) Ensure 'Turn off printing over HTTP' is set to 'Enabled' (Automated) | 169 |
| 3.10.20.1.7 (L2) Ensure 'Turn off Registration if URL connection is referring to Microsoft.com' is set to 'Enabled' (Automated) | 171 |
| 3.10.20.1.8 (L2) Ensure 'Turn off Search Companion content file updates' is set to 'Enabled' (Automated) | 173 |
| 3.10.20.1.9 (L2) Ensure 'Turn off the "Order Prints" picture task' is set to 'Enabled' (Automated) | 175 |
| 3.10.20.1.10 (L2) Ensure 'Turn off the "Publish to Web" task for files and folders' is set to 'Enabled' (Automated) | 177 |
| 3.10.20.1.11 (L2) Ensure 'Turn off the Windows Messenger Customer Experience Improvement Program' is set to 'Enabled' (Automated) | 179 |
| 3.10.20.1.12 (L2) Ensure 'Turn off Windows Customer Experience Improvement Program' is set to 'Enabled' (Automated) | 181 |
| 3.10.20.1.13 (L2) Ensure 'Turn off Windows Error Reporting' is set to 'Enabled' (Automated) | 183 |
| 3.10.21 iSCSI | 185 |
| 3.10.22 KDC | 185 |
| 3.10.23 Kerberos | 185 |
| 3.10.23.1 (L2) Ensure 'Support device authentication using certificate' is set to 'Enabled: Automatic' (Automated) | 186 |
| 3.10.24 Locale Services | 188 |
| 3.10.24.1 (L2) Ensure 'Disallow copying of user input methods to the system account for sign-in' is set to 'Enabled' (Automated) | 189 |
| 3.10.25 Logon | 191 |
| 3.10.25.1 (L1) Ensure 'Block user from showing account details on sign-in' is set to 'Enabled' (Automated) | 192 |
| 3.10.25.2 (L1) Ensure 'Do not display network selection UI' is set to 'Enabled' (Automated) | 194 |
| 3.10.25.3 (L1) Ensure 'Do not enumerate connected users on domain-joined computers' is set to 'Enabled' (Automated) | 196 |
| 3.10.25.4 (L1) Ensure 'Enumerate local users on domain-joined computers' is set to 'Disabled' (Automated) | 198 |
| 3.10.25.5 (L1) Ensure 'Turn off app notifications on the lock screen' is set to 'Enabled' (Automated) | 200 |
| 3.10.25.6 (L1) Ensure 'Turn off picture password sign-in' is set to 'Enabled' (Automated) | 202 |
| 3.10.25.7 (L1) Ensure 'Turn on convenience PIN sign-in' is set to 'Disabled' (Automated) | 204 |
| 3.10.26 Mitigation Options | 206 |
| 3.10.27 Net Logon | 206 |
| 3.10.28 Power Management | 206 |
| 3.10.28.1 Button Settings | 206 |
| 3.10.28.2 Hard Disk Settings | 206 |
| 3.10.28.3 Notification Settings | 206 |
| 3.10.28.4 Power Throttling Settings | 206 |
| 3.10.28.5 Sleep Settings | 206 |
| 3.10.28.5.1 (L1) Ensure 'Allow network connectivity during connected-standby (on battery)' is set to 'Disabled' (Automated) | 207 |
| 3.10.28.5.2 (L1) Ensure 'Allow network connectivity during connected-standby (plugged in)' is set to 'Disabled' (Automated) | 209 |
| 3.10.28.5.3 (BL) Ensure 'Allow standby states (S1-S3) when sleeping (on battery)' is set to 'Disabled' (Automated) | 211 |
| 3.10.28.5.4 (BL) Ensure 'Allow standby states (S1-S3) when sleeping (plugged in)' is set to 'Disabled' (Automated) | 213 |
| 3.10.28.5.5 (L1) Ensure 'Require a password when a computer wakes (on battery)' is set to 'Enabled' (Automated) | 215 |

| | |
|---|------------|
| 3.10.28.5.6 (L1) Ensure 'Require a password when a computer wakes (plugged in)' is set to 'Enabled' (Automated)..... | 217 |
| 3.10.29 Remote Assistance | 219 |
| 3.10.29.1 (L1) Ensure 'Configure Offer Remote Assistance' is set to 'Disabled' (Automated)..... | 220 |
| 3.10.29.2 (L1) Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled' (Automated)..... | 222 |
| 3.10.30 Remote Procedure Call..... | 224 |
| 3.10.30.1 (L1) Ensure 'Enable RPC Endpoint Mapper Client Authentication' is set to 'Enabled' (Automated) | 225 |
| 3.10.30.2 (L1) Ensure 'Restrict Unauthenticated RPC clients' is set to 'Enabled: Authenticated' (Automated) | 227 |
| 3.10.31 Remote Storage Access | 229 |
| 3.10.32 Scripts | 229 |
| 3.10.33 Security Settings | 229 |
| 3.10.34 Server Manager | 229 |
| 3.10.35 Shutdown | 229 |
| 3.10.36 Shutdown Options | 229 |
| 3.10.37 System Restore | 229 |
| 3.10.38 Troubleshooting and Diagnostics | 229 |
| 3.10.38.1 Application Compatibility Diagnostic..... | 229 |
| 3.10.38.2 Corrupted File Recovery | 230 |
| 3.10.38.3 Disk Diagnostic | 230 |
| 3.10.38.4 Fault Tolerant Heap | 230 |
| 3.10.38.5 Microsoft Support Diagnostic Tool..... | 230 |
| 3.10.38.5.1 (L2) Ensure 'Microsoft Support Diagnostic Tool: Turn on MSDT interactive communication with support provider' is set to 'Disabled' (Automated)..... | 231 |
| 3.10.39 Trusted Platform Module Services | 233 |
| 3.10.40 User Profiles | 233 |
| 3.10.41 Windows File Protection | 233 |
| 3.10.42 Windows Time Service | 233 |
| 3.10.42.1 Time Providers..... | 233 |
| 3.10.42.1.1 (L1) Ensure 'Enable Windows NTP Client' is set to 'Enabled' (Automated) | 234 |
| 3.10.42.1.2 (L1) Ensure 'Enable Windows NTP Server' is set to 'Disabled' (Automated) | 236 |
| 3.11 Windows Components | 238 |
| 3.11.1 ActiveX Installer Service | 238 |
| 3.11.2 App Package Deployment | 238 |
| 3.11.3 App runtime | 238 |
| 3.11.3.1 (L1) Ensure 'Allow Microsoft accounts to be optional' is set to 'Enabled' (Automated) | 239 |
| 3.11.3.2 (L2) Ensure 'Block launching Universal Windows apps with Windows Runtime API access from hosted content.' is set to 'Enabled' (Automated) | 241 |
| 3.11.4 Application Compatibility | 243 |
| 3.11.5 Attachment Manager..... | 243 |
| 3.11.5.1 (L1) Ensure 'Do not preserve zone information in file attachments (User)' is set to 'Disabled' (Automated) | 244 |
| 3.11.5.2 (L1) Ensure 'Notify antivirus programs when opening attachments (User)' is set to 'Enabled' (Automated) | 246 |
| 3.11.6 AutoPlay Policies | 248 |
| 3.11.6.1 (L1) Ensure 'Disallow Autoplay for non-volume devices' is set to 'Enabled' (Automated) | 249 |
| 3.11.6.2 (L1) Ensure 'Set the default behavior for AutoRun' is set to 'Enabled: Do not execute any autorun commands' (Automated)..... | 251 |
| 3.11.6.3 (L1) Ensure 'Turn off Autoplay' is set to 'Enabled: All drives' (Automated) | 253 |
| 3.11.7 BitLocker Drive Encryption | 255 |
| 3.11.7.1 Fixed Data Drives..... | 255 |

| | |
|--|------------|
| 3.11.7.1.1 (BL) Ensure 'Choose how BitLocker-protected fixed drives can be recovered' is set to 'Enabled' (Automated)..... | 256 |
| 3.11.7.1.2 (BL) Ensure 'Choose how BitLocker-protected fixed drives can be recovered: Recovery Key' is set to 'Enabled: Allow 256-bit recovery key' (Automated) | 258 |
| 3.11.7.1.3 (BL) Ensure 'Choose how BitLocker-protected fixed drives can be recovered: Recovery Password' is set to 'Enabled: Allow 48-digit recovery password' (Automated) | 260 |
| 3.11.7.1.4 (BL) Ensure 'Choose how BitLocker-protected fixed drives can be recovered: Allow data recovery agent' is set to 'Enabled: True' (Automated) | 262 |
| 3.11.7.1.5 (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) | 264 |
| 3.11.7.1.6 (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)..... | 266 |
| 3.11.7.1.7 (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)..... | 268 |
| 3.11.7.1.8 (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) | 270 |
| 3.11.7.2 Operating System Drives..... | 272 |
| 3.11.7.2.1 (BL) Ensure 'Allow enhanced PINs for startup' is set to 'Enabled' (Automated) ... | 273 |
| 3.11.7.2.2 (BL) Ensure 'Choose how BitLocker-protected operating system drives can be recovered' is set to 'Enabled' (Automated) | 275 |
| 3.11.7.2.3 (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) | 278 |
| 3.11.7.2.4 (BL) Ensure 'Choose how BitLocker-protected operating system drives can be recovered: Recovery Password' is set to 'Enabled: Require 48-digit recovery password' (Automated) | 280 |
| 3.11.7.2.5 (BL) Ensure 'Choose how BitLocker-protected operating system drives can be recovered: Allow data recovery agent' is set to 'Enabled: False' (Automated)..... | 282 |
| 3.11.7.2.6 (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) | 284 |
| 3.11.7.2.7 (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)..... | 286 |
| 3.11.7.2.8 (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) | 288 |
| 3.11.7.2.9 (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) | 290 |
| 3.11.7.2.10 (BL) Ensure 'Require additional authentication at startup' is set to 'Enabled' (Automated) | 292 |
| 3.11.7.2.11 (BL) Ensure 'Require additional authentication at startup: Allow BitLocker without a compatible TPM' is set to 'Enabled: False' (Automated) | 294 |
| 3.11.7.2.12 (BL) Ensure 'Require additional authentication at startup: Configure TPM startup key and PIN:' is set to 'Enabled: Do not allow startup key and PIN with TPM' (Automated) | 296 |
| 3.11.7.2.13 (BL) Ensure 'Require additional authentication at startup: Configure TPM startup key:' is set to 'Enabled: Do not allow startup key with TPM' (Automated) | 298 |
| 3.11.7.2.14 (BL) Ensure 'Require additional authentication at startup: Configure TPM startup PIN:' is set to 'Enabled: Require startup PIN with TPM' (Automated) | 300 |
| 3.11.7.2.15 (BL) Ensure 'Require additional authentication at startup: Configure TPM startup:' is set to 'Enabled: Do not allow TPM' (Automated) | 302 |
| 3.11.7.3 Removable Data Drives..... | 304 |

| | |
|---|------------|
| 3.11.7.3.1 (BL) Ensure 'Deny write access to removable drives not protected by BitLocker' is set to 'Enabled' (Automated)..... | 305 |
| 3.11.7.3.2 (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) | 307 |
| 3.11.8 Credential User Interface..... | 309 |
| 3.11.8.1 (L1) Ensure 'Do not display the password reveal button' is set to 'Enabled' (Automated) | 310 |
| 3.11.8.2 (L1) Ensure 'Enumerate administrator accounts on elevation' is set to 'Disabled' (Automated) | 312 |
| 3.11.8.3 (L1) Ensure 'Prevent the use of security questions for local accounts' is set to 'Enabled' (Automated)..... | 314 |
| 3.11.9 Data Collection and Preview Builds..... | 316 |
| 3.11.10 Delivery Optimization | 316 |
| 3.11.11 Desktop Window Manager | 316 |
| 3.11.12 Device and Driver Compatibility | 316 |
| 3.11.13 Digital Locker..... | 316 |
| 3.11.14 Event Forwarding | 316 |
| 3.11.15 Event Log Service | 316 |
| 3.11.15.1 Application | 316 |
| 3.11.15.1.1 (L1) Ensure 'Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Automated) | 317 |
| 3.11.15.1.2 (L1) Ensure 'Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (Automated) | 319 |
| 3.11.15.2 Security..... | 321 |
| 3.11.15.2.1 (L1) Ensure 'Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Automated) | 322 |
| 3.11.15.2.2 (L1) Ensure 'Specify the maximum log file size (KB)' is set to 'Enabled: 196,608 or greater' (Automated) | 324 |
| 3.11.15.3 Setup..... | 326 |
| 3.11.15.3.1 (L1) Ensure 'Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Automated) | 327 |
| 3.11.15.3.2 (L1) Ensure 'Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (Automated) | 329 |
| 3.11.15.4 System | 331 |
| 3.11.15.4.1 (L1) Ensure 'Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Automated) | 332 |
| 3.11.15.4.2 (L1) Ensure 'Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (Automated) | 334 |
| 3.11.16 Event Logging | 336 |
| 3.11.17 Event Viewer | 336 |
| 3.11.18 File Explorer..... | 336 |
| 3.11.18.1 (L1) Ensure 'Configure Windows Defender SmartScreen' is set to 'Enabled: Warn and prevent bypass' (Automated) | 337 |
| 3.11.18.2 (L1) Ensure 'Turn off Data Execution Prevention for Explorer' is set to 'Disabled' (Automated) | 339 |
| 3.11.18.3 (L1) Ensure 'Turn off heap termination on corruption' is set to 'Disabled' (Automated) | 341 |
| 3.11.18.4 (L1) Ensure 'Turn off shell protocol protected mode' is set to 'Disabled' (Automated) | 343 |
| 3.11.19 File Revocation..... | 345 |
| 3.11.20 Home Group..... | 345 |
| 3.11.20.1 (L1) Ensure 'Prevent the computer from joining a homegroup' is set to 'Enabled' (Automated) | 346 |
| 3.11.21 IME | 348 |
| 3.11.22 Instant Search..... | 348 |

| | |
|---|------------|
| 3.11.23 Internet Explorer..... | 348 |
| 3.11.23.1 (L1) Ensure 'Disable Internet Explorer 11 as a standalone browser' is set to 'Enabled: Always' (Automated) | 349 |
| 3.11.24 Internet Information Services | 351 |
| 3.11.25 Location and Sensors..... | 351 |
| 3.11.25.1 Windows Location Provider | 351 |
| 3.11.26 Maintenance Scheduler | 351 |
| 3.11.27 Microsoft Account..... | 351 |
| 3.11.27.1 (L1) Ensure 'Block all consumer Microsoft account user authentication' is set to 'Enabled' (Automated)..... | 352 |
| 3.11.28 Microsoft Defender Antivirus | 354 |
| 3.11.28.1 Client Interface..... | 354 |
| 3.11.28.2 Exclusions..... | 354 |
| 3.11.28.3 MAPS | 354 |
| 3.11.28.3.1 (L1) Ensure 'Configure local setting override for reporting to Microsoft MAPS' is set to 'Disabled' (Automated) | 355 |
| 3.11.28.3.2 (L2) Ensure 'Join Microsoft MAPS' is set to 'Disabled' (Automated) | 357 |
| 3.11.28.4 Microsoft Defender Exploit Guard | 359 |
| 3.11.28.5 MpEngine..... | 359 |
| 3.11.28.6 Network Inspection System..... | 359 |
| 3.11.28.7 Quarantine..... | 359 |
| 3.11.28.8 Real-time Protection..... | 359 |
| 3.11.28.9 Remediation | 359 |
| 3.11.28.10 Reporting..... | 359 |
| 3.11.28.10.1 (L2) Ensure 'Configure Watson events' is set to 'Disabled' (Automated) | 360 |
| 3.11.28.11 (L1) Ensure 'Turn off Microsoft Defender Antivirus' is set to 'Disabled' (Automated) | 362 |
| 3.11.29 Microsoft Management Console..... | 364 |
| 3.11.30 Microsoft User Experience Virtualization | 364 |
| 3.11.31 Network Sharing..... | 364 |
| 3.11.31.1 (L1) Ensure 'Prevent users from sharing files within their profile. (User)' is set to 'Enabled' (Automated)..... | 365 |
| 3.11.32 Online Assistance | 367 |
| 3.11.33 Portable Operating System | 367 |
| 3.11.34 Presentation Settings | 367 |
| 3.11.35 Push To Install..... | 367 |
| 3.11.35.1 (L2) Ensure 'Turn off Push To Install service' is set to 'Enabled' (Automated)..... | 368 |
| 3.11.36 Remote Desktop Services | 370 |
| 3.11.36.1 RD Gateway..... | 370 |
| 3.11.36.2 RD Licensing..... | 370 |
| 3.11.36.3 Remote Desktop Connection Client | 370 |
| 3.11.36.3.1 RemoteFX USB Device Redirection | 370 |
| 3.11.36.3.2 (L1) Ensure 'Do not allow passwords to be saved' is set to 'Enabled' (Automated) | 371 |
| 3.11.36.4 Remote Desktop Session Host | 373 |
| 3.11.36.4.1 Azure Virtual Desktop..... | 373 |
| 3.11.36.4.2 Connections | 373 |
| 3.11.36.4.2.1 (L2) Ensure 'Allow users to connect remotely by using Remote Desktop Services' is set to 'Disabled' (Automated)..... | 374 |
| 3.11.36.4.3 Device and Resource Redirection..... | 376 |
| 3.11.36.4.3.1 (L2) Ensure 'Do not allow COM port redirection' is set to 'Enabled' (Automated) | 377 |
| 3.11.36.4.3.2 (L1) Ensure 'Do not allow drive redirection' is set to 'Enabled' (Automated) | 379 |
| 3.11.36.4.3.3 (L2) Ensure 'Do not allow LPT port redirection' is set to 'Enabled' (Automated) | 381 |

| | |
|---|------------|
| 3.11.36.4.3.4 (L2) Ensure 'Do not allow supported Plug and Play device redirection' is set to 'Enabled' (Automated)..... | 383 |
| 3.11.36.4.4 Licensing | 385 |
| 3.11.36.4.5 Printer Redirection..... | 385 |
| 3.11.36.4.6 Profiles | 385 |
| 3.11.36.4.7 RD Connection Broker | 385 |
| 3.11.36.4.8 Remote Session Environment..... | 385 |
| 3.11.36.4.9 Security | 385 |
| 3.11.36.4.9.1 (L1) Ensure 'Always prompt for password upon connection' is set to 'Enabled' (Automated) | 386 |
| 3.11.36.4.9.2 (L1) Ensure 'Require secure RPC communication' is set to 'Enabled' (Automated) | 388 |
| 3.11.36.4.9.3 (L1) Ensure 'Require use of specific security layer for remote (RDP) connections' is set to 'Enabled: SSL' (Automated) | 390 |
| 3.11.36.4.9.4 (L1) Ensure 'Require user authentication for remote connections by using Network Level Authentication' is set to 'Enabled' (Automated) | 392 |
| 3.11.36.4.9.5 (L1) Ensure 'Set client connection encryption level' is set to 'Enabled: High Level' (Automated) | 394 |
| 3.11.36.4.10 Session Time Limits | 396 |
| 3.11.36.4.10.1 (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) | 397 |
| 3.11.36.4.10.2 (L2) Ensure 'Set time limit for disconnected sessions' is set to 'Enabled: 1 minute' (Automated)..... | 399 |
| 3.11.36.4.11 Temporary folders | 401 |
| 3.11.36.4.11.1 (L1) Ensure 'Do not delete temp folders upon exit' is set to 'Disabled' (Automated) | 402 |
| 3.11.37 RSS Feeds..... | 404 |
| 3.11.37.1 (L1) Ensure 'Prevent downloading of enclosures' is set to 'Enabled' (Automated) | 405 |
| 3.11.38 Security Center..... | 407 |
| 3.11.39 Shutdown Options | 407 |
| 3.11.40 Smart Card | 407 |
| 3.11.41 Sound Recorder | 407 |
| 3.11.42 Store | 407 |
| 3.11.42.1 (L1) Ensure 'Turn off the offer to update to the latest version of Windows' is set to 'Enabled' (Automated)..... | 408 |
| 3.11.42.2 (L2) Ensure 'Turn off the Store application' is set to 'Enabled' (Automated) | 410 |
| 3.11.43 Sync your settings | 412 |
| 3.11.44 Tablet PC | 412 |
| 3.11.45 Tenant Restrictions..... | 412 |
| 3.11.46 Windows Calendar | 412 |
| 3.11.47 Windows Color System | 412 |
| 3.11.48 Windows Error Reporting..... | 412 |
| 3.11.49 Windows Installer..... | 412 |
| 3.11.49.1 (L2) Ensure 'Prevent Internet Explorer security prompt for Windows Installer scripts' is set to 'Disabled' (Automated) | 413 |
| 3.11.50 Windows Logon Options | 415 |
| 3.11.50.1 (L1) Ensure 'Sign-in and lock last interactive user automatically after a restart' is set to 'Disabled' (Automated)..... | 416 |
| 3.11.51 Windows Media Digital Rights Management | 418 |
| 3.11.52 Windows Media Player | 418 |
| 3.11.52.1 Playback | 418 |
| 3.11.52.1.1 (L2) Ensure 'Prevent Codec Download (User)' is set to 'Enabled' (Automated) | 419 |
| 3.11.53 Windows Mobility Center | 421 |
| 3.11.54 Windows PowerShell | 421 |
| 3.11.54.1 (L1) Ensure 'Turn on PowerShell Script Block Logging' is set to 'Enabled' (Automated) | 422 |

| | |
|---|------------|
| 3.11.54.2 (L1) Ensure 'Turn on PowerShell Transcription' is set to 'Enabled' (Automated) ... | 424 |
| 3.11.55 Windows Remote Management (WinRM) | 426 |
| 3.11.55.1 WinRM Client..... | 426 |
| 3.11.55.1.1 (L1) Ensure 'Allow Basic authentication' is set to 'Disabled' (Automated) | 427 |
| 3.11.55.1.2 (L1) Ensure 'Allow unencrypted traffic' is set to 'Disabled' (Automated) | 429 |
| 3.11.55.1.3 (L1) Ensure 'Disallow Digest authentication' is set to 'Enabled' (Automated) | 431 |
| 3.11.55.2 WinRM Service..... | 433 |
| 3.11.55.2.1 (L1) Ensure 'Allow Basic authentication' is set to 'Disabled' (Automated) | 434 |
| 3.11.55.2.2 (L2) Ensure 'Allow remote server management through WinRM' is set to 'Disabled' (Automated) | 436 |
| 3.11.55.2.3 (L1) Ensure 'Allow unencrypted traffic' is set to 'Disabled' (Automated) | 438 |
| 3.11.55.2.4 (L1) Ensure 'Disallow WinRM from storing RunAs credentials' is set to 'Enabled' (Automated) | 440 |
| 3.11.56 Windows Remote Shell..... | 442 |
| 3.11.56.1 (L2) Ensure 'Allow Remote Shell Access' is set to 'Disabled' (Automated) | 443 |
| 4 Application Defaults | 445 |
| 5 Auditing..... | 445 |
| 5.1 (L1) Ensure 'Account Logon Audit Credential Validation' is set to 'Success and Failure' (Automated) | 446 |
| 5.2 (L1) Ensure 'Account Logon Logoff Audit Account Lockout' is set to include 'Failure' (Automated) | 448 |
| 5.3 (L1) Ensure 'Account Logon Logoff Audit Group Membership' is set to include 'Success' (Automated) | 450 |
| 5.4 (L1) Ensure 'Account Logon Logoff Audit Logoff' is set to include 'Success' (Automated) | 452 |
| 5.5 (L1) Ensure 'Account Logon Logoff Audit Logon' is set to 'Success and Failure' (Automated) | 454 |
| 5.6 (L1) Ensure 'Account Management Audit Application Group Management' is set to 'Success and Failure' (Automated) | 456 |
| 5.7 (L1) Ensure 'Audit Authentication Policy Change' is set to include 'Success' (Automated) | 458 |
| 5.8 (L1) Ensure 'Audit Authorization Policy Change' is set to include 'Success' (Automated) | 460 |
| 5.9 (L1) Ensure 'Audit Changes to Audit Policy' is set to include 'Success' (Automated) | 462 |
| 5.10 (L1) Ensure 'Audit File Share Access' is set to 'Success and Failure' (Automated) | 464 |
| 5.11 (L1) Ensure 'Audit Other Logon Logoff Events' is set to 'Success and Failure' (Automated) | 466 |
| 5.12 (L1) Ensure 'Audit Security Group Management' is set to include 'Success' (Automated) | 468 |
| 5.13 (L1) Ensure 'Audit Security System Extension' is set to include 'Success' (Automated) | 470 |
| 5.14 (L1) Ensure 'Audit Special Logon' is set to include 'Success' (Automated) | 472 |
| 5.15 (L1) Ensure 'Audit User Account Management' is set to 'Success and Failure' (Automated) | 474 |
| 5.16 (L1) Ensure 'Detailed Tracking Audit PNP Activity' is set to include 'Success' (Automated) | 477 |
| 5.17 (L1) Ensure 'Detailed Tracking Audit Process Creation' is set to include 'Success' (Automated) | 479 |
| 5.18 (L1) Ensure 'Object Access Audit Detailed File Share' is set to include 'Failure' (Automated) | 481 |
| 5.19 (L1) Ensure 'Object Access Audit Other Object Access Events' is set to 'Success and Failure' (Automated) | 483 |
| 5.20 (L1) Ensure 'Object Access Audit Removable Storage' is set to 'Success and Failure' (Automated) | 485 |
| 5.21 (L1) Ensure 'Policy Change Audit MPSSVC Rule Level Policy Change' is set to 'Success and Failure' (Automated) | 487 |

| | |
|--|------------|
| 5.22 (L1) Ensure 'Policy Change Audit Other Policy Change Events' is set to include 'Failure' (Automated) | 490 |
| 5.23 (L1) Ensure 'Privilege Use Audit Sensitive Privilege Use' is set to 'Success and Failure' (Automated) | 492 |
| 5.24 (L1) Ensure 'System Audit I Psec Driver' is set to 'Success and Failure' (Automated) .. | 495 |
| 5.25 (L1) Ensure 'System Audit Other System Events' is set to 'Success and Failure' (Automated) | 498 |
| 5.26 (L1) Ensure 'System Audit Security State Change' is set to include 'Success' (Automated) | 500 |
| 5.27 (L1) Ensure 'System Audit System Integrity' is set to 'Success and Failure' (Automated) | 502 |
| 6 Authentication..... | 504 |
| 7 BitLocker | 504 |
| 8 BITS | 504 |
| 9 Bluetooth..... | 504 |
| 10 Browser | 504 |
| 11 Camera | 504 |
| 11.1 (L2) Ensure 'Allow Camera' is set to 'Not allowed' (Automated) | 505 |
| 12 Cellular | 507 |
| 13 Cloud Desktop | 507 |
| 14 Config Refresh..... | 507 |
| 15 Connectivity | 507 |
| 16 Control Policy Conflict | 507 |
| 17 Converters..... | 507 |
| 18 Credential Providers..... | 507 |
| 19 Cryptography | 507 |
| 20 Data Protection | 508 |
| 21 Defender | 508 |
| 21.1 (L1) Ensure 'Allow Behavior Monitoring' is set to 'Allowed' (Automated) | 509 |
| 21.2 (L1) Ensure 'Allow Email Scanning' is set to 'Allowed' (Automated) | 511 |
| 21.3 (L1) Ensure 'Allow Full Scan Removable Drive Scanning' is set to 'Allowed' (Automated) | 513 |
| 21.4 (L1) Ensure 'Allow Realtime Monitoring' is set to 'Allowed' (Automated) | 515 |
| 21.5 (L1) Ensure 'Allow scanning of all downloaded files and attachments' is set to 'Allowed' (Automated) | 517 |
| 21.6 (L1) Ensure 'Allow Script Scanning' is set to 'Allowed' (Automated) | 519 |
| 21.7 (L1) Ensure 'Attack Surface Reduction rules' are configured (Automated) | 521 |
| 21.8 (L2) Ensure 'Enable File Hash Computation' is set to 'Enable' (Automated)..... | 524 |
| 21.9 (L1) Ensure 'Enable Network Protection' is set to 'Enabled (block mode)' (Automated) | 526 |
| 21.10 (L1) Ensure 'PUA Protection' is set to 'PUA Protection on' (Automated) | 528 |
| 22 Delivery Optimization | 530 |
| 22.1 (L1) Ensure 'DO Download Mode' is NOT set to 'HTTP blended with Internet Peering' (Automated) | 531 |
| 23 Device Guard..... | 533 |

| | |
|---|------------|
| 23.1 (NG) Ensure 'Enable Virtualization Based Security' is set to 'Enable virtualization based security' (Automated) | 534 |
| 23.2 (NG) Ensure 'Require Platform Security Features' is set to 'Turns on VBS with Secure Boot' or higher (Automated)..... | 536 |
| 23.3 (NG) Ensure 'Credential Guard' is set to 'Enabled with UEFI lock' (Automated)..... | 538 |
| 23.4 (NG) Ensure 'Configure System Guard Launch' is set to 'Unmanaged Enables Secure Launch if supported by hardware' (Automated)..... | 540 |
| 24 Device Lock..... | 542 |
| 24.1 (L1) Ensure 'Alphanumeric Device Password Required' is set to 'Password, Numeric PIN, or Alphanumeric PIN required' (Automated)..... | 543 |
| 24.2 (L1) Ensure 'Device Password Expiration' is set to '365 or fewer days, but not 0' (Automated) | 545 |
| 24.3 (L1) Ensure 'Device Password History' is set to '24 or more password(s)' (Automated) | 547 |
| 24.4 (L1) Ensure 'Min Device Password Complex Characters' is set to 'Digits lowercase letters and uppercase letters are required' (Automated) | 550 |
| 24.5 (L1) Ensure 'Min Device Password Length' is set to '14 or more character(s)' (Automated) | 553 |
| 24.6 (L1) Ensure 'Minimum Password Age' is set to '1 or more day(s)' (Automated) | 556 |
| 25 Dma Guard | 558 |
| 26 Eap..... | 558 |
| 27 Education | 558 |
| 28 Enterprise Cloud Print..... | 558 |
| 29 eSIM..... | 558 |
| 30 Experience | 558 |
| 30.1 (L1) Ensure 'Allow Cortana' is set to 'Block' (Automated)..... | 559 |
| 30.2 (L2) Ensure 'Allow Windows Spotlight (User)' is set to 'Block' (Automated) | 561 |
| 30.3 (L1) Ensure 'Do not show feedback notifications' is set to 'Feedback notifications are disabled' (Automated) | 563 |
| 31 Exploit Guard | 565 |
| 32 Federated Authentication..... | 565 |
| 33 Feeds | 565 |
| 33.1 (L2) Ensure 'Enable news and interests' is set to 'Not Allowed' (Automated) | 566 |
| 34 File Explorer | 568 |
| 35 Firewall | 568 |
| 35.1 (L1) Ensure 'Enable Domain Network Firewall' is set to 'True' (Automated) | 569 |
| 35.2 (L1) Ensure 'Enable Domain Network Firewall: Default Inbound Action for Domain Profile' is set to 'Block' (Automated) | 571 |
| 35.3 (L1) Ensure 'Enable Domain Network Firewall: Disable Inbound Notifications' is set to 'True' (Automated) | 573 |
| 35.4 (L1) Ensure 'Enable Private Network Firewall' is set to 'True' (Automated) | 575 |
| 35.5 (L1) Ensure 'Enable Private Network Firewall: Default Inbound Action for Private Profile' is set to 'Block' (Automated) | 577 |
| 35.6 (L1) Ensure 'Enable Private Network Firewall: Disable Inbound Notifications' is set to 'True' (Automated) | 579 |
| 35.7 (L1) Ensure 'Enable Public Network Firewall' is set to 'True' (Automated) | 581 |
| 35.8 (L1) Ensure 'Enable Public Network Firewall: Allow Local Ipsec Policy Merge' is set to 'False' (Automated) | 583 |

| | |
|---|------------|
| 35.9 (L1) Ensure 'Enable Public Network Firewall: Allow Local Policy Merge' is set to 'False' (Automated) | 585 |
| 35.10 (L1) Ensure 'Enable Public Network Firewall: Default Inbound Action for Public Profile' is set to 'Block' (Automated) | 587 |
| 35.11 (L1) Ensure 'Enable Public Network Firewall: Disable Inbound Notifications' is set to 'True' (Automated) | 589 |
| 36 FSLogix | 591 |
| 37 Games | 591 |
| 38 Handwriting..... | 591 |
| 39 Human Presence..... | 591 |
| 40 Kerberos..... | 591 |
| 41 Kiosk Browser..... | 591 |
| 42 Lanman Workstation | 591 |
| 42.1 (L1) Ensure 'Enable insecure guest logons' is set to 'Disabled' (Automated) | 592 |
| 43 Licensing..... | 594 |
| 43.1 (L2) Ensure 'Disallow KMS Client Online AVS Validation' is set to 'Allow' (Automated) | 595 |
| 44 List Sync..... | 597 |
| 45 Local Policies Security Options..... | 597 |
| 45.1 (L1) Ensure 'Accounts: Block Microsoft accounts' is set to 'Users can't add or log on with Microsoft accounts' (Automated) | 598 |
| 45.2 (L1) Ensure 'Accounts: Enable Guest account status' is set to 'Disabled' (Automated) | 600 |
| 45.3 (L1) Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled' (Automated) | 602 |
| 45.4 (L1) Configure 'Accounts: Rename administrator account' (Automated) | 604 |
| 45.5 (L1) Configure 'Accounts: Rename guest account' (Automated) | 606 |
| 45.6 (L2) Ensure 'Devices: Prevent users from installing printer drivers when connecting to shared printers' is set to 'Enable' (Automated) | 608 |
| 45.7 (L1) Ensure 'Interactive logon: Do not display last signed-in' is set to 'Enabled' (Automated) | 610 |
| 45.8 (L1) Ensure 'Interactive logon: Do not require CTRL+ALT+DEL' is set to 'Disabled' (Automated) | 612 |
| 45.9 (L1) Ensure 'Interactive logon: Machine inactivity limit' is set to '900 or fewer second(s), but not 0' (Automated) | 614 |
| 45.10 (L1) Configure 'Interactive logon: Message text for users attempting to log on' (Automated) | 616 |
| 45.11 (L1) Configure 'Interactive logon: Message title for users attempting to log on' (Automated) | 618 |
| 45.12 (L1) Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or higher (Automated) | 620 |
| 45.13 (L1) Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled' (Automated)..... | 622 |
| 45.14 (L1) Ensure 'Microsoft network client: Digitally sign communications (if server agrees)' is set to 'Enabled' (Automated)..... | 625 |
| 45.15 (L1) Ensure 'Microsoft network client: Send unencrypted password to third-party SMB servers' is set to 'Disabled' (Automated)..... | 628 |
| 45.16 (L1) Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled' (Automated)..... | 630 |
| 45.17 (L1) Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled' (Automated)..... | 633 |

| | |
|--|------------|
| 45.18 (L1) Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts' is set to 'Enabled' (Automated) | 636 |
| 45.19 (L1) Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled' (Automated) | 638 |
| 45.20 (L1) Ensure 'Network access: Restrict anonymous access to Named Pipes and Shares' is set to 'Enabled' (Automated) | 640 |
| 45.21 (L1) Ensure 'Network access: Restrict clients allowed to make remote calls to SAM' is set to 'Administrators: Remote Access: Allow' (Automated) | 642 |
| 45.22 (L1) Ensure 'Network security: Allow Local System to use computer identity for NTLM' is set to 'Allow' (Automated) | 644 |
| 45.23 (L1) Ensure 'Network Security: Allow PKU2U authentication requests' is set to 'Block' (Automated) | 646 |
| 45.24 (L1) Ensure 'Network security: Do not store LAN Manager hash value on next password change' is set to 'Enabled' (Automated) | 648 |
| 45.25 (L1) Ensure 'Network security: LAN Manager authentication level' is set to 'Send LM and NTLMv2 responses only. Refuse LM and NTLM' (Automated) | 650 |
| 45.26 (L1) Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' is set to 'Require NTLM and 128-bit encryption' (Automated) | 653 |
| 45.27 (L1) Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require NTLM and 128-bit encryption' (Automated) | 655 |
| 45.28 (L1) Ensure 'Network security: Restrict NTLM: Audit Incoming NTLM Traffic' is set to 'Enable auditing for all accounts' (Automated) | 657 |
| 45.29 (L1) Ensure 'User Account Control: Behavior of the elevation prompt for administrators' is set to 'Prompt for consent on the secure desktop' or higher (Automated) | 659 |
| 45.30 (L1) Ensure 'User Account Control: Behavior of the elevation prompt for standard users' is set to 'Automatically deny elevation requests' (Automated) | 661 |
| 45.31 (L1) Ensure 'User Account Control: Detect application installations and prompt for elevation' is set to 'Enabled' (Automated) | 663 |
| 45.32 (L1) Ensure 'User Account Control: Only elevate UIAccess applications that are installed in secure locations' is set to 'Enabled' (Automated) | 665 |
| 45.33 (L1) Ensure 'User Account Control: Use Admin Approval Mode' is set to 'Enabled' (Automated) | 667 |
| 45.34 (L1) Ensure 'User Account Control: Switch to the secure desktop when prompting for elevation' is set to 'Enabled' (Automated) | 669 |
| 45.35 (L1) Ensure 'User Account Control: Run all administrators in Admin Approval Mode' is set to 'Enabled' (Automated) | 671 |
| 45.36 (L1) Ensure 'User Account Control: Virtualize file and registry write failures to per-user locations' is set to 'Enabled' (Automated) | 673 |
| 46 Lock Down | 675 |
| 47 Memory Dump..... | 675 |
| 48 Microsoft App Store..... | 675 |
| 48.1 (L1) Ensure 'Allow apps from the Microsoft app store to auto update' is set to 'Allowed' (Automated) | 676 |
| 48.2 (L1) Ensure 'Allow Game DVR' is set to 'Block' (Automated) | 678 |
| 48.3 (L2) Ensure 'Disable Store Originated Apps' is set to 'Enabled' (Automated) | 680 |
| 48.4 (L1) Ensure 'MSI Allow user control over installs' is set to 'Disabled' (Automated) | 682 |
| 48.5 (L1) Ensure 'MSI Always install with elevated privileges' is set to 'Disabled' (Automated) | 684 |
| 48.6 (L1) Ensure 'MSI Always install with elevated privileges (User)' is set to 'Disabled' (Automated) | 686 |
| 48.7 (L1) Ensure 'Require Private Store Only' is set to 'Only Private store is enabled' (Automated) | 688 |

| | |
|--|------------|
| 49 Microsoft Defender for Endpoint | 690 |
| 50 Mixed Reality..... | 690 |
| 51 Network Isolation..... | 690 |
| 52 Network List Manager..... | 690 |
| 53 News and interests | 690 |
| 54 Notifications..... | 690 |
| 55 PDE | 690 |
| 56 Power..... | 690 |
| 57 Printer Provisioning..... | 691 |
| 58 Privacy..... | 691 |
| 58.1 (L2) Ensure 'Allow Cross Device Clipboard' is set to 'Block' (Automated) | 692 |
| 58.2 (L1) Ensure 'Allow Input Personalization' is set to 'Block' (Automated)..... | 694 |
| 58.3 (L2) Ensure 'Disable Advertising ID' is set to 'Enabled' (Automated) | 696 |
| 58.4 (L1) Ensure 'Let Apps Activate With Voice Above Lock' is set to 'Enabled: Force Deny' (Automated) | 698 |
| 58.5 (L2) Ensure 'Upload User Activities' is set to 'Disabled' (Automated) | 700 |
| 59 Remote Desktop | 702 |
| 60 Search | 702 |
| 60.1 (L2) Ensure 'Allow Cloud Search' is set to 'Not allowed' (Automated) | 703 |
| 60.2 (L1) Ensure 'Allow Indexing Encrypted Stores Or Items' is set to 'Block' (Automated) .. | 705 |
| 60.3 (L1) Ensure 'Allow Search To Use Location' is set to 'Block' (Automated)..... | 707 |
| 61 Security | 709 |
| 62 Settings | 709 |
| 62.1 (L2) Ensure 'Allow Online Tips' is set to 'Block' (Automated) | 710 |
| 63 Shared PC | 712 |
| 64 Smart Screen | 712 |
| 65 Speech..... | 712 |
| 66 Storage | 712 |
| 67 System..... | 712 |
| 67.1 (L1) Ensure 'Allow Telemetry' is set to 'Basic' (Automated) | 713 |
| 67.2 (L2) Ensure 'Allow Font Providers' is set to 'Not allowed' (Automated)..... | 715 |
| 67.3 (L2) Ensure 'Disable One Drive File Sync' is set to 'Sync Disabled' (Automated)..... | 717 |
| 68 Task Manager..... | 719 |
| 69 System Services | 719 |
| 69.1 (L2) Ensure 'Bluetooth Audio Gateway Service (BTAGService)' is set to 'Disabled' (Automated) | 720 |
| 69.2 (L2) Ensure 'Bluetooth Support Service (bthserv)' is set to 'Disabled' (Automated) | 722 |
| 69.3 (L1) Ensure 'Computer Browser (Browser)' is set to 'Disabled' or 'Not Installed' (Automated) | 724 |
| 69.4 (L2) Ensure 'Downloaded Maps Manager (MapsBroker)' is set to 'Disabled' (Automated) | 727 |
| 69.5 (L2) Ensure 'Geolocation Service (lfsvc)' is set to 'Disabled' (Automated) | 729 |

| | |
|--|-----|
| 69.6 (L1) Ensure 'IIS Admin Service (IISADMIN)' is set to 'Disabled' or 'Not Installed' (Automated) | 731 |
| 69.7 (L1) Ensure 'Infrared monitor service (irmon)' is set to 'Disabled' or 'Not Installed' (Automated) | 733 |
| 69.8 (L1) Ensure 'Internet Connection Sharing (ICS) (SharedAccess)' is set to 'Disabled' (Automated) | 735 |
| 69.9 (L2) Ensure 'Link-Layer Topology Discovery Mapper (lltdsvc)' is set to 'Disabled' (Automated) | 738 |
| 69.10 (L1) Ensure 'LxssManager (LxssManager)' is set to 'Disabled' or 'Not Installed' (Automated) | 740 |
| 69.11 (L1) Ensure 'Microsoft FTP Service (FTPSVC)' is set to 'Disabled' or 'Not Installed' (Automated) | 742 |
| 69.12 (L2) Ensure 'Microsoft iSCSI Initiator Service (MSiSCSI)' is set to 'Disabled' (Automated) | 744 |
| 69.13 (L1) Ensure 'OpenSSH SSH Server (sshd)' is set to 'Disabled' or 'Not Installed' (Automated) | 746 |
| 69.14 (L2) Ensure 'Peer Name Resolution Protocol (PNRPsvc)' is set to 'Disabled' (Automated) | 748 |
| 69.15 (L2) Ensure 'Peer Networking Grouping (p2psvc)' is set to 'Disabled' (Automated) | 750 |
| 69.16 (L2) Ensure 'Peer Networking Identity Manager (p2pimsvc)' is set to 'Disabled' (Automated) | 752 |
| 69.17 (L2) Ensure 'PNRP Machine Name Publication Service (PNRPAutoReg)' is set to 'Disabled' (Automated) | 754 |
| 69.18 (L2) Ensure 'Print Spooler (Spooler)' is set to 'Disabled' (Automated) | 756 |
| 69.19 (L2) Ensure 'Problem Reports and Solutions Control Panel Support (wercplsupport)' is set to 'Disabled' (Automated) | 758 |
| 69.20 (L2) Ensure 'Remote Access Auto Connection Manager (RasAuto)' is set to 'Disabled' (Automated) | 760 |
| 69.21 (L2) Ensure 'Remote Desktop Configuration (SessionEnv)' is set to 'Disabled' (Automated) | 762 |
| 69.22 (L2) Ensure 'Remote Desktop Services (TermService)' is set to 'Disabled' (Automated) | 764 |
| 69.23 (L2) Ensure 'Remote Desktop Services UserMode Port Redirector (UmRdpService)' is set to 'Disabled' (Automated) | 766 |
| 69.24 (L1) Ensure 'Remote Procedure Call (RPC) Locator (RpcLocator)' is set to 'Disabled' (Automated) | 768 |
| 69.25 (L2) Ensure 'Remote Registry (RemoteRegistry)' is set to 'Disabled' (Automated) | 770 |
| 69.26 (L1) Ensure 'Routing and Remote Access (RemoteAccess)' is set to 'Disabled' (Automated) | 772 |
| 69.27 (L2) Ensure 'Server (LanmanServer)' is set to 'Disabled' (Automated) | 774 |
| 69.28 (L1) Ensure 'Simple TCP/IP Services (simptcp)' is set to 'Disabled' or 'Not Installed' (Automated) | 776 |
| 69.29 (L2) Ensure 'SNMP Service (SNMP)' is set to 'Disabled' or 'Not Installed' (Automated) | 778 |
| 69.30 (L1) Ensure 'Special Administration Console Helper (sacsrvr)' is set to 'Disabled' or 'Not Installed' (Automated) | 780 |
| 69.31 (L1) Ensure 'SSDP Discovery (SSDPSRV)' is set to 'Disabled' (Automated) | 782 |
| 69.32 (L1) Ensure 'UPnP Device Host (upnphost)' is set to 'Disabled' (Automated)..... | 784 |
| 69.33 (L1) Ensure 'Web Management Service (WMSvc)' is set to 'Disabled' or 'Not Installed' (Automated) | 786 |
| 69.34 (L2) Ensure 'Windows Error Reporting Service (WerSvc)' is set to 'Disabled' (Automated) | 788 |
| 69.35 (L2) Ensure 'Windows Event Collector (Webservice)' is set to 'Disabled' (Automated) | 790 |
| 69.36 (L1) Ensure 'Windows Media Player Network Sharing Service (WMPNetworkSvc)' is set to 'Disabled' or 'Not Installed' (Automated) | 792 |

| | |
|--|------------|
| 69.37 (L1) Ensure 'Windows Mobile Hotspot Service (icssvc)' is set to 'Disabled' (Automated) | 794 |
| 69.38 (L2) Ensure 'Windows Push Notifications System Service (WpnService)' is set to 'Disabled' (Automated) | 796 |
| 69.39 (L2) Ensure 'Windows PushToInstall Service (PushToInstall)' is set to 'Disabled' (Automated) | 798 |
| 69.40 (L2) Ensure 'Windows Remote Management (WS-Management) (WinRM)' is set to 'Disabled' (Automated) | 800 |
| 69.41 (L1) Ensure 'World Wide Web Publishing Service (W3SVC)' is set to 'Disabled' or 'Not Installed' (Automated) | 802 |
| 69.42 (L1) Ensure 'Xbox Accessory Management Service (XboxGipSvc)' is set to 'Disabled' (Automated) | 804 |
| 69.43 (L1) Ensure 'Xbox Live Auth Manager (XblAuthManager)' is set to 'Disabled' (Automated) | 806 |
| 69.44 (L1) Ensure 'Xbox Live Game Save (XblGameSave)' is set to 'Disabled' (Automated) | 808 |
| 69.45 (L1) Ensure 'Xbox Live Networking Service (XboxNetApiSvc)' is set to 'Disabled' (Automated) | 810 |
| 70 Task Scheduler | 812 |
| 71 Text Input | 812 |
| 72 Time Language Settings..... | 812 |
| 73 Troubleshooting | 812 |
| 74 User Rights | 812 |
| 74.1 (L1) Ensure 'Access Credential Manager As Trusted Caller' is set to 'No One' (Automated) | 813 |
| 74.2 (L1) Ensure 'Access From Network' is set to 'Administrators, Remote Desktop Users' (Automated) | 815 |
| 74.3 (L1) Ensure 'Act As Part Of The Operating System' is set to 'No One' (Automated) | 818 |
| 74.4 (L1) Ensure 'Allow Local Log On' is set to 'Administrators, Users' (Automated) | 820 |
| 74.5 (L1) Ensure 'Backup Files And Directories' is set to 'Administrators' (Automated) | 822 |
| 74.6 (L1) Ensure 'Change System Time' is set to 'Administrators, LOCAL SERVICE' (Automated) | 824 |
| 74.7 (L1) Ensure 'Create Global Objects' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' (Automated) | 827 |
| 74.8 (L1) Ensure 'Create Page File' is set to 'Administrators' (Automated) | 829 |
| 74.9 (L1) Ensure 'Create Permanent Shared Objects' is set to 'No One' (Automated) | 831 |
| 74.10 (L1) Configure 'Create Symbolic Links' (Automated) | 833 |
| 74.11 (L1) Ensure 'Create Token' is set to 'No One' (Automated) | 835 |
| 74.12 (L1) Ensure 'Debug Programs' is set to 'Administrators' (Automated) | 837 |
| 74.13 (L1) Ensure 'Deny Access From Network' to include 'Guests, Local account' (Automated) | 839 |
| 74.14 (L1) Ensure 'Deny Local Log On' to include 'Guests' (Automated) | 841 |
| 74.15 (L1) Ensure 'Deny Remote Desktop Services Log On' to include 'Guests, Local account' (Automated) | 843 |
| 74.16 (L1) Ensure 'Enable Delegation' is set to 'No One' (Automated) | 845 |
| 74.17 (L1) Ensure 'Generate Security Audits' is set to 'LOCAL SERVICE, NETWORK SERVICE' (Automated) | 847 |
| 74.18 (L1) Ensure 'Impersonate Client' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' (Automated) | 849 |
| 74.19 (L1) Ensure 'Increase Scheduling Priority' is set to 'Administrators, Window Manager\Window Manager Group' (Automated) | 851 |
| 74.20 (L1) Ensure 'Load Unload Device Drivers' is set to 'Administrators' (Automated) | 853 |
| 74.21 (L1) Ensure 'Lock Memory' is set to 'No One' (Automated) | 855 |
| 74.22 (L1) Ensure 'Manage auditing and security log' is set to 'Administrators' (Automated) | 857 |

| | |
|---|------------|
| 74.23 (L1) Ensure 'Manage Volume' is set to 'Administrators' (Automated) | 859 |
| 74.24 (L1) Ensure 'Modify Firmware Environment' is set to 'Administrators' (Automated) | 861 |
| 74.25 (L1) Ensure 'Modify Object Label' is set to 'No One' (Automated) | 863 |
| 74.26 (L1) Ensure 'Profile Single Process' is set to 'Administrators' (Automated) | 865 |
| 74.27 (L1) Ensure 'Remote Shutdown' is set to 'Administrators' (Automated) | 867 |
| 74.28 (L1) Ensure 'Restore Files And Directories' is set to 'Administrators' (Automated) | 869 |
| 74.29 (L1) Ensure 'Take Ownership' is set to 'Administrators' (Automated) | 871 |
| 75 Virtualization Based Technology..... | 873 |
| 76 Wi-Fi Settings..... | 873 |
| 77 Widgets..... | 873 |
| 78 Windows Defender Security Center | 873 |
| 78.1 (L1) Ensure 'Disallow Exploit Protection Override' is set to '(Enable)' (Automated) | 874 |
| 79 Windows Hello For Business..... | 876 |
| 79.1 (L1) Ensure 'Facial Features Use Enhanced Anti Spoofing' is set to 'true' (Automated) | 877 |
| 79.2 (L1) Ensure 'Minimum PIN Length' is set to '6 more character(s)' (Automated)..... | 879 |
| 79.3 (L1) Ensure 'Require Security Device' is set to 'true' (Automated) | 881 |
| 80 Windows Ink Workspace | 883 |
| 80.1 (L2) Ensure 'Allow suggested apps in Windows Ink Workspace' is set to 'Block' (Automated) | 884 |
| 80.2 (L1) Ensure 'Allow Windows Ink Workspace' is set to 'Enabled: but the user can't access it above the lock screen' OR 'Disabled' (Automated)..... | 886 |
| 81 Windows Logon | 888 |
| 82 Windows Subsystem For Linux..... | 888 |
| 83 Windows Update For Business..... | 888 |
| 83.1 (L1) Ensure 'Allow Auto Update' is set to 'Enabled' (Automated) | 889 |
| 83.2 (L1) Ensure 'Defer Feature Updates Period in Days' is set to 'Enabled: 180 or more days' (Automated) | 891 |
| 83.3 (L1) Ensure 'Defer Quality Updates Period (Days)' is set to 'Enabled: 0 days' (Automated) | 893 |
| 83.4 (L1) Ensure 'Manage preview builds' is set to 'Disable Preview builds' (Automated) | 895 |
| 83.5 (L1) Ensure 'Scheduled Install Day' is set to 'Every day' (Automated) | 897 |
| 83.6 (L1) Ensure 'Block "Pause Updates" ability' is set to 'Block' (Automated) | 899 |
| 84 Wireless Display | 901 |
| 85 Windows LAPS | 901 |
| 85.1 (L1) Ensure 'Backup Directory' is set to 'Backup the password to Azure AD only' (Automated) | 902 |
| 85.2 (L1) Ensure 'Password Age Days' is set to 'Configured: 30 or fewer' (Automated) | 904 |
| 85.3 (L1) Ensure 'Password Complexity' is set to 'Large letters + small letters + numbers + special characters' (Automated) | 906 |
| 85.4 (L1) Ensure 'Password Length' is set to 'Configured: 15 or more' (Automated)..... | 908 |
| 85.5 (L1) Ensure 'Post-authentication actions' is set to 'Reset the password and logoff the managed account' or higher (Automated) | 910 |
| 85.6 (L1) Ensure 'Post Authentication Reset Delay' is set to 'Configured: 8 or fewer hours, but not 0' (Automated) | 912 |
| 86 Miscellaneous Recommendations..... | 914 |
| 86.1 Custom Profile..... | 914 |
| 86.1.1 (L2) Ensure 'Allow a Windows app to share application data between users' is set to 'Disabled' (Automated)..... | 915 |

| | |
|---|------------|
| 86.1.2 (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) | 917 |
| 86.1.3 (L2) Ensure 'Configure Authenticated Proxy usage for the Connected User Experience and Telemetry service' is set to 'Enabled: Disable Authenticated Proxy usage' (Automated) | 919 |
| 86.1.4 (BL) Ensure 'Enumeration policy for external devices incompatible with Kernel DMA Protection' is set to 'Enabled: Block All' (Automated) | 921 |
| 86.1.5 (L1) Ensure 'Prevent non-admin users from installing packaged Windows apps' is set to 'Enabled' (Automated) | 923 |
| 86.1.6 (L2) Ensure 'Turn off location' is set to 'Enabled' (Automated) | 925 |
| 86.1.7 (L1) Ensure 'Turn off Microsoft consumer experiences' is set to 'Enabled' (Automated) | 927 |
| 86.1.8 (L2) Ensure 'Turn off notifications network usage' is set to 'Enabled' (Automated) | 929 |
| Appendix: Summary Table | 931 |
| Appendix: Change History | 994 |

Overview

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

- Monitoring the base operating system for vulnerabilities and quickly updating with the latest security patches
- Monitoring applications and libraries for vulnerabilities and quickly updating with the latest security patches

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

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

This secure configuration guide is based on **Windows 10** and is intended for all versions of the **Windows 10** operating system, including older versions. This secure configuration guide was tested against **Microsoft Windows 10 Release 22H2 Enterprise**.

Intune is continually updating to support settings that are backed by group policy. This benchmark is based off settings that were available via Intune configuration profiles at the time of publication.

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

This CIS Microsoft Windows Benchmark is written for MDM-joined systems using Intune's (Microsoft Endpoint Manager) configuration profiles and not domain-joined or stand-alone systems.

Consensus Guidance

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

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

Typographical Conventions

The following typographical conventions are used throughout this guide:

| Convention | Meaning |
|--|---|
| Stylized Monospace font | Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented. |
| Monospace font | Used for inline code, commands, 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 |

Recommendation Definitions

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

Title

Concise description for the recommendation's intended configuration.

Assessment Status

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

Automated

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

Manual

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

Profile

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

Description

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

Rationale Statement

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

Impact Statement

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

Audit Procedure

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

Remediation Procedure

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

Default Value

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

References

Additional documentation relative to the recommendation.

CIS Critical Security Controls® (CIS Controls®)

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

Additional Information

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

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1 (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 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.

- **Next Generation Windows Security (NG)**

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.

- **BitLocker (BL)**

This profile includes BitLocker-related recommendations.

Acknowledgements

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

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

Editor

Caleb Eifert
Jennifer Jarose
Matthew Woods

Contributor

Phil Chatham
Haemish Edgerton
Hardeep Mehrotara
Phil White
Kevin Zhang

Recommendations

1 Above Lock

This section contains recommendations for Above Lock.

1.1 (L1) Ensure 'Allow Cortana Above Lock' is set to 'Block' (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: Block.

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:

1. Navigate to the following registry location and note the *WinningProvider* GUID. This value confirms under which User GUID the policy is set.

HKLM\SOFTWARE\Microsoft\PolicyManager\current\device\AboveLock:AllowCortanaAboveLock_WinningProvider

2. Navigate to the following registry location and confirm the value is set to 0.

HKLM\SOFTWARE\Microsoft\PolicyManager\Providers\{GUID}\Default\Device\AboveLock:AllowCortanaAboveLock

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Block.

Above Lock\Allow Cortana Above Lock

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 |
|------------------|--|------|------|------|
| 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 | 16.11 <u>Lock Workstation Sessions After Inactivity</u> Automatically lock workstation sessions after a standard period of inactivity. | ● | ● | ● |

2 Accounts

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

3 Administrative Templates

This section contains recommendations for Administrative Templates.

3.1 Control Panel

This section contains recommendations for Control Panel.

3.1.1 Add or Remove Programs

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

3.1.2 Display

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

3.1.3 Personalization

This section contains recommendations for Personalization.

3.1.3.1 (L1) Ensure 'Enable screen saver (User)' 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 with a REG_SZ value of 1.

HKU\ [USER SID]\Software\Policies\Microsoft\Windows\Control Panel\Desktop:ScreenSaveActive

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

Administrative Templates\Control Panel\Personalization\Enable screen saver (User)

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 | <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> | ● | ● | ● |

3.1.3.2 (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 with a REG_DWORD value of 1.

HKLM\SOFTWARE\Policies\Microsoft\Windows\Personalization>NoLockScreenCamera

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

Administrative Templates\Control Panel\Personalization\Prevent enabling lock screen camera

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 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| v7 | 16.11 <u>Lock Workstation Sessions After Inactivity</u> Automatically lock workstation sessions after a standard period of inactivity. | ● | ● | ● |

3.1.3.3 (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 with a REG_DWORD value of 1.

HKLM\SOFTWARE\Policies\Microsoft\Windows\Personalization>NoLockScreenSlidesho
w

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

Administrative Templates\Control Panel\Personalization\Prevent enabling lock screen slide show

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 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| v7 | 16.11 <u>Lock Workstation Sessions After Inactivity</u> Automatically lock workstation sessions after a standard period of inactivity. | ● | ● | ● |

3.1.4 Printers

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

3.1.5 Programs

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

3.1.6 Regional and Language Options

This section contains recommendations for Regional and Language Options.

3.1.6.1 Handwriting personalization

This section contains recommendations for Handwriting personalization.

3.1.7 User Account

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

3.2 Desktop

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

3.3 LAPS (legacy)

This section was for the legacy Microsoft LAPS, which was replaced by Windows LAPS. This section is intentionally blank and exists to ensure the structure of the Intune benchmarks are consistent.

3.4 MS Security Guide

This section contains recommendations for MS Security Guide.

3.4.1 (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 with a REG_DWORD value of 0.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:LocalAccountTokenFilterPolicy
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

```
Administrative Templates\MS Security Guide\Apply UAC restrictions to local accounts on network logons
```

Default Value:

Enabled. (UAC token-filtering is applied to local accounts on network logons. Membership in powerful groups such as Administrators and disabled and powerful privileges are removed from the resulting access token.)

References:

1. <https://learn.microsoft.com/en-us/windows/security/identity-protection/access-control/local-accounts>
2. <https://techcommunity.microsoft.com/t5/microsoft-security-baselines/disabling-smbv1-through-group-policy/ba-p/701069>

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| 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. | ● | ● | ● |

3.4.2 (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 with a REG_DWORD value of 4.

HKLM\SYSTEM\CurrentControlSet\Services\mrxsmb10:Start

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled: Disable driver (recommended).

Administrative Templates\MS Security Guide\Configure SMB v1 client driver

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 or newer: Enabled: Disable driver.

References:

1. <https://techcommunity.microsoft.com/t5/microsoft-security-baselines/disabling-smbv1-through-group-policy/ba-p/701069>
2. <https://learn.microsoft.com/en-us/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3>

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. | | ● | ● |

3.4.3 (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 with a REG_DWORD value of 0.

HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters:SMB1

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`.

Administrative Templates\MS Security Guide\Configure SMB v1 server

Default Value:

Windows 10 R1703 and older: Enabled.

Windows 10 R1709 or newer: Disabled.

References:

1. <https://techcommunity.microsoft.com/t5/microsoft-security-baselines/disabling-smbv1-through-group-policy/ba-p/701069>

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. | | ● | ● |

3.4.4 (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 with a REG_DWORD value of 0.

HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\kernel:DisableExceptionChainValidation

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

Administrative Templates\MS Security Guide\Enable Structured Exception Handling Overwrite Protection (SEHOP)

More information is available at [MSKB 956607: How to enable Structured Exception Handling Overwrite Protection \(SEHOP\) in Windows operating systems](#)

Default Value:

Disabled for 32-bit processes.

References:

1. <https://learn.microsoft.com/en-us/windows/security/threat-protection/override-mitigation-options-for-app-related-security-policies>

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. | | ● | ● |

3.4.5 (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 or 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 with a REG_DWORD value of 0.

```
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest:UseLogonCredential
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to **Disabled**.

Administrative Templates\MS Security Guide\WDigest Authentication (disabling may require KB2871997)

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 or newer: Disabled. (Lsass.exe does not retain a copy of the user's plaintext password in memory.)

References:

1. <https://www.microsoft.com/en-us/download/details.aspx?id=36036>
2. <https://support.microsoft.com/en-us/topic/microsoft-security-advisory-update-to-improve-credentials-protection-and-management-may-13-2014-93434251-04ac-b7f3-52aa-9f951c14b649>

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. | ● | | ● |

3.5 MSS (Legacy)

This section contains recommendations for the Microsoft Solutions for Security (MSS) settings.

3.5.1 (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.

Warning: [Windows Autopilot - Policy Conflicts](#): Windows Autopilot pre-provisioning doesn't work when this GPO policy settings is enabled. An exception to this recommendation will be needed if Windows AutoPilot is used.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a REG_DWORD value of 0.

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon:AutoAdminLogon

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled.

Administrative Templates\MSS (Legacy)\MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)

Default Value:

Disabled.

References:

1. <https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/recovery-console-allow-automatic-administrative-logon>
2. <https://techcommunity.microsoft.com/t5/microsoft-security-baselines/the-mss-settings/ba-p/701055>

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. | ● | ● | ● |

3.5.2 (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 with a REG_DWORD value of 2.

```
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters:DisableIPSourceRouting
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled: Highest protection, source routing is completely disabled.

```
Administrative Templates\MSS (Legacy)\MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)
```

Default Value:

No additional protection, source routed packets are allowed.

References:

1. <https://techcommunity.microsoft.com/t5/microsoft-security-baselines/the-mss-settings/ba-p/701055>

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| v7 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |

3.5.3 (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 with a REG_DWORD value of 2.

HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters:DisableIPSourceRouting

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled: Highest protection, source routing is completely disabled.

Administrative Templates\MSS (Legacy)\MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)

Default Value:

Medium, source routed packets ignored when IP forwarding is enabled.

References:

1. <https://techcommunity.microsoft.com/t5/microsoft-security-baselines/the-mss-settings/ba-p/701055>

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| v7 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |

3.5.4 (L2) Ensure 'MSS: (DisableSavePassword) Prevent the dial-up password from being saved (recommended)' 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 with a REG_DWORD value of 1.

HKLM\SYSTEM\CurrentControlSet\Services\RasMan\Parameters:DisableSavePassword

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

Administrative Templates\MSS (Legacy)\MSS:(DisableSavePassword) Prevent the dial-up password from being saved (recommended)

Default Value:

Disabled. (Saving of dial-up and VPN passwords is allowed.)

References:

1. <https://techcommunity.microsoft.com/t5/microsoft-security-baselines/the-mss-settings/ba-p/701055>

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. | ● | ● | ● |
| v7 | 5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software. | ● | ● | ● |

3.5.5 (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. This group policy setting is backed by the following registry location with a REG_DWORD value of 0.

HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters:EnableICMPRedirect

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`.

```
Administrative Templates\{MSS (Legacy)\}\MSS: (EnableICMPRedirect) Allow ICMP  
redirects to override OSPF generated routes
```

Default Value:

Enabled. (ICMP redirects can override OSPF-generated routes.)

References:

1. <https://techcommunity.microsoft.com/t5/microsoft-security-baselines/the-mss-settings/ba-p/701055>

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. | ● | ● | ● |
| 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. | | ● | ● |

3.5.6 (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 with a REG_DWORD value of 300000.

HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters:KeepAliveTime

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled: 300,000 or 5 minutes (recommended).

Administrative Templates\MSS (Legacy)\MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds

Default Value:

7,200,000 milliseconds or 120 minutes.

References:

1. <https://techcommunity.microsoft.com/t5/microsoft-security-baselines/the-mss-settings/ba-p/701055>

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| v7 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |

3.5.7 (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 with a REG_DWORD value of 1.

HKLM\SYSTEM\CurrentControlSet\Services\NetBT\Parameters:NoNameReleaseOnDemand

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

Administrative Templates\一贯性 (Legacy)\一贯性: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers

Default Value:

Enabled.

References:

1. <https://techcommunity.microsoft.com/t5/microsoft-security-baselines/the-mss-settings/ba-p/701055>

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|------|------|------|
| v8 | <u>4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure</u> Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. | ● | ● | ● |
| v7 | <u>5.1 Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software. | ● | ● | ● |

3.5.8 (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 with a REG_DWORD value of 0.

```
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters:PerformRouterDiscover  
y
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to **Disabled**.

```
Administrative Templates\MSS (Legacy)\MSS: (PerformRouterDiscovery) Allow  
IRDP to detect and configure Default Gateway addresses (could lead to DoS)
```

Default Value:

Enable only if DHCP sends the Perform Router Discovery option.

References:

1. <https://techcommunity.microsoft.com/t5/microsoft-security-baselines/the-mss-settings/ba-p/701055>

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. | | ● | ● |

3.5.9 (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/dlls/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 with a REG_DWORD value of 1.

HKLM\SYSTEM\CurrentControlSet\Control\Session Manager:SafeDllSearchMode

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

Administrative Templates\MSS (Legacy)\MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)

Default Value:

Enabled.

References:

1. <https://techcommunity.microsoft.com/t5/microsoft-security-baselines/the-mss-settings/ba-p/701055>

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. | | ● | ● |

3.5.10 (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 with a REG_DWORD value of 5.

| |
|--|
| HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon:ScreenSaverGracePeriod |
|--|

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled: 5 or fewer seconds.

| |
|--|
| Administrative Templates\MSS (Legacy)\MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended) |
|--|

Default Value:

5 seconds.

References:

1. <https://techcommunity.microsoft.com/t5/microsoft-security-baselines/the-mss-settings/ba-p/701055>

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. | ● | ● | ● |

**3.5.11 (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 with a REG_DWORD value of 3.

HKLM\SYSTEM\CurrentControlSet\Services\TCPIP6\Parameters:TcpMaxDataRetransmissions

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled: 3.

Administrative Templates\MSS (Legacy)\MSS: (TcpMaxDataRetransmissions IPv6)
How many times unacknowledged data is retransmitted

Default Value:

5 times.

References:

1. <https://techcommunity.microsoft.com/t5/microsoft-security-baselines/the-mss-settings/ba-p/701055>

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|------|------|------|
| v8 | 4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. | ● | ● | ● |
| v7 | 11.1 Maintain Standard Security Configurations for Network Devices Maintain standard, documented security configuration standards for all authorized network devices. | | ● | ● |

3.5.12 (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 with a REG_DWORD value of 3.

HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters:TcpMaxDataRetransmissions

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled: 3.

Administrative Templates\MSS (Legacy)\MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted

Default Value:

5 times.

References:

1. <https://techcommunity.microsoft.com/t5/microsoft-security-baselines/the-mss-settings/ba-p/701055>

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|------|------|------|
| v8 | 4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. | ● | ● | ● |
| v7 | 11.1 Maintain Standard Security Configurations for Network Devices Maintain standard, documented security configuration standards for all authorized network devices. | | ● | ● |

3.5.13 (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 with a REG_DWORD value of 90.

HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\Security:WarningLevel

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled: 90% or less.

Administrative Templates\一贯性 (Legacy)\一贯性: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning

Default Value:

0%. (No warning event is generated.)

References:

1. <https://techcommunity.microsoft.com/t5/microsoft-security-baselines/the-mss-settings/ba-p/701055>

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|------|------|------|
| v8 | 8.3 Ensure Adequate Audit Log Storage Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process. | ● | ● | ● |
| v7 | 6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements. | | ● | ● |
| v7 | 6.4 Ensure adequate storage for logs Ensure that all systems that store logs have adequate storage space for the logs generated. | | ● | ● |

3.6 Network

This section contains recommendations for Network.

3.6.1 Background Intelligent Transfer Service (BITS)

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

3.6.2 BranchCache

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

3.6.3 DirectAccess Client Experience Settings

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

3.6.4 DNS Client

This section contains recommendations for DNS Client.

3.6.4.1 (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 with a REG_DWORD value of 0.

| |
|---|
| HKLM\SOFTWARE\Policies\Microsoft\Windows NT\DNSClient:EnableMulticast |
|---|

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

Administrative Templates\Network\DNS Client\Turn off multicast name resolution

Default Value:

Disabled. (LLMNR will be enabled on all available network adapters.)

References:

1. https://learn.microsoft.com/en-usopenspecs/windows_protocols/ms-llmnrp/02b1d227-d7a2-4026-9fd6-27ea5651fe85

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. | ● | ● | ● |

3.6.5 Hotspot Authentication

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

3.6.6 Lanman Server

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

3.6.7 Lanman Workstation

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

3.6.8 Link-Layer Topology Discovery

This section contains recommendations for Link-Layer Topology Discovery.

3.6.8.1 (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 with a REG_DWORD value of 0.

```
HKLM\Software\Policies\Microsoft\Windows\LLTD:AllowLLTDIOOnDomain  
HKLM\Software\Policies\Microsoft\Windows\LLTD:AllowLLTDIOOnPublicNet  
HKLM\Software\Policies\Microsoft\Windows\LLTD:EnableLLTDIO  
HKLM\Software\Policies\Microsoft\Windows\LLTD:ProhibitLLTDIOOnPrivateNet
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to **Disabled**.

```
Administrative Templates\Network\Link-Layer Topology Discovery\Turn on Mapper  
I/O (LLTDIO) driver
```

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 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| v7 | 5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software. | ● | ● | ● |

3.6.8.2 (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 with a REG_DWORD value of 0.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\LLTD:AllowRspndrOnDomain  
HKLM\SOFTWARE\Policies\Microsoft\Windows\LLTD:AllowRspndrOnPublicNet  
HKLM\SOFTWARE\Policies\Microsoft\Windows\LLTD:EnableRspndr  
HKLM\SOFTWARE\Policies\Microsoft\Windows\LLTD:ProhibitRspndrOnPrivateNet
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to **Disabled**.

```
Administrative Templates\Network\Link-Layer Topology Discovery\Turn on Responder
```

Default Value:

Disabled. (The Responder (RSPNDR) network protocol driver is turned off.)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| v7 | 5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software. | ● | ● | ● |

3.6.9 Network Connections

This section contains recommendations for Network Connections.

3.6.9.1 (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 with a REG_DWORD value of 0.

| |
|---|
| HKLM\SOFTWARE\Policies\Microsoft\Windows\Network Connections:NC_AllowNetBridge_NLA |
|---|

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

Administrative Templates\Network\Network Connections\Prohibit installation and configuration of Network Bridge on your DNS domain network

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 | <u>4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure</u> Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. | ● | ● | ● |
| v7 | <u>11.3 Use Automated Tools to Verify Standard Device Configurations and Detect Changes</u> Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviations are discovered. | | ● | ● |

3.6.9.2 (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 with a REG_DWORD value of 0.

HKLM\SOFTWARE\Policies\Microsoft\Windows\Network
Connections:NC_ShowSharedAccessUI

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

Administrative Templates\Network\Network Connections\Prohibit use of Internet Connection Sharing on your DNS domain network

Default Value:

Disabled. (All users are allowed to turn on Mobile Hotspot.)

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> | ● | ● | ● |

3.6.9.3 (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 with a REG_DWORD value of 1.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\Network  
Connections:NC_StdDomainUserSetLocation
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

```
Administrative Templates\Network\Network Connections\Require domain users to  
elevate when setting a network's location
```

Default Value:

Disabled. (Users can set a network's location without elevating.)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| 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. | ● | ● | ● |

3.6.10 Network Connectivity Status Indicator

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

3.6.11 Network Provider

This section contains recommendations for Network Provider.

3.6.11.1 (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 "Require 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.

Note #2: If the environment is 100% managed by Intune these shares will not be available. An exception to this recommendation will be needed.

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 with a REG_SZ value of `RequireMutualAuthentication=1, RequireIntegrity=1`.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths:\*\NETLOGON  
HKLM\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths:\*\SYSVOL
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled with the following paths configured, at a minimum:
`*\NETLOGON RequireMutualAuthentication=1, RequireIntegrity=1`
`*\SYSVOL RequireMutualAuthentication=1, RequireIntegrity=1`

```
Administrative Templates\Network\Network Provider\Hardened UNC Paths
```

Default Value:

Disabled. (No UNC paths are hardened.)

References:

1. https://learn.microsoft.com/en-usopenspecs/windows_protocols/ms-dfsc/149a3039-98ce-491a-9268-2f5ddef08192

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| v7 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |

3.6.12 Offline Files

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

3.6.13 QoS Packet Scheduler

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

3.6.14 SNMP

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

3.6.15 SSL Configuration Settings

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

3.6.16 TCPIP Settings

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

3.6.17 Windows Connect Now

This section contains recommendations for Windows Connect Now.

3.6.17.1 (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 with a REG_DWORD value of 0.

```
HKLM\Software\Policies\Microsoft\Windows\WCN\Registrars:EnableRegistrars  
HKLM\Software\Policies\Microsoft\Windows\WCN\Registrars:DisableUPnPRegistrar  
HKLM\Software\Policies\Microsoft\Windows\WCN\Registrars:DisableInBand802DOT11  
Registrar  
HKLM\Software\Policies\Microsoft\Windows\WCN\Registrars:DisableFlashConfigReg  
istrar  
HKLM\Software\Policies\Microsoft\Windows\WCN\Registrars:DisableWPDRegistrar
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to **Disabled**.

```
Administrative Templates\Network\Windows Connect Now\Configuration of  
wireless settings using Windows Connect Now
```

Default Value:

WCN operations are enabled and allowed over all media.

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>15.4 <u>Disable Wireless Access on Devices if Not Required</u></p> <p>Disable wireless access on devices that do not have a business purpose for wireless access.</p> | ● | ● | ● |
| v7 | <p>15.5 <u>Limit Wireless Access on Client Devices</u></p> <p>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.</p> | ● | ● | ● |

3.6.17.2 (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 with a REG_DWORD value of 1.

HKLM\SOFTWARE\Policies\Microsoft\Windows\WCN\UI:DisableWcnUi

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

Administrative Templates\Network\Windows Connect Now\Prohibit access of the Windows Connect Now wizards

Default Value:

Disabled. (Users can access all WCN wizard tasks.)

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. | ● | ● | ● |

3.6.18 Windows Connection Manager

This section contains recommendations for Windows Connection Manager.

3.6.18.1 (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 with a REG_DWORD value of 3.

HKLM\SOFTWARE\Policies\Microsoft\Windows\WcmSvc\GroupPolicy:fMinimizeConnections

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled: 3 = Prevent Wi-Fi when on Ethernet.

Administrative Templates\Network\Windows Connection Manager\Minimize the number of simultaneous connections to the Internet or a Windows Domain

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 |
|------------------|---|------|------|------|
| v8 | 4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. | ● | ● | ● |
| 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. | | | ● |

3.6.18.2 (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 with a REG_DWORD value of 1.

HKLM\SOFTWARE\Policies\Microsoft\Windows\WcmSvc\GroupPolicy:fBlockNonDomain

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

Administrative Templates\Network\Windows Connection Manager\Prohibit connection to non-domain networks when connected to domain authenticated network

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 |
|------------------|--|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| v7 | 12.4 <u>Deny Communication over Unauthorized Ports</u> 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. | ● | ● | ● |

3.6.19 Wireless Display

This section contains recommendations for Wireless Display.

3.6.19.1 (L1) Ensure 'Require PIN pairing' is set to 'Enabled' (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.

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:

1. Navigate to the following registry location and note the *WinningProvider* GUID. This value confirms under which User GUID the policy is set.

HKLM\SOFTWARE\Microsoft\PolicyManager\current\device\ADMX_wlansvc:SetPINEnforced_WinningProvider

2. Navigate to the following registry location and confirm the value is set to <enabled/>.

HKLM\SOFTWARE\Microsoft\PolicyManager\Providers\{GUID}\Default\Device\ADMX_wlansvc:SetPINEnforced

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

Administrative Templates\Network\Wireless Display\Require pin pairing

Default Value:

Disabled. (A PIN is not required for pairing to a wireless display device.)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| v7 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |

3.7 Printers

This section contains recommendations for Printers.

3.7.1 (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 location with a REG_DWORD value of 2.

| |
|--|
| HKLM\Software\Policies\Microsoft\Windows NT\Printers:RegisterSpoolerRemoteRpcEndPoint |
|--|

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to **Disabled**.

| |
|--|
| Administrative Templates\Printers\Allow Print Spooler to accept client connections |
|--|

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 |
|------------------|---|------|------|------|
| v8 | 4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. | ● | ● | ● |
| 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. | ● | ● | ● |

3.7.2 (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 with a REG_DWORD value of 0.

```
HKLM\Software\Policies\Microsoft\Windows  
NT\Printers\PointAndPrint:NoWarningNoElevationOnInstall
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled: Show warning and elevation prompt.

Administrative Templates\Printers\Point and Print Restrictions: When installing drivers for a new connection

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>

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| v7 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |

3.7.3 (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 with a REG_DWORD value of 0.

| |
|--|
| HKLM\Software\Policies\Microsoft\Windows NT\Printers\PointAndPrint:UpdatePromptSettings |
|--|

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled: Show warning and elevation prompt.

Administrative Templates\Printers\Point and Print Restrictions: When updating drivers for an existing connection

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>

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| v7 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |

3.8 Shared Folders

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

3.9 Start Menu and Taskbar

This section contains recommendations for Start Menu and Taskbar.

3.9.1 Notifications

This section contains recommendations for Notifications.

3.9.1.1 (L1) Ensure 'Turn off toast notifications on the lock screen (User)' 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 with a REG_DWORD value of 1.

```
HKU\ [USER  
SID]\Software\Policies\Microsoft\Windows\CurrentVersion\PushNotifications:NoT  
oastApplicationNotificationOnLockScreen
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

```
Administrative Templates\Start Menu and Taskbar\Notifications\Turn off toast  
notifications on the lock screen (User)
```

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 |
|------------------|--|------|------|------|
| 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 | 16.11 <u>Lock Workstation Sessions After Inactivity</u> Automatically lock workstation sessions after a standard period of inactivity. | ● | ● | ● |

3.10 System

This section contains recommendations for System.

3.10.1 Access-Denied Assistance

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

3.10.2 App-V

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

3.10.3 Application Compatibility Settings

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

3.10.4 Audit Process Creation

This section contains recommendations for Audit Process Creation.

3.10.4.1 (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 with a REG_DWORD value of 1.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\Audit:ProcessCreationIncludeCmdLine_Enabled
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

Administrative Templates\System\Audit Process Creation\Include command line in process creation events

Default Value:

Disabled. (Process command line information will not be included in Audit Process Creation events.)

References:

1. https://learn.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 | 16.4 Encrypt or Hash all Authentication Credentials Encrypt or hash with a salt all authentication credentials when stored. | | ● | ● |

3.10.5 Credentials Delegation

This section contains recommendations for Credentials Delegation.

3.10.5.1 (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 with a REG_DWORD value of 0.

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\CredSSP\Parameters:AllowEncryptionOracle

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled: Force Updated Clients.

Administrative Templates\System\Credentials Delegation\Encryption Oracle Remediation

Default Value:

Without the May 2018 security update: Enabled: Vulnerable (Client applications which use CredSSP will expose the remote servers to attacks by supporting fall back to the insecure versions and services using CredSSP will accept unpatched clients.)

With the May 2018 security update: Enabled: Mitigated (Client applications which use CredSSP will not be able to fall back to the insecure version but services using CredSSP will accept unpatched clients.)

References:

1. <https://learn.microsoft.com/en-us/windows/win32/secauthn/credential-security-support-provider>

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|------|------|------|
| v8 | 10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™. | | ● | ● |
| v7 | 3.4 Deploy Automated Operating System Patch Management Tools Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor. | ● | ● | ● |

3.10.5.2 (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 with a REG_DWORD value of 1.

| |
|--|
| HKLM\SOFTWARE\Policies\Microsoft\Windows\CredentialsDelegation:AllowProtectedCreds |
|--|

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

Administrative Templates\System\Credentials Delegation\Remote host allows delegation of non-exportable credentials

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://learn.microsoft.com/en-us/windows/security/identity-protection/remote-credential-guard>

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| v7 | 16.5 <u>Encrypt Transmittal of Username and Authentication Credentials</u> Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels. | | ● | ● |

3.10.6 Ctrl+Alt+Del Options

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

3.10.7 Device Guard

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

3.10.8 Device Health Attestation Service

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

3.10.9 Device Installation

This section contains recommendations for Device Installation.

3.10.9.1 Device Installation Restrictions

This section contains recommendations for Device Installation Restrictions.

3.10.9.1.1 (BL) Ensure 'Prevent installation of devices that match any of these device IDs' is set to 'Enabled' (Automated)

Profile Applicability:

- BitLocker (BL)

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 (or 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 with a REG_DWORD value of 1.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\DeviceInstall\Restrictions:DenyDeviceIDs
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

```
Administrative Templates\System\Device Installation\Device Installation Restrictions\Prevent installation of devices that match any of these device IDs
```

Default Value:

Disabled. (Devices can be installed and updated as allowed or prevented by other policy settings.)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| v7 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |

3.10.9.1.2 (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:

- BitLocker (BL)

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 (or 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 with a REG_DWORD value of 1.

HKLM\SOFTWARE\Policies\Microsoft\Windows\DeviceInstall\Restrictions:DenyDeviceIDsRetroactive

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled, and check the Also apply to matching devices that are already installed. button.

Administrative Templates\System\Device Installation\Device Installation Restrictions\Prevent installation of devices that match any of these device IDs

Default Value:

False (unchecked). (Pre-existing devices matching the device IDs will not be disabled or removed.)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| v7 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |

3.10.9.1.3 (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:

- BitLocker (BL)

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 (or 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 with a REG_SZ value of `PCI\CC_0C0A`.

HKLM\SOFTWARE\Policies\Microsoft\Windows\DeviceInstall\Restrictions\DenyDeviceIDs:1

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled, and add `PCI\CC_0C0A` to the Device IDs list.

Administrative Templates\System\Device Installation\Device Installation Restrictions\Prevent installation of devices that match any of these device IDs

Default Value:

None. (No device ID types are prevented from installation.)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| v7 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |

3.10.9.1.4 (BL) Ensure 'Prevent installation of devices using drivers that match these device setup classes' is set to 'Enabled' (Automated)

Profile Applicability:

- BitLocker (BL)

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 with a REG_DWORD value of 1.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\DeviceInstall\Restrictions:DenyDeviceClasses
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

```
Administrative Templates\System\Device Installation\Device Installation Restrictions\Prevent installation of devices using drivers that match these device setup classes
```

Default Value:

Disabled. (Devices can be installed and updated as allowed or prevented by other policy settings.)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| v7 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |

3.10.9.1.5 (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:

- BitLocker (BL)

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:

{7ebefbc0-3200-11d2-b4c2-00a0C9697d07}, {c06ff265-ae09-48f0-812c-16753d7cba83},
and {6bdd1fc1-810f-11d0-bec7-08002be2092f}

HKLM\SOFTWARE\Policies\Microsoft\Windows\DeviceInstall\Restrictions:DenyDeviceClassesRetroactive

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled, and check the Also apply to matching devices that are already installed. button.

Administrative Templates\System\Device Installation\Device Installation Restrictions\Prevent installation of devices using drivers that match these device setup classes

Default Value:

False (unchecked). (Pre-existing devices matching the device setup classes will not be disabled or removed.)

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™. | | ● | ● |

3.10.9.1.6 (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:

- BitLocker (BL)

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), *i.LINK* (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 with a REG_SZ value of {d48179be-ec20-11d1-b6b8-00c04fa372a7}, {7ebefbc0-3200-11d2-b4c2-00a0C9697d07}, {c06ff265-ae09-48f0-812c-16753d7cba83}, and {6bdd1fc1-810f-11d0-bec7-08002be2092f}.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\DeviceInstall\Restrictions\DenyDeviceClasses:<numeric value>
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog 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.

```
Administrative Templates\System\Device Installation\Device Installation Restrictions\Prevent installation of devices using drivers that match these device setup classes
```

Default Value:

None. (No device setup classes are prevented from installation.)

Additional Information:

Documented in [MSKB 2516445](#).

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| v7 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |

3.10.9.2 (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 third-party utility software from automatically being installed under the context of the `SYSTEM` account.

Rationale:

Installation of software should be conducted by an authorized system administrator and not a standard user. Allowing automatic third-party software installations under the context of the `SYSTEM` account has potential for allowing unauthorized access via backdoors or installation software bugs.

Impact:

Standard users without administrator privileges will not be able to install associated third-party utility software for peripheral devices. This may limit the use of advanced features of those devices unless/until an administrator installs the associated utility software for the device.

Audit:

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

| |
|--|
| HKLM\SOFTWARE\Policies\Microsoft\Windows\Device Metadata:PreventDeviceMetadataFromNetwork |
|--|

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

Administrative Templates\System\Device Installation\Prevent device metadata retrieval from the Internet

Default Value:

Disabled. (The setting in the Device Installation Settings dialog box controls whether Windows retrieves device metadata from the Internet.)

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 | 10.5 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™. | | ● | ● |

3.10.10 Disk NV Cache

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

3.10.11 Disk Quotas

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

3.10.12 Driver Installation

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

3.10.13 Early Launch Antimalware

This section contains recommendations for Early Launch Antimalware.

3.10.13.1 (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 with a REG_DWORD value of 3.

HKLM\SYSTEM\CurrentControlSet\Policies\EarlyLaunch:DriverLoadPolicy

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled: `Good, unknown and bad but critical.

Administrative Templates\System\Early Launch Antimalware\Boot-Start Driver Initialization Policy

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. | | ● | ● |

3.10.14 Enhanced Storage Access

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

3.10.15 File Classification Infrastructure

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

3.10.16 File Share Shadow Copy Provider

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

3.10.17 Filesystem

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

3.10.18 Folder Redirection

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

3.10.19 Group Policy

This section contains recommendations for Group Policy.

3.10.19.1 (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 registry policies in the background while the computer is in use. When background updates are disabled, registry policy changes will not take effect until the next user logon or system restart.

This setting affects all policy settings within the Administrative Templates folder and any other policies that store values in the registry.

The recommended state for this setting is: Enabled: FALSE (unchecked).

Rationale:

Setting this option to false (unchecked) will ensure that domain registry policy changes are applied more quickly, as compared to waiting until the next user logon or system restart.

Impact:

Group Policy settings within the Administrative Templates folder (and other policies that store values in the registry) will be reapplied even when the system is in use, which may have a slight impact on performance.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a REG_DWORD value of 0.

HKLM\SOFTWARE\Policies\Microsoft\Windows\Group Policy\{35378EAC-683F-11D2-A89A-00C04FBBCFA2}:NoBackgroundPolicy

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled.

Administrative Templates\MSI (Legacy) \

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled, then set the Do not apply during periodic background processing option to FALSE (unchecked).

Administrative Templates\System\Group Policy\Configure registry policy processing

Default Value:

Disabled. (Group policies are not reapplied until the next logon or restart.)

References:

1. [https://learn.microsoft.com/en-us/previous-versions/ms813374\(v=msdn.10\)?redirectedfrom=MSDN](https://learn.microsoft.com/en-us/previous-versions/ms813374(v=msdn.10)?redirectedfrom=MSDN)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. | ● | ● | ● |
| 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. | | ● | ● |

**3.10.19.2 (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 reapplys registry policies even if the registry policies have not changed.

This setting affects all registry policy settings within the Administrative Templates folder and any other policies that store values in the registry.

The recommended state for this setting is: Enabled: TRUE (checked).

Rationale:

Setting this option to true (checked) will ensure unauthorized local changes are reverted to match the domain-based Group Policy settings.

Impact:

Group Policy settings within the Administrative Templates folder (and other policies that store values in the registry) will be reapplied even if they have not been changed, which may cause Group Policy refreshes to take longer.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a REG_DWORD value of 0.

HKLM\SOFTWARE\Policies\Microsoft\Windows\Group Policy\{35378EAC-683F-11D2-A89A-00C04FBBCFA2}:NoGPOListChanges

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled, then set the Process even if the Group Policy objects have not changed option to TRUE (checked).

Administrative Templates\System\Group Policy\Configure registry policy processing

Default Value:

Disabled. (Group policies are not reapplied if they have not been changed.)

References:

1. [https://learn.microsoft.com/en-us/previous-versions/ms813374\(v=msdn.10\)?redirectedfrom=MSDN](https://learn.microsoft.com/en-us/previous-versions/ms813374(v=msdn.10)?redirectedfrom=MSDN)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. | ● | ● | ● |
| 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. | | ● | ● |

3.10.19.3 (L1) Ensure 'Configure security 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 security policies in the background while the computer is in use. When background updates are disabled, updates to security policies will not take effect until the next user logon or system restart.

This setting affects all policy settings that use the built-in security template of Group Policy (e.g. Windows Settings\Security Settings).

The recommended state for this setting is: Enabled: FALSE (unchecked).

Rationale:

Setting this option to false (unchecked) will ensure that domain security policy changes are applied more quickly, as compared to waiting until the next user logon or system restart.

Impact:

Built-in security template settings will be reapplied by Group Policy even when the system is in use, which may have a slight impact on performance.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a REG_DWORD value of 0.

HKLM\SOFTWARE\Policies\Microsoft\Windows\Group Policy\{827D319E-6EAC-11D2-A4EA-00C04F79F83A}:NoBackgroundPolicy

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled, then set the Do not apply during periodic background processing option to FALSE (unchecked).

```
Administrative Templates\System\Group Policy\Configure security policy processing
```

Default Value:

Disabled. (Group policies are not reapplied until the next logon or restart.)

References:

1. [https://learn.microsoft.com/en-us/previous-versions/ms813374\(v=msdn.10\)?redirectedfrom=MSDN](https://learn.microsoft.com/en-us/previous-versions/ms813374(v=msdn.10)?redirectedfrom=MSDN)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. | ● | ● | ● |
| 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. | | ● | ● |

**3.10.19.4 (L1) Ensure 'Configure security policy processing:
Process even if the Group Policy objects have not changed' is set
to 'Enabled: TRUE' (Automated)**

Profile Applicability:

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

Description:

The "Process even if the Group Policy objects have not changed" option updates and reapplies security policies even if the security policies have not changed.

This setting affects all policy settings within the built-in security template of Group Policy (e.g. Windows Settings\Security Settings).

The recommended state for this setting is: Enabled: TRUE (checked).

Rationale:

Setting this option to true (checked) will ensure unauthorized local changes are reverted to match the domain-based Group Policy settings.

Impact:

Built-in security template settings will be reapplied even if they have not been changed, which may cause Group Policy refreshes to take longer.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a REG_DWORD value of 0.

HKLM\SOFTWARE\Policies\Microsoft\Windows\Group Policy\{827D319E-6EAC-11D2-A4EA-00C04F79F83A}:NoGPOListChanges

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled, then set the Process even if the Group Policy objects have not changed option to TRUE (checked).

Administrative Templates\System\Group Policy\Configure security policy processing

Default Value:

Disabled. (Group policies are not reapplied if they have not been changed.)

References:

1. [https://learn.microsoft.com/en-us/previous-versions/ms813374\(v=msdn.10\)?redirectedfrom=MSDN](https://learn.microsoft.com/en-us/previous-versions/ms813374(v=msdn.10)?redirectedfrom=MSDN)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. | ● | ● | ● |
| 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. | | ● | ● |

3.10.19.5 (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 with a REG_DWORD value of 0.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\System:EnableCdp
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to **Disabled**.

```
Administrative Templates\System\Group Policy\Continue experiences on this device
```

Default Value:

The default behavior depends on the Windows edition.

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. | ● | ● | ● |

3.10.19.6 (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 backed by the following registry location with the key not existing.

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:DisableBkGndGroupPolicy

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to **Disabled**.

Administrative Templates\System\Group Policy\Turn off background refresh of Group

Default Value:

Disabled. (Updates can be applied while users are working.)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|------|------|------|
| v8 | <p>4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.</p> | ● | ● | ● |
| 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> | | ● | ● |

3.10.20 Internet Communication Management

This section contains recommendations for Internet Communication Management.

3.10.20.1 Internet Communication settings

This section contains recommendations for Internet Communication settings.

3.10.20.1.1 (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 with a REG_DWORD value of 1.

HKLM\SOFTWARE\Policies\Microsoft\Windows\Explorer:NoUseStoreOpenWith

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off access to the Store

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 |
|------------------|---|------|------|------|
| 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. | ● | ● | |

3.10.20.1.2 (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 with a REG_DWORD value of 1.

HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Printers:DisableWebPnPDownload

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off downloading of print drivers over HTTP

Default Value:

Disabled. (Users can download print drivers over HTTP.)

References:

1. [https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/jj618315\(v=ws.11\)#individual-group-policy-settings-that-affect-computer-configuration](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/jj618315(v=ws.11)#individual-group-policy-settings-that-affect-computer-configuration)
2. [https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/jj618315\(v=ws.11\)#individual-group-policy-settings-that-affect-computer-configuration](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/jj618315(v=ws.11)#individual-group-policy-settings-that-affect-computer-configuration)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| v7 | 2.7 <u>Utilize Application Whitelisting</u> Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets. | | | ● |

3.10.20.1.3 (L2) Ensure 'Turn off Help Experience Improvement Program (User)' 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 with a REG_DWORD value of 1.

HKU\ [USER
SID]\Software\Policies\Microsoft\Assistance\Client\1.0>NoImplicitFeedback

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

Administrative Templates\System\Internet Communication Management\Internet Communication Settings\Turn off Help Experience Improvement Program

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 |
|------------------|--|------|------|------|
| 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. | ● | ● | ● |

3.10.20.1.4 (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 with a REG_DWORD value of 1.

HKLM\SOFTWARE\Policies\Microsoft\Windows\Internet Connection Wizard:ExitOnMSICW

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com

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 |
|------------------|--|------|------|------|
| 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. | ● | ● | ● |

3.10.20.1.5 (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 with a REG_DWORD value of 1.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer>NoWebService
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

```
Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off Internet download for Web publishing and online ordering wizards
```

Default Value:

Disabled. (A list of providers is downloaded when the user uses the web publishing or online ordering wizards.)

References:

1. <https://learn.microsoft.com/en-us/windows/win32/lwef/pubwiz-intro>

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>7.4 <u>Maintain and Enforce Network-Based URL Filters</u></p> <p>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.</p> | ● | ● | ● |

3.10.20.1.6 (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 with a REG_DWORD value of 1.

HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Printers:DisableHTTPPrinting

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off printing over HTTP

Default Value:

Disabled. (Users can choose to print to Internet printers over HTTP.)

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>13.3 <u>Monitor and Block Unauthorized Network Traffic</u></p> <p>Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.</p> | ● | ● | ● |

3.10.20.1.7 (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 with a REG_DWORD value of 1.

HKLM\SOFTWARE\Policies\Microsoft\Windows\Registration Wizard
Control:NoRegistration

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off Registration if URL connection is referring to Microsoft.com

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 |
|------------------|--|------|------|------|
| 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. | ● | ● | ● |

3.10.20.1.8 (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 with a REG_DWORD value of 1.

HKLM\SOFTWARE\Policies\Microsoft\SearchCompanion:DisableContentFileUpdates

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off Search Companion content file updates

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 |
|------------------|---|------|------|------|
| 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> | ● | ● | ● |

3.10.20.1.9 (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 with a REG_DWORD value of 1.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer>NoOnlinePrintsWizard
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

```
Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off the "Order Prints" picture task
```

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 |
|------------------|---|------|------|------|
| 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> | ● | ● | ● |

3.10.20.1.10 (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 with a REG_DWORD value of 1.

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer>NoPublishing
Wizard

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

Administrative Templates\System\Internet Communication Management\Internet
Communication settings\Turn off the "Publish to Web" task for files and
folders

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 |
|------------------|---|------|------|------|
| 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> | ● | ● | ● |

3.10.20.1.11 (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 with a REG_DWORD value of 2.

HKLM\SOFTWARE\Policies\Microsoft\Messenger\Client:CEIP

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off the Windows Messenger Customer Experience Improvement Program

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 |
|------------------|---|------|------|------|
| 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> | ● | ● | ● |

3.10.20.1.12 (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 with a REG_DWORD value of 0.

HKLM\SOFTWARE\Policies\Microsoft\SQMClient\Windows:CEIPEnable

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off Windows Customer Experience Improvement Program

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 |
|------------------|---|------|------|------|
| 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> | ● | ● | ● |

3.10.20.1.13 (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 locations with a REG_DWORD value of 1 (Disabled) and 0 (DoReport).

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\Windows Error Reporting:Disabled  
HKLM\SOFTWARE\Policies\Microsoft\PCHealth\ErrorReporting:DoReport
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

```
Administrative Templates\System\Internet Communication Management\Internet  
Communication settings\Turn off Windows Error Reporting
```

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 |
|------------------|--|------|------|------|
| 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. | ● | ● | ● |

3.10.21 iSCSI

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

3.10.22 KDC

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

3.10.23 Kerberos

This section contains recommendations for Kerberos.

3.10.23.1 (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 location with a REG_DWORD value of 0 (DevicePKInitBehavior) and 1 (DevicePKInitEnabled).

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\kerberos\parameters:DevicePKInitBehavior  
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\kerberos\parameters:DevicePKInitEnabled
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled: Automatic.

```
Administrative Templates\System\Kerberos\Support device authentication using certificate
```

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 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| v7 | 1.6 <u>Address Unauthorized Assets</u> Ensure that unauthorized assets are either removed from the network, quarantined or the inventory is updated in a timely manner. | ● | ● | ● |
| v7 | 1.8 <u>Utilize Client Certificates to Authenticate Hardware Assets</u> Use client certificates to authenticate hardware assets connecting to the organization's trusted network. | | | ● |

3.10.24 Locale Services

This section contains recommendations for Locale Services.

3.10.24.1 (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 with a REG_DWORD value of 1.

HKLM\SOFTWARE\Policies\Microsoft\Control Panel\International:BlockUserInputMethodsForSignIn

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

Administrative Templates\System\Locale Services\Disallow copying of user input methods to the system account for sign-in

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 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| v7 | 16.11 <u>Lock Workstation Sessions After Inactivity</u> Automatically lock workstation sessions after a standard period of inactivity. | ● | ● | ● |

3.10.25 Logon

This section contains recommendations for Logon.

3.10.25.1 (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 with a REG_DWORD value of 1.

HKLM\SOFTWARE\Policies\Microsoft\Windows\System:BlockUserFromShowingAccountDetailsOnSignin

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

Administrative Templates\System\Logon\Block user from showing account details on sign-in

Default Value:

Disabled. (Users may choose to show account details on the sign-in screen.)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|------|------|------|
| v8 | <p>4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.</p> | ● | ● | ● |
| v7 | <p>5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.</p> | ● | ● | ● |

3.10.25.2 (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 with a REG_DWORD value of 1.

HKLM\SOFTWARE\Policies\Microsoft\Windows\System:DontDisplayNetworkSelectionUI

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

Administrative Templates\System\Logon\Do not display network selection UI

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.)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| v7 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |

3.10.25.3 (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 with a REG_DWORD value of 1.

HKLM\SOFTWARE\Policies\Microsoft\Windows\System:DontEnumerateConnectedUsers

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

Administrative Templates\System\Logon\Do not enumerate connected users on domain-joined computers

Default Value:

Disabled. (Connected users will be enumerated on domain-joined computers.)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| v7 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |

3.10.25.4 (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 with a REG_DWORD value of 0.

HKLM\SOFTWARE\Policies\Microsoft\Windows\System:EnumerateLocalUsers

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to **Disabled**.

Administrative Templates\System\Logon\Enumerate local users on domain-joined computers

Default Value:

Disabled. (The Logon UI will not enumerate local users on domain-joined computers.)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| v7 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |

3.10.25.5 (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.

Warning: If the [Self Service Password Reset \(SSPR\)](#) feature is used in Microsoft Entra ID, an exception to this recommendation is needed as it's known to interfere with SSPR.

Rationale:

App notifications might display sensitive business or personal data.

Impact:

No app notifications are displayed on the lock screen.

Audit:

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

HKLM\SOFTWARE\Policies\Microsoft\Windows\System:DisableLockScreenAppNotifications

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

Administrative Templates\System\Logon\Turn off app notifications on the lock screen

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 |
|------------------|--|------|------|------|
| 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 | 16.11 <u>Lock Workstation Sessions After Inactivity</u> Automatically lock workstation sessions after a standard period of inactivity. | ● | ● | ● |

3.10.25.6 (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 with a REG_DWORD value of 1.

HKLM\SOFTWARE\Policies\Microsoft\Windows\System:BlockDomainPicturePassword

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

Administrative Templates\System\Logon\Turn off picture password sign-in

Default Value:

Disabled. (Users can set up and use a picture password.)

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> | | ● | ● |

3.10.25.7 (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 user can sign in using a convenience PIN.

Note: The user's password will be cached in the system vault when using this feature.

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

Rationale:

A PIN is created from a much smaller selection of characters than a password, so in most cases a PIN will be much less robust than a password.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a `REG_DWORD` value of `0`.

`HKLM\SOFTWARE\Policies\Microsoft\Windows\System:AllowDomainPINLogon`

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`.

`Administrative Templates\System\Logon\Turn on convenience PIN sign-in`

Default Value:

`Disabled`. (A user can't set up and use a convenience PIN.)

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> | | ● | ● |

3.10.26 Mitigation Options

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

3.10.27 Net Logon

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

3.10.28 Power Management

This section contains recommendations for Power Management.

3.10.28.1 Button Settings

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

3.10.28.2 Hard Disk Settings

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

3.10.28.3 Notification Settings

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

3.10.28.4 Power Throttling Settings

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

3.10.28.5 Sleep Settings

This section contains recommendations for Sleep Settings.

3.10.28.5.1 (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 with a REG_DWORD value of 0.

```
HKLM\SOFTWARE\Policies\Microsoft\Power\PowerSettings\f15576e8-98b7-4186-b944-eafa664402d9:DCSettingIndex
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to **Disabled**.

```
Administrative Templates\System\Power Management\Sleep Settings\Allow network connectivity during connected-standby (on battery)
```

Default Value:

Enabled. (Network connectivity will be maintained in standby while on battery.)

References:

1. <https://learn.microsoft.com/en-us/windows-hardware/design/device-experiences/modern-standby>

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| 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. | | ● | ● |

3.10.28.5.2 (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 with a REG_DWORD value of 0.

```
HKLM\SOFTWARE\Policies\Microsoft\Power\PowerSettings\f15576e8-98b7-4186-b944-eafa664402d9:ACSettingIndex
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to **Disabled**.

```
Administrative Templates\System\Power Management\Sleep Settings\Allow network connectivity during connected-standby (plugged in)
```

Default Value:

Enabled. (Network connectivity will be maintained in standby while plugged in.)

References:

1. <https://learn.microsoft.com/en-us/windows-hardware/design/device-experiences/modern-standby>

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| 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. | | ● | ● |

3.10.28.5.3 (BL) Ensure 'Allow standby states (S1-S3) when sleeping (on battery)' is set to 'Disabled' (Automated)

Profile Applicability:

- BitLocker (BL)

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 with a REG_DWORD value of 0.

HKLM\SOFTWARE\Policies\Microsoft\Power\PowerSettings\abfc2519-3608-4c2a-94ea-171b0ed546ab:DCSettingIndex

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to **Disabled**.

Administrative Templates\System\Power Management\Sleep Settings\Allow standby states (S1-S3) when sleeping (on battery)

Default Value:

Enabled. (Windows is allowed to use standby states when putting the computer in a sleep state.)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|------|------|------|
| v8 | <p>4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.</p> | ● | ● | ● |
| v7 | <p>5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.</p> | ● | ● | ● |

3.10.28.5.4 (BL) Ensure 'Allow standby states (S1-S3) when sleeping (plugged in)' is set to 'Disabled' (Automated)

Profile Applicability:

- BitLocker (BL)

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 with a REG_DWORD value of 0.

```
HKLM\SOFTWARE\Policies\Microsoft\Power\PowerSettings\abfc2519-3608-4c2a-94ea-171b0ed546ab:ACSettingIndex
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to **Disabled**.

```
Administrative Templates\System\Power Management\Sleep Settings\Allow standby states (S1-S3) when sleeping (plugged in)
```

Default Value:

Enabled. (Windows is allowed to use standby states when putting the computer in a sleep state.)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|------|------|------|
| v8 | <p>4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.</p> | ● | ● | ● |
| v7 | <p>5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.</p> | ● | ● | ● |

3.10.28.5.5 (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 with a REG_DWORD value of 1.

HKLM\SOFTWARE\Policies\Microsoft\Power\PowerSettings\0e796bdb-100d-47d6-a2d5-f7d2daa51f51:DCSettingIndex

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

Administrative Templates\System\Power Management\Sleep Settings\Require a password when a computer wakes (on battery)

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 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| v7 | 16.11 <u>Lock Workstation Sessions After Inactivity</u> Automatically lock workstation sessions after a standard period of inactivity. | ● | ● | ● |

3.10.28.5.6 (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 with a REG_DWORD value of 1.

HKLM\SOFTWARE\Policies\Microsoft\Power\PowerSettings\0e796bdb-100d-47d6-a2d5-f7d2daa51f51:ACSettingIndex

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

Administrative Templates\System\Power Management\Sleep Settings\Require a password when a computer wakes (plugged in)

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 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| v7 | 16.11 <u>Lock Workstation Sessions After Inactivity</u> Automatically lock workstation sessions after a standard period of inactivity. | ● | ● | ● |

3.10.29 Remote Assistance

This section contains recommendations for Remote Assistance.

3.10.29.1 (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 with a REG_DWORD value of 0.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal  
Services:fAllowUnsolicited
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to **Disabled**.

```
Administrative Templates\System\Remote Assistance\Configure Offer Remote  
Assistance
```

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 |
|------------------|--|------|------|------|
| 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. | ● | ● | ● |

3.10.29.2 (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 with a REG_DWORD value of 0.

HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services:fAllowToGetHelp

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to **Disabled**.

Administrative Templates\System\Remote Assistance\Configure Solicited Remote Assistance

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 |
|------------------|---|------|------|------|
| 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> | ● | ● | ● |

3.10.30 Remote Procedure Call

This section contains recommendations for Remote Procedure Call.

3.10.30.1 (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 in effect 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 with a REG_DWORD value of 1.

| |
|--|
| HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Rpc:EnableAuthEpResolution |
|--|

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to DisaEnabled`ed.

Administrative Templates\System\Remote Procedure Call\Enable RPC Endpoint Mapper Client Authentication

Default Value:

Disabled. (RPC clients will not authenticate to the Endpoint Mapper Service, but they will be able to communicate with the Windows NT4 Server Endpoint Mapper Service.)

References:

1. <https://learn.microsoft.com/en-us/windows/win32/rpc/how-rpc-works>

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| 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. | | ● | ● |

3.10.30.2 (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 with a REG_DWORD value of 1.

HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Rpc:RestrictRemoteClients

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled: Authenticated.

Administrative Templates\System\Remote Procedure Call\Restrict
Unauthenticated RPC clients

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.)

References:

1. <https://learn.microsoft.com/en-us/windows/win32/rpc/how-rpc-works>

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| 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. | | ● | ● |

3.10.31 Remote Storage Access

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

3.10.32 Scripts

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

3.10.33 Security Settings

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

3.10.34 Server Manager

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

3.10.35 Shutdown

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

3.10.36 Shutdown Options

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

3.10.37 System Restore

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

3.10.38 Troubleshooting and Diagnostics

This section contains recommendations for Troubleshooting and Diagnostics.

3.10.38.1 Application Compatibility Diagnostic

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

3.10.38.2 Corrupted File Recovery

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

3.10.38.3 Disk Diagnostic

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

3.10.38.4 Fault Tolerant Heap

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

3.10.38.5 Microsoft Support Diagnostic Tool

This section contains recommendations for Microsoft Support Diagnostic Tool.

3.10.38.5.1 (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 third-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 with a REG_DWORD value of 0.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\ScriptedDiagnosticsProvider\Policy:DisableQueryRemoteServer
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`.

```
Administrative Templates\System\Troubleshooting and Diagnostics\Microsoft Support Diagnostic Tool\Microsoft Support Diagnostic Tool: Turn on MSDT interactive communication with support provider
```

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 |
|------------------|---|------|------|------|
| 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> | ● | ● | ● |

3.10.39 Trusted Platform Module Services

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

3.10.40 User Profiles

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

3.10.41 Windows File Protection

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

3.10.42 Windows Time Service

This section contains recommendations for Windows Time Service.

3.10.42.1 Time Providers

This section contains recommendations for Time Providers.

3.10.42.1.1 (L1) Ensure 'Enable Windows NTP Client' is set to 'Enabled' (Automated)

Profile Applicability:

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

Description:

This policy setting specifies whether the Windows NTP Client is enabled. Enabling the Windows NTP Client allows synchronization from a systems computer clock to NTP server(s).

The recommended state for this setting is: Enabled.

Note: If a third-party time provider is used in the environment, an exception to this recommendation will be needed.

Rationale:

A reliable and accurate account of time is important for a number of services and security requirements, including but not limited to distributed applications, authentication services, multi-user databases and logging services. The use of an NTP client (with secure operation) establishes functional accuracy and is a focal point when reviewing security relevant events.

Impact:

System time will be synced to the configured NTP server(s).

Audit:

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

HKLM\SOFTWARE\Policies\Microsoft\W32Time\TimeProviders\NtpClient:Enabled

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

Administrative Templates\System\Windows Time Service\Time Providers\Enable Windows NTP Client

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. | | ● | ● |

3.10.42.1.2 (L1) Ensure 'Enable Windows NTP Server' is set to 'Disabled' (Automated)

Profile Applicability:

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

Description:

This policy setting specifies whether the Windows NTP Server is enabled. Disabling this setting prevents the system from acting as a NTP Server (time source) to service NTP requests from other systems (NTP Clients).

The recommended state for this setting is: Disabled.

Rationale:

The configuration of proper time synchronization is critically important in an enterprise managed environment both due to the sensitivity of Kerberos authentication timestamps and also to ensure accurate security logging. This should be done through a known NTP server. Member servers and workstations should not typically be time sources for other clients.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a REG_DWORD value of 0.

HKLM\SOFTWARE\Policies\Microsoft\W32Time\TimeProviders\NtpServer:Enabled

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`.

Administrative Templates\System\Windows Time Service\Time Providers\Enable Windows NTP Server

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. | | ● | ● |

3.11 Windows Components

This section contains recommendations for Windows Components.

3.11.1 ActiveX Installer Service

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

3.11.2 App Package Deployment

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

3.11.3 App runtime

This section contains recommendations for App runtime.

3.11.3.1 (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 with a REG_DWORD value of 1.

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:MSAOptional

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

Administrative Templates\Windows Components\App runtime\Allow Microsoft accounts to be optional

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. | | ● | ● |

3.11.3.2 (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 with a REG_DWORD value of 1.

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:BlockHostedAppAccessWinRT

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

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.

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. | ● | ● | |

3.11.4 Application Compatibility

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

3.11.5 Attachment Manager

This section contains recommendations for Attachment Manager.

3.11.5.1 (L1) Ensure 'Do not preserve zone information in file attachments (User)' 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 with a REG_DWORD value of 2.

```
HKU\ [USER  
SID]\Software\Microsoft\Windows\CurrentVersion\Policies\Attachments:SaveZoneInformation
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`.

Administrative Templates\Windows Components\Attachment Manager\Do not preserve zone information in file attachments (User)

Default Value:

`Disabled`. (Windows marks file attachments with their zone information.)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| v7 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |

3.11.5.2 (L1) Ensure 'Notify antivirus programs when opening attachments (User)' 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 with a REG_DWORD value of 3.

```
HKU\ [USER  
SID]\Software\Microsoft\Windows\CurrentVersion\Policies\Attachments:ScanWithAntivirus
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

```
Administrative Templates\Windows Components\Attachment Manager\Notify antivirus programs when opening attachments (User)
```

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. | | ● | ● |

3.11.6 AutoPlay Policies

This section contains recommendations for AutoPlay Policies.

3.11.6.1 (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 with a REG_DWORD value of 1.

HKLM\SOFTWARE\Policies\Microsoft\Windows\Explorer>NoAutoplayfornonVolume

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

Administrative Templates\Windows Components\AutoPlay Policies\Disallow Autoplay for non-volume devices

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. | ● | ● | ● |

3.11.6.2 (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 with a `REG_DWORD` value of 1.

`HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer>NoAutorun`

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled: Do not execute any autorun commands.

`Administrative Templates\Windows Components\AutoPlay Policies\Set the default behavior for AutoRun`

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 | 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. | ● | ● | ● |

3.11.6.3 (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 with a REG_DWORD value of 255.

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer>NoDriveTypeA
utoRun

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled: All drives.

Administrative Templates\Windows Components\AutoPlay Policies\Turn off
Autoplay

Default Value:

Disabled. (Autoplay is enabled.)

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. | ● | ● | ● |

3.11.7 BitLocker Drive Encryption

This section contains recommendations for BitLocker Drive Encryption.

3.11.7.1 Fixed Data Drives

This section contains recommendations for Fixed Data Drives.

3.11.7.1.1 (BL) Ensure 'Choose how BitLocker-protected fixed drives can be recovered' is set to 'Enabled' (Automated)

Profile Applicability:

- BitLocker (BL)

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 with a REG_DWORD value of 1.

HKLM\SOFTWARE\Policies\Microsoft\FVE:FDVRecovery

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

Administrative Templates\Windows Components\BitLocker Drive Encryption\Fixed Data Drives\Choose how BitLocker-protected fixed drives can be recovered

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. | ● | ● | ● |

3.11.7.1.2 (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:

- BitLocker (BL)

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 with a REG_DWORD value of 2.

HKLM\SOFTWARE\Policies\Microsoft\FVE:FDVRecoveryKey

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled: Allow 256-bit recovery key.

Administrative Templates\Windows Components\BitLocker Drive Encryption\Fixed Data Drives\Choose how BitLocker-protected fixed drives can be recovered: Recovery Key

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. | ● | ● | ● |

3.11.7.1.3 (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:

- BitLocker (BL)

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 with a REG_DWORD value of 2.

| |
|--|
| HKLM\SOFTWARE\Policies\Microsoft\FVE:FDVRecoveryPassword |
|--|

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled: Allow 48-digit recovery password.

Administrative Templates\Windows Components\BitLocker Drive Encryption\Fixed Data Drives\Choose how BitLocker-protected fixed drives can be recovered:
Recovery Password

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. | ● | ● | ● |

3.11.7.1.4 (BL) Ensure 'Choose how BitLocker-protected fixed drives can be recovered: Allow data recovery agent' is set to 'Enabled: True' (Automated)

Profile Applicability:

- BitLocker (BL)

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.

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 with a REG_DWORD value of 1.

HKLM\SOFTWARE\Policies\Microsoft\FVE:FDVManageDRA

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled: True.

Administrative Templates\Windows Components\BitLocker Drive Encryption\Fixed Data Drives\Choose how BitLocker-protected fixed drives can be recovered:
Allow data recovery agent

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. | ● | ● | ● |

3.11.7.1.5 (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:

- BitLocker (BL)

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). 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 with a REG_DWORD value of 1.

HKLM\SOFTWARE\Policies\Microsoft\FVE:FDVActiveDirectoryInfoToStore

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled: Backup recovery passwords and key packages.

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:

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. | ● | ● | ● |

3.11.7.1.6 (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:

- BitLocker (BL)

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.

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 with a REG_DWORD value of 0.

HKLM\SOFTWARE\Policies\Microsoft\FVE:FDVRequireActiveDirectoryBackup

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled: False.

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

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. | ● | ● | ● |

3.11.7.1.7 (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:

- BitLocker (BL)

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.

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 with a REG_DWORD value of 1.

HKLM\SOFTWARE\Policies\Microsoft\FVE:FDVHideRecoveryPage

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled: True.

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

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. | ● | ● | ● |

3.11.7.1.8 (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:

- BitLocker (BL)

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.

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 with a REG_DWORD value of 0.

HKLM\SOFTWARE\Policies\Microsoft\FVE:FDVActiveDirectoryBackup

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled: False.

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

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. | ● | ● | ● |

3.11.7.2 Operating System Drives

This section contains recommendations for Operating System Drives.

3.11.7.2.1 (BL) Ensure 'Allow enhanced PINs for startup' is set to 'Enabled' (Automated)

Profile Applicability:

- BitLocker (BL)

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 with a REG_DWORD value of 1.

HKLM\SOFTWARE\Policies\Microsoft\FVE:UseEnhancedPin

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives\Allow enhanced PINs for startup

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. | | ● | ● |

3.11.7.2.2 (BL) Ensure 'Choose how BitLocker-protected operating system drives can be recovered' is set to 'Enabled' (Automated)

Profile Applicability:

- BitLocker (BL)

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 with a REG_DWORD value of 1.

```
HKLM\SOFTWARE\Policies\Microsoft\FVE:OSRecovery
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

```
Administrative Templates\Windows Components\BitLocker Drive  
Encryption\Operating System Drives\Choose how BitLocker-protected operating  
system drives can be recovered
```

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. | ● | ● | ● |

3.11.7.2.3 (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:

- BitLocker (BL)

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 compliant.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a REG_DWORD value of 0.

HKLM\SOFTWARE\Policies\Microsoft\FVE:OSRecoveryKey

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled: Do not allow 256-bit recovery key.

Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives\Choose how BitLocker-protected operating system drives can be recovered: Recovery Key

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. | ● | ● | ● |

3.11.7.2.4 (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:

- BitLocker (BL)

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 compliant.

Audit:

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

HKLM\SOFTWARE\Policies\Microsoft\FVE:OSRecoveryPassword

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled: Require 48-digit recovery password.

Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives\Choose how BitLocker-protected operating system drives can be recovered: Recovery Password

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. | ● | ● | ● |

3.11.7.2.5 (BL) Ensure 'Choose how BitLocker-protected operating system drives can be recovered: Allow data recovery agent' is set to 'Enabled: False' (Automated)

Profile Applicability:

- BitLocker (BL)

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.

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 with a REG_DWORD value of 0.

HKLM\SOFTWARE\Policies\Microsoft\FVE:OSManageDRA

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled: False.

Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives\Choose how BitLocker-protected operating system drives can be recovered: Allow data recovery agent

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. | ● | ● | ● |

3.11.7.2.6 (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:

- BitLocker (BL)

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 with a REG_DWORD value of 1.

HKLM\SOFTWARE\Policies\Microsoft\FVE:OSActiveDirectoryInfoToStore

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled: Store recovery passwords and key packages.

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:

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. | ● | ● | ● |

3.11.7.2.7 (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:

- BitLocker (BL)

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.

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 with a REG_DWORD value of 1.

HKLM\SOFTWARE\Policies\Microsoft\FVE:OSRequireActiveDirectoryBackup

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled: True.

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

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. | ● | ● | ● |

3.11.7.2.8 (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:

- BitLocker (BL)

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.

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 with a REG_DWORD value of 1.

HKLM\SOFTWARE\Policies\Microsoft\FVE:OSHideRecoveryPage

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled: True.

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

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. | ● | ● | ● |

3.11.7.2.9 (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:

- BitLocker (BL)

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.

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 with a REG_DWORD value of 1.

HKLM\SOFTWARE\Policies\Microsoft\FVE:OSActiveDirectoryBackup

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled: True.

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

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. | ● | ● | ● |

3.11.7.2.10 (BL) Ensure 'Require additional authentication at startup' is set to 'Enabled' (Automated)

Profile Applicability:

- BitLocker (BL)

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 with a REG_DWORD value of 1.

HKLM\SOFTWARE\Policies\Microsoft\FVE:UseAdvancedStartup

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives\Require additional authentication at startup

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 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| 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. | ● | ● | ● |

3.11.7.2.11 (BL) Ensure 'Require additional authentication at startup: Allow BitLocker without a compatible TPM' is set to 'Enabled: False' (Automated)

Profile Applicability:

- BitLocker (BL)

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.

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 with a REG_DWORD value of 0.

HKLM\SOFTWARE\Policies\Microsoft\FVE:EnableBDEWithNoTPM

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled: False.

Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives\Require additional authentication at startup: Allow BitLocker without a compatible TPM

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 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| 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. | ● | ● | ● |

3.11.7.2.12 (BL) Ensure 'Require additional authentication at startup: Configure TPM startup key and PIN:' is set to 'Enabled: Do not allow startup key and PIN with TPM' (Automated)

Profile Applicability:

- BitLocker (BL)

Description:

This policy setting allows you to configure whether BitLocker requires additional authentication each time the computer starts. 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.

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.

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: Do not allow startup key and PIN with TPM.

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 TPM, PIN *and* startup key will not be a permitted combination for BitLocker authentication. 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 with a REG_DWORD value of 0.

HKLM\SOFTWARE\Policies\Microsoft\FVE:UseTPMKeyPIN

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled: Do not allow startup key and PIN with TPM.

Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives\Require additional authentication at startup: Configure TPM startup key and PIN:

Default Value:

Allow startup key and PIN with TPM. (A TPM can be used in conjunction with both a PIN *and* startup key.)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| 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. | ● | ● | ● |

3.11.7.2.13 (BL) Ensure 'Require additional authentication at startup: Configure TPM startup key:' is set to 'Enabled: Do not allow startup key with TPM' (Automated)

Profile Applicability:

- BitLocker (BL)

Description:

This policy setting allows you to configure whether BitLocker requires additional authentication each time the computer starts. 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.

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.

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: Do not allow startup key with TPM.

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 TPM and a startup key will not be a permitted combination for BitLocker authentication.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a REG_DWORD value of 0.

HKLM\SOFTWARE\Policies\Microsoft\FVE:UseTPMKey

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled: Do not allow startup key with TPM.

Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives\Require additional authentication at startup: Configure TPM startup key:

Default Value:

Allow startup key with TPM. (A TPM can be used in conjunction with a startup key.)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| 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. | ● | ● | ● |

3.11.7.2.14 (BL) Ensure 'Require additional authentication at startup: Configure TPM startup PIN:' is set to 'Enabled: Require startup PIN with TPM' (Automated)

Profile Applicability:

- BitLocker (BL)

Description:

This policy setting allows you to configure whether BitLocker requires additional authentication each time the computer starts. 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.

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.

The recommended state for this setting is: Enabled: Require startup PIN with TPM.

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 startup PIN will be required in addition to a TPM for BitLocker authentication. 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 with a REG_DWORD value of 1.

HKLM\SOFTWARE\Policies\Microsoft\FVE:UseTPMPIN

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled: Require startup PIN with TPM.

Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives\Require additional authentication at startup: Configure TPM startup PIN:

Default Value:

Allow (but not require) a startup PIN with TPM.

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. | ● | ● | ● |

3.11.7.2.15 (BL) Ensure 'Require additional authentication at startup: Configure TPM startup:' is set to 'Enabled: Do not allow TPM' (Automated)

Profile Applicability:

- BitLocker (BL)

Description:

This policy setting allows you to configure whether BitLocker requires additional authentication each time the computer starts. 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.

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.

The recommended state for this setting is: Enabled: Do not allow TPM.

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 TPM alone will be insufficient authentication for use with 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 with a REG_DWORD value of 0.

| |
|---|
| HKLM\Software\Policies\Microsoft\FVE:UseTPM |
|---|

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled: Do not allow TPM.

Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives\Require additional authentication at startup: Configure TPM startup:

Default Value:

Allow TPM. (A TPM can be used without also requiring a startup PIN or key.)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| 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. | ● | ● | ● |

3.11.7.3 Removable Data Drives

This section contains recommendations for Removable Data Drives.

3.11.7.3.1 (BL) Ensure 'Deny write access to removable drives not protected by BitLocker' is set to 'Enabled' (Automated)

Profile Applicability:

- BitLocker (BL)

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 with a REG_DWORD value of 1.

HKLM\SYSTEM\CurrentControlSet\Policies\Microsoft\FVE:RDVDenyWriteAccess

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

Administrative Templates\Windows Components\BitLocker Drive Encryption\Removable Data Drives\Deny write access to removable drives not protected by BitLocker

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 | <p>3.9 Encrypt Data on Removable Media Encrypt data on removable media.</p> | | ● | ● |
| v7 | <p>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.</p> | ● | ● | ● |
| v7 | <p>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.</p> | | | ● |

3.11.7.3.2 (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:

- BitLocker (BL)

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.

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 with a REG_DWORD value of 0.

HKLM\SOFTWARE\Policies\Microsoft\FVE:RDVDenyCrossOrg

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled: False.

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

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 | <p>3.9 Encrypt Data on Removable Media Encrypt data on removable media.</p> | | ● | ● |
| v7 | <p>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.</p> | ● | ● | ● |
| v7 | <p>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.</p> | | | ● |

3.11.8 Credential User Interface

This section contains recommendations for Credential User Interface.

3.11.8.1 (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 with a REG_DWORD value of 1.

HKLM\SOFTWARE\Policies\Microsoft\Windows\CredUI:DisablePasswordReveal

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

Administrative Templates\Windows Components\Credential User Interface\Do not display the password reveal button

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.)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| v7 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |

3.11.8.2 (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 with a REG_DWORD value of 0.

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\CredUI:EnumerateAdministrators

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to **Disabled**.

Administrative Templates\Windows Components\Credential User Interface\Enumerate administrator accounts on elevation

Default Value:

Disabled. (Users will be required to always type in a username and password to elevate.)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| v7 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |

3.11.8.3 (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 with a REG_DWORD value of 1.

HKLM\SOFTWARE\Policies\Microsoft\Windows\System>NoLocalPasswordResetQuestions

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

Administrative Templates\Windows Components\Credential User Interface\Prevent the use of security questions for local accounts

Default Value:

Not Configured. (Local user accounts are able to set up and use security questions to reset their passwords.)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| v7 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |

3.11.9 Data Collection and Preview Builds

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

3.11.10 Delivery Optimization

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

3.11.11 Desktop Window Manager

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

3.11.12 Device and Driver Compatibility

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

3.11.13 Digital Locker

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

3.11.14 Event Forwarding

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

3.11.15 Event Log Service

This section contains recommendations for Event Log Service.

3.11.15.1 Application

This section contains recommendations for Application.

3.11.15.1.1 (L1) Ensure '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 with a REG_SZ value of 0.

HKLM\SOFTWARE\Policies\Microsoft\Windows\EventLog\Application:Retention

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to **Disabled**.

Administrative Templates\Windows Components\Event Log Service\Application\Control Event Log behavior when the log file reaches its maximum size

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. | | ● | ● |

3.11.15.1.2 (L1) Ensure '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 with a REG_DWORD value of 32768 or greater.

HKLM\SOFTWARE\Policies\Microsoft\Windows\EventLog\Application:MaxSize

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled: 32,768 or greater.

Administrative Templates\Windows Components\Event Log Service\Application\Specify the maximum log file size (KB)

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. | | ● | ● |

3.11.15.2 Security

This section contains recommendations for Security.

3.11.15.2.1 (L1) Ensure '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 with a REG_SZ value of 0.

HKLM\SOFTWARE\Policies\Microsoft\Windows\EventLog\Security:Retention

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to **Disabled**.

Administrative Templates\Windows Components\Event Log Service\Security\Control Event Log behavior when the log file reaches its maximum size

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. | | ● | ● |

3.11.15.2.2 (L1) Ensure '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 with a REG_DWORD value of 196608 or greater.

HKLM\SOFTWARE\Policies\Microsoft\Windows\EventLog\Security:MaxSize

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled: 196,608 or greater.

Administrative Templates\Windows Components\Event Log Service\Specify the maximum log file size (KB)

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. | | ● | ● |

3.11.15.3 Setup

This section contains recommendations for Setup.

3.11.15.3.1 (L1) Ensure '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 with a REG_SZ value of 0.

HKLM\SOFTWARE\Policies\Microsoft\Windows\EventLog\Setup:Retention

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to **Disabled**.

Administrative Templates\Windows Components\Event Log Service\Setup\Control Event Log behavior when the log file reaches its maximum size

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. | | ● | ● |

3.11.15.3.2 (L1) Ensure '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 with a REG_DWORD value of 32768 or greater.

HKLM\SOFTWARE\Policies\Microsoft\Windows\EventLog\Setup:MaxSize

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled: 32,768 or greater.

Administrative Templates\Windows Components\Event Log Service\Setup\Specify the maximum log file size (KB)

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. | | ● | ● |

3.11.15.4 System

This section contains recommendations for System.

3.11.15.4.1 (L1) Ensure '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 with a REG_SZ value of 0.

HKLM\SOFTWARE\Policies\Microsoft\Windows\EventLog\System:Retention

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to **Disabled**.

Administrative Templates\Windows Components\Event Log Service\System\Control Event Log behavior when the log file reaches its maximum size

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. | | ● | ● |

3.11.15.4.2 (L1) Ensure '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 with a REG_DWORD value of 32768 or greater.

HKLM\SOFTWARE\Policies\Microsoft\Windows\EventLog\System:MaxSize

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled: 32,768 or greater.

Administrative Templates\Windows Components\Event Log Service\System\Specify the maximum log file size (KB)

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. | | ● | ● |

3.11.16 Event Logging

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

3.11.17 Event Viewer

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

3.11.18 File Explorer

This section contains recommendations for File Explorer.

3.11.18.1 (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 and prevented from running unrecognized programs downloaded from the Internet.

Audit:

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

HKLM\SOFTWARE\Policies\Microsoft\Windows\System:EnableSmartScreen

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled: Warn and prevent bypass.

Administrative Templates\Windows Components\File Explorer\Configure Windows Defender SmartScreen

Default Value:

Disabled. (Windows Defender SmartScreen behavior is managed by administrators on the PC by using Windows Defender SmartScreen Settings in Action Center.)

References:

1. <https://learn.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-smartscreen/microsoft-defender-smartscreen-overview>

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. | | ● | ● |

3.11.18.2 (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 with a REG_DWORD value of 0.

HKLM\SOFTWARE\Policies\Microsoft\Windows\Explorer:NoDataExecutionPrevention

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`.

Administrative Templates\Windows Components\File Explorer\Turn off Data Execution Prevention for Explorer

Default Value:

Disabled. (Data Execution Prevention will block certain types of malware from exploiting Explorer.)

References:

1. <https://learn.microsoft.com/en-us/windows/win32/memory/data-execution-prevention>

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. | ● | ● | ● |

3.11.18.3 (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 with a REG_DWORD value of 0.

HKLM\SOFTWARE\Policies\Microsoft\Windows\Explorer:NoHeapTerminationOnCorruption

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to **Disabled**.

Administrative Templates\Windows Components\File Explorer\Turn off heap termination on corruption

Default Value:

Disabled. (Heap termination on corruption is enabled.)

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> | | ● | ● |

3.11.18.4 (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 with a REG_DWORD value of 0.

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer:PreXPSP2ShellProtocolBehavior

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to **Disabled**.

Administrative Templates\Windows Components\File Explorer\Turn off shell protocol protected mode

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 |
|------------------|--|------|------|------|
| v8 | <p>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.</p> | | ● | ● |
| v7 | <p>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.</p> | | ● | ● |

3.11.19 File Revocation

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

3.11.20 Home Group

This section contains recommendations for Home Group.

3.11.20.1 (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 with a REG_DWORD value of 1.

| |
|---|
| HKLM\SOFTWARE\Policies\Microsoft\Windows\HomeGroup:DisableHomeGroup |
|---|

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

Administrative Templates\Windows Components\HomeGroup\Prevent the computer from joining a homegroup

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.)

References:

1. <https://support.microsoft.com/en-us/topic/9f802c8c-900f-60fb-826f-6fe06add8fe9#homegroup-start-to-finish=windows-81&v1h=win81tab6&v2h=win7tab1>

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. | | ● | ● |

3.11.21 IME

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

3.11.22 Instant Search

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

3.11.23 Internet Explorer

This section contains recommendations for Internet Explorer.

3.11.23.1 (L1) Ensure 'Disable Internet Explorer 11 as a standalone browser' is set to 'Enabled: Always' (Automated)

Profile Applicability:

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

Description:

This policy setting restricts the launching of Internet Explorer as a standalone browser.

This setting performs the following actions when enabled:

- Prevents Internet Explorer 11 from launching as a standalone browser.
- Restricts Internet Explorer's usage to Microsoft Edge's native *Internet Explorer mode*.
- Redirects all attempts at launching Internet Explorer 11 to Microsoft Edge Stable Channel browser.
- Overrides any other policies that redirect to Internet Explorer 11.

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

Rationale:

Official support for Internet Explorer (IE) 11 desktop applications (workstation) ended on June 22, 2022. Unsupported software could contain vulnerabilities that are left unpatched. Unpatched vulnerabilities can lead to application weaknesses that could allow attackers to leverage the security vulnerability by running malicious code.

Impact:

Users will no longer be able to launch IE 11 and will be redirected to Microsoft Edge.

Note: IE 11 is still supported on Windows 10 LTSC and Windows Server versions.

Note #2: On February 14, 2023, a [Microsoft Edge update](#) disabled IE 11 on Windows 10 (except those mentioned above).

Audit:

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

HKLM\SOFTWARE\Policies\Microsoft\Internet Explorer>Main:NotifyDisableIEOptions

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled: Always.

Administrative Templates\Windows Components\Internet Explorer\Disable Internet Explorer 11 as a standalone browser

Default Value:

Disabled. (All sites are opened using the current active browser settings.)

References:

1. <https://learn.microsoft.com/en-us/deployedge/edge-ie-disable-ie11>
2. <https://techcommunity.microsoft.com/t5/windows-it-pro-blog/internet-explorer-11-desktop-app-retirement-faq/ba-p/2366549>

Additional Information:

Applies to Windows 10 **only**.

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | <u>9.1 Ensure Use of Only Fully Supported Browsers and Email Clients</u> Ensure only fully supported browsers and email clients are allowed to execute in the enterprise, only using the latest version of browsers and email clients provided through the vendor. | ● | ● | ● |
| v7 | <u>7.1 Ensure Use of Only Fully Supported Browsers and Email Clients</u> Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers and email clients provided by the vendor. | ● | ● | ● |

3.11.24 Internet Information Services

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

3.11.25 Location and Sensors

This section contains recommendations for Location and Sensors.

3.11.25.1 Windows Location Provider

This section contains recommendations for Windows Location Provider.

3.11.26 Maintenance Scheduler

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

3.11.27 Microsoft Account

This section contains recommendations for Microsoft Account.

3.11.27.1 (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 with a REG_DWORD value of 1.

| |
|---|
| HKLM\SOFTWARE\Policies\Microsoft\MicrosoftAccount:DisableUserAuth |
|---|

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

Administrative Templates\Windows Components\Microsoft accounts\Block all consumer Microsoft account user authentication

Default Value:

Disabled. (Applications and services on the device will be permitted to authenticate using consumer Microsoft accounts via the Windows OnlineID and WebAccountManager APIs.)

References:

1. <https://learn.microsoft.com/en-us/windows/security/identity-protection/access-control/microsoft-accounts#bkmk-restrictuse>

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 5.6 Centralize Account Management Centralize account management through a directory or identity service. | | ● | ● |
| v7 | 16.8 Disable Any Unassociated Accounts Disable any account that cannot be associated with a business process or business owner. | ● | ● | ● |

3.11.28 Microsoft Defender Antivirus

This section contains recommendations for Microsoft Defender Antivirus.

3.11.28.1 Client Interface

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

3.11.28.2 Exclusions

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

3.11.28.3 MAPS

This section contains recommendations for MAPS.

3.11.28.3.1 (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 with a REG_DWORD value of 0.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows  
Defender\Spynet:LocalSettingOverrideSpynetReporting
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to **Disabled**.

```
Administrative Templates\Windows Components\Microsoft Defender  
Antivirus\MAPS\Configure local setting override for reporting to Microsoft  
MAPS
```

Default Value:

Disabled. (Group Policy will take priority over the local preference setting.)

References:

1. <https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-cloud-protection-microsoft-defender-antivirus?view=o365-worldwide>

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. | | ● | ● |

3.11.28.3.2 (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:

HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet:SpynetReporting

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Disabled.

Administrative Templates\Windows Components\Microsoft Defender Antivirus\MAPS\Join Microsoft MAPS

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 |
|------------------|---|------|------|------|
| 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. | | ● | ● |

3.11.28.4 Microsoft Defender Exploit Guard

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

3.11.28.5 MpEngine

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

3.11.28.6 Network Inspection System

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

3.11.28.7 Quarantine

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

3.11.28.8 Real-time Protection

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

3.11.28.9 Remediation

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

3.11.28.10 Reporting

This section contains recommendations for Reporting.

3.11.28.10.1 (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 with a REG_DWORD value of 1.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows  
Defender\Reporting:DisableGenericRePorts
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to **Disabled**.

```
Administrative Templates\Windows Components\Microsoft Defender  
Antivirus\Reporting\Configure Watson events
```

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 |
|------------------|--|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| v7 | 13.3 <u>Monitor and Block Unauthorized Network Traffic</u> Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals. | | | ● |

3.11.28.11 (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 third-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 with a REG_DWORD value of 0.

HKLM\SOFTWARE\Policies\Microsoft\Windows Defender:DisableAntiSpyware

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to **Disabled**.

Administrative Templates\Windows Components\Microsoft Defender Antivirus\Turn off Microsoft Defender Antivirus

Default Value:

Disabled. (Microsoft Defender Antivirus runs and computers are scanned for malware and other potentially unwanted software.)

References:

1. <https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-antivirus-windows?view=o365-worldwide>

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. | | ● | ● |

3.11.29 Microsoft Management Console

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

3.11.30 Microsoft User Experience Virtualization

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

3.11.31 Network Sharing

This section contains recommendations for Network Sharing.

3.11.31.1 (L1) Ensure 'Prevent users from sharing files within their profile. (User)' 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 with a REG_DWORD value of 1.

```
HKU\ [USER  
SID]\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer>NoInplaceSharing
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

```
Administrative Templates\Windows Components\Network Sharing\Prevent users from sharing files within their profile. (User)
```

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 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| v7 | 14.6 <u>Protect Information through Access Control Lists</u> 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. | ● | ● | ● |

3.11.32 Online Assistance

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

3.11.33 Portable Operating System

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

3.11.34 Presentation Settings

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

3.11.35 Push To Install

This section contains recommendations for Push To Install.

3.11.35.1 (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 with a REG_DWORD value of 1.

HKLM\SOFTWARE\Policies\Microsoft\PushToInstall:DisablePushToInstall

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

Administrative Templates\Windows Components\Push to Install\Turn off Push To Install service

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 |
|------------------|---|------|------|------|
| 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. | ● | ● | |

3.11.36 Remote Desktop Services

This section contains recommendations for Remote Desktop Services.

3.11.36.1 RD Gateway

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

3.11.36.2 RD Licensing

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

3.11.36.3 Remote Desktop Connection Client

This section contains recommendations for Remote Desktop Connection Client.

3.11.36.3.1 RemoteFX USB Device Redirection

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

3.11.36.3.2 (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 with a REG_DWORD value of 1.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal  
Services:DisablePasswordSaving
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

```
Administrative Templates\Windows Components\Remote Desktop Services\Remote  
Desktop Connection Client\Do not allow passwords to be saved
```

Default Value:

Disabled. (Users will be able to save passwords using Remote Desktop Connection.)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| v7 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |

3.11.36.4 Remote Desktop Session Host

This section contains recommendations for Remote Desktop Session Host.

3.11.36.4.1 Azure Virtual Desktop

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

3.11.36.4.2 Connections

This section contains recommendations for Connections.

3.11.36.4.2.1 (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 with a REG_DWORD value of 1.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services:fDenyTSConnections
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to **Disabled**.

```
Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Connections\Allow users to connect remotely by using Remote Desktop Services
```

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 |
|------------------|---|------|------|------|
| 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> | ● | ● | ● |

3.11.36.4.3 Device and Resource Redirection

This section contains recommendations for Device and Resource Redirection.

3.11.36.4.3.1 (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 with a REG_DWORD value of 1.

HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services:fDisableCcm

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Device and Resource Redirection\Do not allow COM port redirection

Default Value:

Disabled. (Remote Desktop Services allows COM port redirection.)

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> | ● | ● | ● |

3.11.36.4.3.2 (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 with a REG_DWORD value of 1.

HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services:fDisableCdm

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Device and Resource Redirection\Do not allow drive redirection

Default Value:

Disabled. (An RD Session Host maps client drives automatically upon connection.)

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. | | ● | ● |

3.11.36.4.3.3 (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 with a REG_DWORD value of 1.

HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services:fDisableLPT

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Device and Resource Redirection\Do not allow LPT port redirection

Default Value:

Disabled. (Remote Desktop Services allows LPT port redirection.)

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> | ● | ● | ● |

3.11.36.4.3.4 (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 with a REG_DWORD value of 1.

HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services:fDisablePNPRedir

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Device and Resource Redirection\Do not allow supported Plug and Play device redirection

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 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| v7 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |

3.11.36.4.4 Licensing

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

3.11.36.4.5 Printer Redirection

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

3.11.36.4.6 Profiles

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

3.11.36.4.7 RD Connection Broker

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

3.11.36.4.8 Remote Session Environment

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

3.11.36.4.9 Security

This section contains recommendations for Security.

3.11.36.4.9.1 (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 with a REG_DWORD value of 1.

| |
|--|
| HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services:fPromptForPassword |
|--|

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security\Always prompt for password upon connection

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 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| 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. | | ● | ● |

3.11.36.4.9.2 (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 with a REG_DWORD value of 1.

HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services:fEncryptRPCTraffic

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security\Require secure RPC communication

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 |
|------------------|---|------|------|------|
| 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. | | ● | ● |

3.11.36.4.9.3 (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 with a REG_DWORD value of 2.

HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services\SecurityLayer

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled: SSL.

Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security\Require use of specific security layer for remote (RDP) connections

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. | | ● | ● |

3.11.36.4.9.4 (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 with a REG_DWORD value of 1.

| |
|--|
| HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services\UserAuthentication |
|--|

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security\Require user authentication for remote connections by using Network Level Authentication

Default Value:

Windows 7 or older: Disabled.

Windows 8.0 or newer: Enabled.

References:

1. <https://social.technet.microsoft.com/wiki/contents/articles/5490.configure-network-level-authentication-for-remote-desktop-services-connections.aspx>

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. | | ● | ● |

3.11.36.4.9.5 (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 with a REG_DWORD value of 3.

HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services:MinEncryptionLevel

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled: High Level.

Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security\Set client connection encryption level

Default Value:

Enabled: High Level. (All communications between clients and RD Session Host servers during remote connections using native RDP encryption must be 128-bit strength. Clients that do not support 128-bit encryption will be unable to establish Remote Desktop Server sessions.)

References:

1. https://learn.microsoft.com/en-usopenspecs/windows_protocols/ms-rdpbcgr/f1c7c93b-94cc-4551-bb90-532a0185246a

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. | | ● | ● |

3.11.36.4.10 Session Time Limits

This section contains recommendations for Session Time Limits.

3.11.36.4.10.1 (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.

In addition, session timeouts that are misconfigured or set for a long period of time can leave the system open to an attacker hijacking the session.

Impact:

Remote Desktop Services will automatically disconnect active but idle sessions after 15 minutes (or the specified amount of time). The user receives a warning two minutes before the session disconnects, which allows the user to press a key or move the mouse to keep the session active. Note that idle session time limits do not apply to console sessions.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a REG_DWORD value of 900000 or less but not 0.

HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services:MaxIdleTime

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled: 15 minutes or less, but not Never (0).

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

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 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| v7 | 16.11 <u>Lock Workstation Sessions After Inactivity</u> Automatically lock workstation sessions after a standard period of inactivity. | ● | ● | ● |

3.11.36.4.10.2 (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.

In addition, session timeouts that are misconfigured or set for a long period of time can leave the system open to an attacker hijacking the session.

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 with a REG_DWORD value of 60000.

| |
|--|
| HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services:MaxDisconnectionTime |
|--|

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled: 1 minute.

Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Session Time Limits\Set time limit for disconnected sessions

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 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| v7 | 16.11 <u>Lock Workstation Sessions After Inactivity</u> Automatically lock workstation sessions after a standard period of inactivity. | ● | ● | ● |

3.11.36.4.11 Temporary folders

This section contains recommendations for Temporary folders.

3.11.36.4.11.1 (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 with a REG_DWORD value of 1.

HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services:DeleteTempDirsOnExit

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to **Disabled**.

Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Temporary Folders\Do not delete temp folders upon exit

Default Value:

Disabled. (Temporary folders are deleted when a user logs off.)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 3.4 Enforce Data Retention Retain data according to the enterprise's data management process. Data retention must include both minimum and maximum timelines. | ● | ● | ● |
| 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. | | ● | ● |

3.11.37 RSS Feeds

This section contains recommendations for RSS Feeds.

3.11.37.1 (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 with a REG_DWORD value of 1.

HKLM\SOFTWARE\Policies\Microsoft\Internet Explorer\Feeds:DisableEnclosureDownload

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

Administrative Templates\Windows Components\RSS Feeds\Prevent downloading of enclosures

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 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 Uninstall or disable any unauthorized browser or email client plugins or add-on applications.</p> | ● | ● | ● |

3.11.38 Security Center

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

3.11.39 Shutdown Options

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

3.11.40 Smart Card

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

3.11.41 Sound Recorder

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

3.11.42 Store

This section contains recommendations for Store.

3.11.42.1 (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 with a REG_DWORD value of 1.

HKLM\SOFTWARE\Policies\Microsoft\WindowsStore:DisableOSUpgrade

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

Administrative Templates\Windows Components\Store\Turn off the offer to update to the latest version of Windows

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 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| 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. | | ● | ● |

3.11.42.2 (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 third-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 with a REG_DWORD value of 1.

HKLM\SOFTWARE\Policies\Microsoft\WindowsStore:RemoveWindowsStore

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

Administrative Templates\Windows Components\Store\Turn off the Store application

Default Value:

Disabled. (Access to the Microsoft Store application is allowed.)

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> | ● | ● | ● |
| v7 | <p>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.</p> | ● | ● | ● |

3.11.43 Sync your settings

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

3.11.44 Tablet PC

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

3.11.45 Tenant Restrictions

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

3.11.46 Windows Calendar

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

3.11.47 Windows Color System

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

3.11.48 Windows Error Reporting

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

3.11.49 Windows Installer

This section contains recommendations for Windows Installer.

3.11.49.1 (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 with a REG_DWORD value of 0.

HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer:SafeForScripting

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to **Disabled**.

Administrative Templates\Windows Components\Windows Installer\Prevent Internet Explorer security prompt for Windows Installer scripts

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. | | ● | ● |

3.11.50 Windows Logon Options

This section contains recommendations for Windows Logon Options.

3.11.50.1 (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 with a REG_DWORD value of 1.

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:DisableAutomaticRestartSignOn

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to **Disabled**.

Administrative Templates\Windows Components\Windows Logon Options\Sign-in and lock last interactive user automatically after a restart

Default Value:

Enabled. (The device securely saves the user's credentials (including the user name, domain and encrypted password) to configure automatic sign-in after a Windows Update restart. After the Windows Update restart, the user is automatically signed-in and the session is automatically locked with all the lock screen apps configured for that user.)

References:

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

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| v7 | 16.11 <u>Lock Workstation Sessions After Inactivity</u> Automatically lock workstation sessions after a standard period of inactivity. | ● | ● | ● |

3.11.51 Windows Media Digital Rights Management

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

3.11.52 Windows Media Player

This section contains recommendations for Windows Media Player.

3.11.52.1 Playback

This section contains recommendations related to Windows Media Player playback.

3.11.52.1.1 (L2) Ensure 'Prevent Codec Download (User)' 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 with a REG_DWORD value of 1.

HKU\ [USER
SID]\Software\Policies\Microsoft\WindowsMediaPlayer:PreventCodecDownload

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

Administrative Templates\Windows Components\Windows Media Player\Playback\Prevent Codec Download (User)

Default Value:

Users can change the setting for the *Download codecs automatically* check box.

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| v7 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |

3.11.53 Windows Mobility Center

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

3.11.54 Windows PowerShell

This section contains recommendations for Windows PowerShell.

3.11.54.1 (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 with a REG_DWORD value of 1.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging:Enable  
ScriptBlockLogging
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

```
Administrative Templates\Windows Components\Windows PowerShell\Turn on  
PowerShell Script Block Logging
```

Default Value:

Enabled. (PowerShell will log script blocks the first time they are used.)

References:

1. https://learn.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. | | ● | ● |

3.11.54.2 (L1) Ensure 'Turn on PowerShell Transcription' is set to 'Enabled' (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: Enabled.

Rationale:

PowerShell transcript input can be very valuable when performing forensic investigations of PowerShell attack incidents to determine what occurred.

Impact:

PowerShell transcript input will be logged to the `PowerShell_transcript` output file, which is saved to the My Documents folder of each users' profile by default.

Warning: There are potential risks of capturing credentials and sensitive information in the `PowerShell_transcript` output file, which could be exposed to users who have read-access to the file.

Warning #2: PowerShell Transcription is not compatible with the natively installed PowerShell v4 on Microsoft Windows 10 Release 1511 and Server 2012 R2 and below. If this recommendation is set as prescribed, PowerShell will need to be updated to at least v5.1 or newer. For more information on updating PowerShell, please see [Windows PowerShell System Requirements - PowerShell | Microsoft Learn](#).

Audit:

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

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\PowerShell\Transcription:EnableTrans  
cripting
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

Administrative Templates\Windows Components\Windows PowerShell\Turn on PowerShell Transcription

Default Value:

Disabled. (Transcription of PowerShell-based applications is disabled by default, although transcription can still be enabled through the `Start-Transcript` cmdlet.)

References:

1. https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_group_policy_settings?view=powershell-7.2#turn-on-powershell-transcription

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. | | ● | ● |

3.11.55 Windows Remote Management (WinRM)

This section contains recommendations for Windows Remote Management (WinRM).

3.11.55.1 WinRM Client

This section contains recommendations for WinRM Client.

3.11.55.1.1 (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 with a REG_DWORD value of 0.

HKLM\SOFTWARE\Policies\Microsoft\Windows\WinRM\Client:AllowBasic

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to **Disabled**.

Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Client\Allow Basic authentication

Default Value:

Disabled. (The WinRM client does not use Basic authentication.)

References:

1. <https://learn.microsoft.com/en-us/windows/win32/winrm/portal>

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. | | ● | ● |

3.11.55.1.2 (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 with a REG_DWORD value of 0.

HKLM\SOFTWARE\Policies\Microsoft\Windows\WinRM\Client:AllowUnencryptedTraffic

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to **Disabled**.

Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Client\Allow unencrypted traffic

Default Value:

Disabled. (The WinRM client sends or receives only encrypted messages over the network.)

References:

1. <https://learn.microsoft.com/en-us/windows/win32/winrm/portal>

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. | ● | ● | ● |

3.11.55.1.3 (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 with a REG_DWORD value of 0.

HKLM\SOFTWARE\Policies\Microsoft\Windows\WinRM\Client:AllowDigest

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Client\Disallow Digest authentication

Default Value:

Disabled. (The WinRM client will use Digest authentication.)

References:

1. <https://learn.microsoft.com/en-us/windows/win32/winrm/portal>

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. | | ● | ● |

3.11.55.2 WinRM Service

This section contains recommendations for WinRM Service.

3.11.55.2.1 (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 with a REG_DWORD value of 0.

HKLM\SOFTWARE\Policies\Microsoft\Windows\WinRM\Service:AllowBasic

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to **Disabled**.

Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Service\Allow Basic authentication

Default Value:

Disabled. (The WinRM service will not accept Basic authentication from a remote client.)

References:

1. <https://learn.microsoft.com/en-us/windows/win32/winrm/portal>

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. | | ● | ● |

3.11.55.2.2 (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 setting is backed by the following registry location with a REG_DWORD value of 0.

HKLM\SOFTWARE\Policies\Microsoft\Windows\WinRM\Service:AllowAutoConfig

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`.

Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Service\Allow remote server management through WinRM

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.)

References:

1. <https://learn.microsoft.com/en-us/windows/win32/winrm/portal>

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> | ● | ● | ● |

3.11.55.2.3 (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 with a REG_DWORD value of 0.

HKLM\SOFTWARE\Policies\Microsoft\Windows\WinRM\Service:AllowUnencryptedTraffic

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to **Disabled**.

Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Service\Allow unencrypted traffic

Default Value:

Disabled. (The WinRM service sends or receives only encrypted messages over the network.)

References:

1. <https://learn.microsoft.com/en-us/windows/win32/winrm/portal>

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. | ● | ● | ● |

3.11.55.2.4 (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 with a `REG_DWORD` value of 1.

HKLM\SOFTWARE\Policies\Microsoft\Windows\WinRM\Service:DisableRunAs

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled.

Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Service\Disallow WinRM from storing RunAs credentials

Default Value:

Disabled. (The WinRM service will allow the RunAsUser and RunAsPassword configuration values to be set for plug-ins and the RunAsPassword value will be stored securely.)

References:

1. <https://learn.microsoft.com/en-us/windows/win32/winrm/portal>

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| v7 | 14.3 Disable Workstation to Workstation Communication Disable all workstation to workstation communication to limit an attacker's ability to move laterally and compromise neighboring systems, through technologies such as Private VLANs or microsegmentation. | | ● | ● |

3.11.56 Windows Remote Shell

This section contains recommendations for Windows Remote Shell.

3.11.56.1 (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 setting is backed by the following registry location with a REG_DWORD value of 0.

HKLM\SOFTWARE\Policies\Microsoft\Windows\WinRM\Service\WinRS:AllowRemoteShellAccess

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Disabled.

Administrative Templates\Windows Components\Windows Remote Shell\Allow Remote Shell Access

Default Value:

Enabled. (New Remote Shell connections 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> | ● | ● | ● |

4 Application Defaults

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

5 Auditing

This section contains recommendations for Auditing.

5.1 (L1) Ensure 'Account Logon 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.

OR

To audit the system using `auditpol.exe`, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"Credential Validation"
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Success and Failure.

```
Auditing\Account Logon Audit Credential Validation
```

Default Value:

No Auditing.

References:

1. <https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-credential-validation>

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. | | ● | ● |

5.2 (L1) Ensure 'Account Logon Logoff 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.

OR

To audit the system using auditpol.exe, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"Account Lockout"
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Failure.

Auditing\Account Logon Logoff Audit Account Lockout

Default Value:

Success.

References:

1. <https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-account-lockout>

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. | ● | ● | ● |

5.3 (L1) Ensure 'Account Logon Logoff 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.

OR

To audit the system using `auditpol.exe`, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"Group Membership"
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Success.

Auditing\Account Logon Logoff Audit Group Membership

Default Value:

No Auditing.

References:

1. <https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-group-membership>

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. | | ● | ● |

5.4 (L1) Ensure 'Account Logon Logoff 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.

OR

To audit the system using `auditpol.exe`, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"Logoff"
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Success.

```
Auditing\Account Logon Logoff Audit Logoff
```

Default Value:

Success.

References:

1. <https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-logoff>

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. | | | ● |

5.5 (L1) Ensure 'Account Logon Logoff 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.

OR

To audit the system using `auditpol.exe`, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"Logon"
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Success and Failure.

```
Auditing\Account Logon Logoff Audit Logon
```

Default Value:

Success.

References:

1. <https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-logon>

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. | | | ● |

5.6 (L1) Ensure 'Account Management 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.

Note: Although Microsoft "[Deprecated](#)" Windows Authorization Manager (AzMan) in Windows Server 2012 and 2012 R2, this feature still exists in the OS (unimproved), and therefore should still be audited.

Rationale:

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.

OR

To audit the system using `auditpol.exe`, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"Application Group Management"
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Success and Failure.

```
Auditing\Account Management Audit Application Group Management
```

Default Value:

No Auditing.

References:

1. <https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-application-group-management>
2. <https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/advanced-security-audit-policy-settings>

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. | | ● | ● |

5.7 (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.

OR

To audit the system using `auditpol.exe`, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"Authentication Policy Change"
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Success.

```
Auditing\Audit Authentication Policy Change
```

Default Value:

Success.

References:

1. <https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-authentication-policy-change>

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. | | ● | ● |

5.8 (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:

- 4703: A user right was adjusted.
- 4704: A user right was assigned.
- 4705: A user right was removed.
- 4670: Permissions on an object were changed.
- 4911: Resource attributes of the object were changed.
- 4913: Central Access Policy on the object was changed.

The recommended state for this setting is to include: Success.

Rationale:

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.

OR

To audit the system using `auditpol.exe`, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"Authorization Policy Change"
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Success.

```
Auditing\Audit Authorization Policy Change
```

Default Value:

Success.

References:

1. <https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-authorization-policy-change>

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. | | ● | ● |

5.9 (L1) Ensure 'Audit Changes to Audit Policy' 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.

OR

To audit the system using `auditpol.exe`, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"Audit Policy Change"
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Success.

```
Auditing\Audit Changes to Audit Policy
```

Default Value:

Success.

References:

1. <https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-audit-policy-change>

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. | | ● | ● |

5.10 (L1) Ensure 'Audit File Share Access' 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.

OR

To audit the system using `auditpol.exe`, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"File Share"
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Success and Failure.

Auditing\Audit File Share Access

Default Value:

No Auditing.

References:

1. <https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-file-share>

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|------|------|------|
| v8 | 8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. | | ● | ● |
| v7 | 6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements. | | ● | ● |
| v7 | 14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. | ● | ● | ● |

5.11 (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.

OR

To audit the system using `auditpol.exe`, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"Other Logon/Logoff Events"
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Success and Failure.

```
Auditing\Audit Other Logon Logoff Events
```

Default Value:

No Auditing.

References:

1. <https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-other-logonlogoff-events>

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. | | | ● |

5.12 (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.

OR

To audit the system using `auditpol.exe`, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"Security Group Management"
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Success.

```
Auditing\Audit Security Group Management
```

Default Value:

Success.

References:

1. <https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-security-group-management>
2. <https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/advanced-security-audit-policy-settings>

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. | | ● | ● |

5.13 (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.

OR

To audit the system using `auditpol.exe`, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"Security System Extension"
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Success.

```
Auditing\Audit Security System Extension
```

Default Value:

No Auditing.

References:

1. <https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-security-system-extension>

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. | | ● | ● |

5.14 (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.

OR

To audit the system using `auditpol.exe`, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"Special Logon"
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Success.

Auditing\Audit Special Logon

Default Value:

Success.

References:

1. <https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-special-logon>

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. | | | ● |

5.15 (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.

OR

To audit the system using `auditpol.exe`, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"User Account Management"
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Success and Failure.

```
Auditing\Audit User Account Management
```

Default Value:

Success.

References:

1. <https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-user-account-management>
2. <https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/advanced-security-audit-policy-settings>

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. | ● | ● | |

5.16 (L1) Ensure 'Detailed Tracking 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.

OR

To audit the system using `auditpol.exe`, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"PNP Activity"
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Success.

Auditing\Detailed Tracking Audit PNP Activity

Default Value:

No Auditing.

References:

1. <https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-pnp-activity>

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. | | ● | ● |

5.17 (L1) Ensure 'Detailed Tracking 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.

OR

To audit the system using `auditpol.exe`, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"Process Creation"
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Success.

```
Auditing\Detailed Tracking Audit Process Creation
```

Default Value:

No Auditing.

References:

1. <https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-process-creation>

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. | | ● | ● |

5.18 (L1) Ensure 'Object Access 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.

OR

To audit the system using auditpol.exe, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"Detailed File Share"
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Failure.

Auditing\Object Access Audit Detailed File Share

Default Value:

No Auditing.

References:

1. <https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-detailed-file-share>

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|------|------|------|
| v8 | 8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. | | ● | ● |
| v7 | 6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements. | | ● | ● |
| v7 | 14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. | ● | ● | ● |

5.19 (L1) Ensure 'Object Access 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.

OR

To audit the system using `auditpol.exe`, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"Audit Other Object Access Events"
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Success and Failure.

```
Auditing\Object Access Audit Other Object Access Events
```

Default Value:

No Auditing.

References:

1. <https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-other-object-access-events>

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. | | ● | ● |

5.20 (L1) Ensure 'Object Access 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.

OR

To audit the system using `auditpol.exe`, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"Removable Storage"
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Success and Failure.

```
Auditing\Object Access Audit Removable Storage
```

Default Value:

No Auditing.

References:

1. <https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-removable-storage>

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. | | ● | ● |

5.21 (L1) Ensure 'Policy Change 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.

OR

To audit the system using `auditpol.exe`, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"MPSSVC Rule-Level Policy Change"
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Success and Failure.

```
Auditing\Policy Change Audit MPSSVC Rule Level Policy Change
```

Default Value:

No Auditing.

References:

1. <https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-mpssvc-rule-level-policy-change>

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> | ● | ● | ● |

5.22 (L1) Ensure 'Policy Change 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.

OR

To audit the system using `auditpol.exe`, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"Other Policy Change Events"
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Failure.

```
Auditing\Policy Change Audit Other Policy Change Events
```

Default Value:

No Auditing.

References:

1. <https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-other-policy-change-events>

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. | | ● | ● |

5.23 (L1) Ensure 'Privilege Use 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.

OR

To audit the system using `auditpol.exe`, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"Sensitive Privilege Use"
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Success and Failure.

```
Auditing\Privilege Use Audit Sensitive Privilege Use
```

Default Value:

No Auditing.

References:

1. <https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-sensitive-privilege-use>

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. | ● | ● | |

5.24 (L1) Ensure 'System Audit / Psec 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.

OR

To audit the system using `auditpol.exe`, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"IPsec Driver"
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Success and Failure.

```
Auditing\System Audit\IPsec Driver
```

Default Value:

No Auditing.

References:

1. <https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-ipsec-driver>

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>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> | ● | ● | |

5.25 (L1) Ensure 'System 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.

OR

To audit the system using `auditpol.exe`, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"Other System Events"
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Success and Failure.

```
Auditing\System Audit Other System Events
```

Default Value:

Success and Failure.

References:

1. <https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-other-system-events>

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. | | ● | ● |

5.26 (L1) Ensure 'System 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.

OR

To audit the system using `auditpol.exe`, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"Security State Change"
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Success.

```
Auditing\System Audit Security State Change
```

Default Value:

Success.

References:

1. <https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-security-state-change>

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. | | ● | ● |

5.27 (L1) Ensure 'System 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.

OR

To audit the system using `auditpol.exe`, perform the following and confirm it is set as prescribed:

```
auditpol /get /subcategory:"System Integrity"
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Success and Failure.

```
Auditing\System Audit System Integrity
```

Default Value:

Success and Failure.

References:

1. <https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-system-integrity>

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. | ● | ● | ● |

6 Authentication

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

7 BitLocker

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

8 BITS

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

9 Bluetooth

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

10 Browser

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

11 Camera

This section contains recommendations for Camera.

11.1 (L2) Ensure 'Allow Camera' is set to 'Not allowed' (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: Not allowed.

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:

1. Navigate to the following registry location and note the *WinningProvider* GUID. This value confirms under which User GUID the policy is set.

HKLM\SOFTWARE\Microsoft\PolicyManager\current\device\Camera:AllowCamera_WinningProvider

2. Navigate to the following registry location and confirm the value is set to 0.

HKLM\SOFTWARE\Microsoft\PolicyManager\Providers\{GUID}\Default\Device\Camera:AllowCamera

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Not allowed:

Camera\Allow Camera

Default Value:

Enabled. (Camera devices are enabled.)

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> | | ● | ● |

12 Cellular

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

13 Cloud Desktop

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

14 Config Refresh

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

15 Connectivity

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

16 Control Policy Conflict

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

17 Converters

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

18 Credential Providers

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

19 Cryptography

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

20 Data Protection

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

21 Defender

This section contains recommendations for Defender.

21.1 (L1) Ensure 'Allow Behavior Monitoring' is set to 'Allowed' (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: Allowed.

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 with a REG_DWORD value of 1.

HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Policy Manager:AllowBehaviorMonitoring

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Allowed.

Defender\Allow Behavior Monitoring

Default Value:

Enabled. (Behavior monitoring will be enabled.)

References:

1. <https://learn.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. | ● | ● | ● |

21.2 (L1) Ensure 'Allow Email Scanning' is set to 'Allowed' (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: Allowed.

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 with a REG_DWORD value of 1.

HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Policy Manager:AllowEmailScanning

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Allowed.

Defender\Allow Email Scanning

Default Value:

Disabled. (E-mail scanning by Microsoft Defender Antivirus will be disabled.)

References:

1. <https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-advanced-scan-types-microsoft-defender-antivirus?view=o365-worldwide#settings-and-locations>

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. | | ● | ● |

21.3 (L1) Ensure 'Allow Full Scan Removable Drive Scanning' is set to 'Allowed' (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: Allowed.

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 with a REG_DWORD value of 1.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Policy Manager:AllowFullScanRemovableDriveScanning
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Allowed.

```
Defender Antivirus\Allow Full Scan Removable Drive Scanning
```

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.)

References:

1. <https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-advanced-scan-types-microsoft-defender-antivirus?view=o365-worldwide#settings-and-locations>

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | <u>10.4 Configure Automatic Anti-Malware Scanning of Removable Media</u> Configure anti-malware software to automatically scan removable media. | | ● | ● |
| v7 | <u>8.4 Configure Anti-Malware Scanning of Removable Devices</u> Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected. | ● | ● | ● |

21.4 (L1) Ensure 'Allow Realtime Monitoring' is set to 'Allowed' (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: Allowed.

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 with a REG_DWORD value of 1.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Policy Manager:AllowRealtimeMonitoring
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Allowed.

```
Defender\Allow Realtime Monitoring
```

Default Value:

Disabled. (Microsoft Defender Antivirus will prompt users to take actions on malware detections.)

References:

1. <https://learn.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-antivirus/configure-real-time-protection-microsoft-defender-antivirus>
2. <https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-protection-features-microsoft-defender-antivirus?view=o365-worldwide>

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. | | ● | ● |

21.5 (L1) Ensure 'Allow scanning of all downloaded files and attachments' is set to 'Allowed' (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: Allowed.

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 with a REG_DWORD value of 1.

HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Policy Manager:AllowIOAVProtection

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Allowed.

Defender\Allow scanning of all downloaded files and attachments

Default Value:

Enabled. (All downloaded files and attachments will be scanned.)

References:

1. <https://learn.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 | 10.1 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. | | ● | ● |

21.6 (L1) Ensure 'Allow Script Scanning' is set to 'Allowed' (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: Allowed.

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 with a REG_DWORD value of 1.

HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Policy Manager:AllowScriptScanning

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Allowed.

Defender\Allow Script Scanning

Default Value:

Enabled. (Script scanning will be enabled.)

References:

1. <https://learn.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. | ● | ● | ● |

21.7 (L1) Ensure 'Attack Surface Reduction rules' are 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 all settings is Block

```
Block abuse of exploited vulnerable signed drivers (Device)
Block Adobe Reader from creating child processes
Block all Office applications from creating child processes
Block credential stealing from the Windows local security authority subsystem
Block executable content from email client and webmail
Block execution of potentially obfuscated scripts
Block JavaScript or VBScript from launching downloaded executable content
Block Office applications from creating executable content
Block Office applications from injecting code into other processes
Block Office communication application from creating child processes
Block persistence through WMI event subscription
Block untrusted and unsigned processes that run from USB
Block Win32 API calls from Office macros
```

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:

```
SOFTWARE\Policies\Microsoft\Windows Defender\Policy Manager  
Type: REG_SZ  
Value Name: ASRRules
```

The contents of `ASRRules` is a single large string containing the GUID of each ASR rule separated with a pipe delimiter like below:

```
56a863a9-875e-4185-98a7-b882c64b5ce5=1|7674ba52-37eb-4a4f-a9a1-  
f0f9a1619a2c=1|D4F940AB-401B-4EFC-AADC-AD5F3C50688A=1|9e6c4e1f-7d60-472f-  
b1a-a39ef669e4b2=1|BE9BA2D9-53EA-4CDC-84E5-9B1EEEE46550=1|5BEB7EFE-FD9A-  
4556-801D-275E5FFC04CC=1|D3E037E1-3EB8-44C8-A917-57927947596D=1|3B576869-  
A4EC-4529-8536-B80A7769E899=1|75668C1F-73B5-4CF0-BB93-  
3ECF5CB7CC84=1|26190899-1602-49e8-8b27-eb1d0a1ce869=1|e6db77e5-3df2-4cf1-  
b95a-636979351e5b=1|b2b3f03d-6a65-4f7b-a9c7-1c7ef74a9ba4=1|92E97FA1-2EDF-  
4476-BDD6-9DD0B4DDDC7B=1
```

GUID Reference:

```
56a863a9-875e-4185-98a7-b882c64b5ce5 - Block abuse of exploited vulnerable  
signed drivers (Device)  
7674ba52-37eb-4a4f-a9a1-f0f9a1619a2c - Block Adobe Reader from creating child  
processes  
d4f940ab-401b-4efc-aadc-ad5f3c50688a - Block all Office applications from  
creating child processes  
9e6c4e1f-7d60-472f-b1a-a39ef669e4b2 - Block credential stealing from the  
Windows local security authority subsystem  
be9ba2d9-53ea-4cdc-84e5-9b1eeee46550 - Block executable content from email  
client and webmail  
5beb7efe-fd9a-4556-801d-275e5ffc04cc - Block execution of potentially  
obfuscated scripts  
d3e037e1-3eb8-44c8-a917-57927947596d - Block JavaScript or VBScript from  
launching downloaded executable content  
3b576869-a4ec-4529-8536-b80a7769e899 - Block Office applications from  
creating executable content  
75668c1f-73b5-4cf0-bb93-3ecf5cb7cc84 - Block Office applications from  
injecting code into other processes  
26190899-1602-49e8-8b27-eb1d0a1ce869 - Block Office communication application  
from creating child processes  
e6db77e5-3df2-4cf1-b95a-636979351e5b - Block persistence through WMI event  
subscription  
b2b3f03d-6a65-4f7b-a9c7-1c7ef74a9ba4 - Block untrusted and unsigned processes  
that run from USB  
92e97fa1-2edf-4476-bdd6-9dd0b4dddc7b - Block Win32 API calls from Office  
macros
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog paths to Block.

```
Defender\Block abuse of exploited vulnerable signed drivers (Device)
Defender\Block Adobe Reader from creating child processes
Defender\Block all Office applications from creating child processes
Defender\Block credential stealing from the Windows local security authority
subsystem
Defender\Block executable content from email client and webmail
Defender\Block execution of potentially obfuscated scripts
Defender\Block JavaScript or VBScript from launching downloaded executable
content
Defender\Block Office applications from creating executable content
Defender\Block Office applications from injecting code into other processes
Defender\Block Office communication application from creating child processes
Defender\Block persistence through WMI event subscription
Defender\Block untrusted and unsigned processes that run from USB
Defender\Block Win32 API calls from Office macros
```

Default Value:

Disabled. (No ASR rules will be configured.)

References:

1. <https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-attack-surface-reduction?view=o365-worldwide>
2. <https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction?view=o365-worldwide>

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. | | ● | ● |

21.8 (L2) Ensure 'Enable File Hash Computation' is set to 'Enable' (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: Enable.

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 with a REG_DWORD value of 1.

| |
|--|
| HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Policy Manager:EnableFileHashComputation |
|--|

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Enable`.

```
Defender\Enable File Hash Computation
```

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. | | ● | ● |

21.9 (L1) Ensure 'Enable Network Protection' is set to 'Enabled (block mode)' (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 mode).

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 with a REG_DWORD value of 1.

HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Policy Manager:EnableNetworkProtection

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled (block mode):

Defender\Enable Network Protection

Default Value:

Disabled. (Users and applications will not be blocked from connecting to dangerous domains.)

References:

1. <https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/network-protection?view=o365-worldwide>

CIS Controls:

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

21.10 (L1) Ensure 'PUA Protection' is set to 'PUA Protection on' (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: PUA Protection on.

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 with a REG_DWORD value of 1.

HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Policy Manager:PUAProtection

Remediation:

To establish the recommended configuration via GP, set the following UI path to PUA Protection on:

Defender\PUA Protection

Default Value:

Disabled. (Applications that are identified by Microsoft as PUA will not be blocked.)

References:

1. <https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/detect-block-potentially-unwanted-apps-microsoft-defender-antivirus?view=o365-worldwide>

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 | 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. | ● | ● | ● |

22 Delivery Optimization

This section contains recommendations for Delivery Optimization.

22.1 (L1) Ensure 'DO Download Mode' is NOT set to 'HTTP blended with Internet Peering' (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:

1. Navigate to the following registry location and note the *WinningProvider* GUID.
This value confirms under which User GUID the policy is set.

HKLM\SOFTWARE\Microsoft\PolicyManager\current\device\DeliveryOptimization:DOD
ownloadMode_WinningProvider

2. Navigate to the following registry location and confirm the value is set to anything *other than* 3.

HKLM\SOFTWARE\Microsoft\PolicyManager\Providers\{GUID}\Default\Device\DeliveryOptimization:DODownloadMode

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to any value *other than* HTTP blended with Internet Peering:

Delivery Optimization\DO Download Mode

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. | ● | ● | ● |

23 Device Guard

This section contains recommendations for Device Guard.

23.1 (NG) Ensure 'Enable Virtualization Based Security' is set to 'Enable virtualization based security' (Automated)

Profile Applicability:

- Next Generation Windows Security (NG)

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 with a REG_DWORD value of 1.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\DeviceGuard:EnableVirtualizationBasedSecurity
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enable virtualization based security:

```
Device Guard\Enable Virtualization Based Security
```

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. | | ● | ● |

23.2 (NG) Ensure 'Require Platform Security Features' is set to 'Turns on VBS with Secure Boot' or higher (Automated)

Profile Applicability:

- Next Generation Windows Security (NG)

Description:

This policy setting specifies whether Virtualization Based Security (VBS) is enabled. VBS uses the Windows Hypervisor to provide support for security services.

The recommended state for this setting is: Turns on VBS with Secure Boot **or** Turns on VBS with Secure Boot and direct memory access (DMA). DMA requires hardware support.

Note: VBS requires a 64-bit version of Windows with Secure Boot enabled, which in turn requires that Windows was installed with a UEFI BIOS configuration, not a Legacy BIOS configuration. In addition, if running Windows on a virtual machine, the hardware-assisted CPU virtualization feature (Intel VT-x or AMD-V) must be exposed by the host to the guest VM.

More information on system requirements for this feature can be found at [Windows Defender Credential Guard Requirements \(Windows 10\) | Microsoft Docs](#)

Note #2: Credential Guard and Device Guard are not currently supported when using Azure IaaS VMs.

Rationale:

Secure Boot can help reduce the risk of bootloader attacks and in conjunction with DMA protections to help protect data from being scraped from memory.

Impact:

Choosing the `Secure Boot` option provides the system with as much protection as is supported by the computer's hardware. A system with input/output memory management units (IOMMUs) will have Secure Boot with DMA protection. A system without IOMMUs will simply have Secure Boot enabled without DMA protection.

Choosing the `Secure Boot with DMA protection` option requires the system to have IOMMUs in order to enable VBS. Without IOMMU hardware support, VBS will be disabled.

Warning: All drivers on the system must be compatible with this feature or the system may crash. Ensure that this policy setting is only deployed to computers which are known to be compatible.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a REG_DWORD value of 1 or 3.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\DeviceGuard:RequirePlatformSecurityFeatures
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Turns on VBS with Secure Boot OR Turns on VBS with Secure Boot and direct memory access (DMA). DMA requires hardware support:

```
Device Guard\Require Platform Security Features
```

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. | | ● | ● |

23.3 (NG) Ensure 'Credential Guard' is set to 'Enabled with UEFI lock' (Automated)

Profile Applicability:

- Next Generation Windows Security (NG)

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 with a REG_DWORD value of 1.

HKLM\SOFTWARE\Policies\Microsoft\Windows\DeviceGuard:LsaCfgFlags

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled with UEFI lock:

Device Guard\Credential Guard

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. | | ● | ● |

23.4 (NG) Ensure 'Configure System Guard Launch' is set to 'Unmanaged Enables Secure Launch if supported by hardware'
(Automated)

Profile Applicability:

- Next Generation Windows Security (NG)

Description:

Secure Launch protects the Virtualization Based Security environment from exploited vulnerabilities in device firmware.

The recommended state for this setting is: Unmanaged Enables Secure Launch if supported by hardware.

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 with a REG_DWORD value of 1.

HKLM\SOFTWARE\Policies\Microsoft\Windows\DeviceGuard:ConfigureSystemGuardLaunch

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Unmanaged Enables Secure Launch if supported by hardware:

Device Guard\Configure System Guard Launch

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. | | ● | ● |

24 Device Lock

This section contains recommendations for Device Lock.

Settings in this section are intended to be configured together with the Windows Hello for Business settings. Device Lock password settings will apply to only local user accounts as long as the key **Policies** exists in this registry key path:

HKLM\SOFTWARE\Microsoft\Policies\PassportForWork\<Tenant-ID>\Device\Policies

If the key does not exist or is removed, then Device Lock password settings will also impact Windows Hello PINs if they are being utilized. This could cause an undesired PIN requirement of 14 characters in length, for example. The Policies key above is created whenever a Windows Hello For Business policy is added to a device and remains in the registry even after the setting is removed from a Settings Catalog profile or is unassigned.

24.1 (L1) Ensure 'Alphanumeric Device Password Required' is set to 'Password, Numeric PIN, or Alphanumeric PIN required' (Automated)

Profile Applicability:

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

Description:

This policy setting determines the type of PIN or password required. This policy only applies if the DeviceLock/DevicePasswordEnabled policy is set to 0. In settings catalog this setting is a pre-requisite for "Min Device Password Complex Characters".

The recommended state for this setting is: Password, Numeric PIN, or Alphanumeric PIN required.

Rationale:

This is a pre-requisite for "Min Device Password Complex Characters", which enforces a more complex local user account password. This has no impact on Entra ID accounts.

Impact:

If an organization is using **Windows Hello for Business**, the the Device Lock password settings can impact PIN polices if those policies are not first defined elsewhere.

Windows will follow the Windows Hello for Business policies for PINs if this key exists:

HKLM\SOFTWARE\Microsoft\Policies\PassportForWork\<Tenant-ID>\Device\Policies.

Otherwise, it will follow Device Lock policies.

This benchmark recommends configuring Device Lock policies for Local User accounts and Windows Hello for Business policies for PINs.

Audit:

1. Navigate to the following registry location and note the *WinningProvider* GUID.
This value confirms under which User GUID the policy is set.

HKLM\SOFTWARE\Microsoft\PolicyManager\current\device\DeviceLock:AlphanumericDevicePasswordRequired_WinningProvider

2. Navigate to the following registry location and confirm the value is set to 2.

HKLM\SOFTWARE\Microsoft\PolicyManager\Providers\{GUID}\Default\Device\DeviceLock:AlphanumericDevicePasswordRequired

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Password, Numeric PIN, or Alphanumeric PIN required:

Device Lock\Device Password Enabled: Alphanumeric Device Password Required

Default Value:

2

References:

1. <https://www.cisecurity.org/white-papers/cis-password-policy-guide/>
2. https://learn.microsoft.com/en-us/windows/client-management/mdm/policy-csp-devicelock?WT.mc_id=Portal-fx#alphanumericdevicepasswordrequired

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. | | ● | ● |

24.2 (L1) Ensure 'Device Password Expiration' 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 730 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.

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.

Warning: If an organization is using **Windows Hello for Business**, the Device Lock password settings can impact PIN policies if those policies are not first defined elsewhere. Windows will follow the Windows Hello for Business policies for PINs if this key exists: `HKLM\SOFTWARE\Microsoft\Policies\PassportForWork\<Tenant-ID>\Device\Policies`. Otherwise, it will follow Device Lock policies.

This benchmark recommends configuring Device Lock policies for Local User accounts and Windows Hello for Business policies for PINs.

Audit:

1. Navigate to the following registry location and note the *WinningProvider* GUID.
This value confirms under which User GUID the policy is set.

HKLM\SOFTWARE\Microsoft\PolicyManager\current\device\DeviceLock:DevicePasswordExpiration_WinningProvider

2. Navigate to the following registry location and confirm the value is set to 365 or fewer days, but not 0.

HKLM\SOFTWARE\Microsoft\PolicyManager\Providers\{GUID}\Default\Device\DeviceLock:DevicePasswordExpiration

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to 365 or fewer days, but not 0:

Device Lock\Device Password Enabled: Device Password Expiration

Default Value:

0

References:

1. <https://www.cisecurity.org/white-papers/cis-password-policy-guide/>
2. https://learn.microsoft.com/en-us/windows/client-management/mdm/policy-csp-devicelock?WT.mc_id=Portal-Microsoft_Intune_Workflows#devicepasswordexpiration

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. | | ● | ● |

24.3 (L1) Ensure 'Device 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. In an Intune managed environment this setting applies to local user accounts and not Entra ID accounts.

The value includes the user's current password. This value denotes that with a setting of 1, the user can't reuse their current password when choosing a new password, while a setting of 5 means that a user can't set their new password to their current password or any of their previous four passwords.

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

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.

Warning: If an organization is using **Windows Hello for Business**, the Device Lock password settings can impact PIN policies if those policies are not first defined elsewhere. Windows will follow the Windows Hello for Business policies for PINs if this key exists: HKLM\SOFTWARE\Microsoft\Policies\PassportForWork\<Tenant-ID>\Device\Policies. Otherwise, it will follow Device Lock policies.

This benchmark recommends configuring Device Lock policies for Local User accounts and Windows Hello for Business policies for PINs.

Audit:

1. Navigate to the following registry location and note the *WinningProvider* GUID. This value confirms under which User GUID the policy is set.

```
HKLM\SOFTWARE\Microsoft\PolicyManager\current\device\DeviceLock:DevicePasswordHistory_WinningProvider
```

2. Navigate to the following registry location and confirm the value is set to 2.

```
HKLM\SOFTWARE\Microsoft\PolicyManager\Providers\{GUID}\Default\Device\DeviceLock:DevicePasswordHistory
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to 24 or more password(s):

```
Device Lock\Device Password Enabled: Device Password History
```

Default Value:

0

References:

1. <https://www.cisecurity.org/white-papers/cis-password-policy-guide/>
2. https://learn.microsoft.com/en-us/windows/client-management/mdm/policy-csp-devicelock?WT.mc_id=Portal-fx#devicepasswordhistory

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. | | ● | ● |

24.4 (L1) Ensure 'Min Device Password Complex Characters' is set to 'Digits lowercase letters and uppercase letters are required' (Automated)

Profile Applicability:

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

Description:

The number of complex element types (uppercase and lowercase letters, numbers, and punctuation) required for a strong PIN or password.

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)

The recommended state for this setting is: Digits lowercase letters and uppercase letters are required.

Note: The enforcement of policies for Microsoft accounts happens on the server, and the server requires a password length of 8 and a complexity of 2. A complexity value of 3 or 4 is unsupported and setting this value on the server makes Microsoft accounts non-compliant.

Rationale:

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

Impact:

If an organization is using **Windows Hello for Business**, the the Device Lock password settings can impact PIN polices if those policies are not first defined elsewhere.

Windows will follow the Windows Hello for Business policies for PINs if this key exists:

HKLM\SOFTWARE\Microsoft\Policies\PassportForWork\<Tenant-ID>\Device\Policies.
Otherwise, it will follow Device Lock policies.

Audit:

1. Navigate to the following registry location and note the *WinningProvider* GUID.
This value confirms under which User GUID the policy is set.

```
HKLM\SOFTWARE\Microsoft\PolicyManager\current\device\DeviceLock:MinDevicePasswordComplexCharacters_WinningProvider
```

2. Navigate to the following registry location and confirm the value is set to 3.

```
HKLM\SOFTWARE\Microsoft\PolicyManager\Providers\{GUID}\Default\Device\DeviceLock:MinDevicePasswordComplexCharacters
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Digits lowercase letters and uppercase letters are required:

```
Device Lock\Device Password Enabled: Alphanumeric Device Password Required:  
Min Device Password Complex Characters
```

Note: As of January 30 2024 this setting is nested under Alphanumeric Device Password Required and may not fully appear in Settings Catalog unless unchecked and re-checked in the settings picker.

Default Value:

1

References:

1. <https://www.cisecurity.org/white-papers/cis-password-policy-guide/>
2. https://learn.microsoft.com/en-us/windows/client-management/mdm/policy-csp-devicelock?WT.mc_id=Portal-Microsoft_Intune_Workflows#mindevicepasswordcomplexcharacters

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> | | ● | ● |

24.5 (L1) Ensure 'Min Device 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 local 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 or newer, passphrases can be quite long and can include spaces. Therefore, a phrase such as "I want to drink a \$5 milkshake" is a valid passphrase; it is a considerably stronger password than an 8 or 10 character string of random numbers and letters, and yet is easier to remember. Users must be educated about the proper selection and maintenance of passwords, especially around password length. In enterprise environments, the ideal value for the Minimum password length setting is 14 characters, however you should adjust this value to meet your organization's business requirements.

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

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.

Warning: If an organization is using **Windows Hello for Business**, the Device Lock password settings can impact PIN policies if those policies are not first defined elsewhere. Windows will follow the Windows Hello for Business policies for PINs if this key exists: `HKLM\SOFTWARE\Microsoft\Policies\PassportForWork\<Tenant-ID>\Device\Policies`. Otherwise, it will follow Device Lock policies.

This benchmark recommends configuring Device Lock policies for Local User accounts and Windows Hello for Business policies for PINs

Note: [Windows Autopilot - Policy Conflicts](#): The out-of-box experience (OOBE) or user desktop auto logon can fail when a device reboots during the device Enrollment Status Page (ESP). This failure can occur when certain DeviceLock policies are applied to a device. An exception to this recommendation might be needed is Windows AutoPilot if used.

Audit:

1. Navigate to the following registry location and note the *WinningProvider* GUID. This value confirms under which User GUID the policy is set.

```
HKLM\SOFTWARE\Microsoft\PolicyManager\current\device\DeviceLock:MinDevicePasswordLength_WinningProvider
```

2. Navigate to the following registry location and confirm the value is set to 14 (or higher).

```
HKLM\SOFTWARE\Microsoft\PolicyManager\Providers\{GUID}\Default\Device\DeviceLock:MinDevicePasswordLength
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to 14 or more character(s):

```
Device Lock\Device Password Enabled: Min Device Password Length
```

Default Value:

4

References:

1. <https://www.cisecurity.org/white-papers/cis-password-policy-guide/>
2. https://learn.microsoft.com/en-us/windows/client-management/mdm/policy-csp-devicelock?WT.mc_id=Portal-Microsoft_Intune_Workflows#mindevicepasswordlength

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. | | ● | ● |

24.6 (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 security setting determines the period of time (in days) that a password must be used before the user can change it. You can set a value between 1 and 998 days, or you can allow changes immediately by setting the number of days to 0.

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

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.

Warning: If an organization is using **Windows Hello for Business**, the Device Lock password settings can impact PIN policies if those policies are not first defined elsewhere. Windows will follow the Windows Hello for Business policies for PINs if this key exists: HKLM\SOFTWARE\Microsoft\Policies\PassportForWork\<Tenant-ID>\Device\Policies. Otherwise, it will follow Device Lock policies.

This benchmark recommends configuring Device Lock policies for Local User accounts and Windows Hello for Business policies for PINs.

Audit:

1. Navigate to the following registry location and note the *WinningProvider* GUID.
This value confirms under which User GUID the policy is set.

HKLM\SOFTWARE\Microsoft\PolicyManager\current\device\DeviceLock:MinimumPasswordAge_WinningProvider

2. Navigate to the following registry location and confirm the value is set to 0.

HKLM\SOFTWARE\Microsoft\PolicyManager\Providers\{GUID}\Default\Device\DeviceLock:MinimumPasswordAge

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to 1 (or more day(s)):

Device Lock\Minimum Password Age

Default Value:

1

References:

1. <https://www.cisecurity.org/white-papers/cis-password-policy-guide/>
2. https://learn.microsoft.com/en-us/windows/client-management/mdm/policy-csp-devicelock?WT.mc_id=Portal-Microsoft_Intune_Workflows#minimumpasswordage

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. | | ● | ● |

25 Dma Guard

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

26 Eap

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

27 Education

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

28 Enterprise Cloud Print

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

29 eSIM

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

30 Experience

This section contains recommendations for Experience.

30.1 (L1) Ensure 'Allow Cortana' is set to 'Block' (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: Block.

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:

1. Navigate to the following registry location and note the *WinningProvider* GUID.
This value confirms under which User GUID the policy is set.

```
HKLM\SOFTWARE\Microsoft\PolicyManager\current\device\Experience:AllowCortana_WinningProvider
```

2. Navigate to the following registry location and confirm the value is set to 0.

```
HKLM\SOFTWARE\Microsoft\PolicyManager\Providers\{GUID}\Default\Device\Experience:AllowCortana
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Block:

```
Experience\Allow Cortana
```

Default Value:

Enabled. (Cortana will be allowed on the device.)

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> | ● | ● | ● |

30.2 (L2) Ensure 'Allow Windows Spotlight (User)' is set to 'Block' (Automated)

Profile Applicability:

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

Description:

This policy setting determines whether all Windows Spotlight features are turned on/off (together).

The recommended state for this setting is: Block.

Note: [Per Microsoft TechNet](#), this policy setting only applies to Windows 10 Enterprise and Windows 10 Education editions.

Note #2: Setting this recommendation to `Block` also disables the Recommendation **Allow Tailored Experiences With Diagnostic Data** which was included in the on-prem Workstation Benchmarks. It was not included in the Intune version since this setting is automatically disabled.

Rationale:

Disabling 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:

1. Navigate to the following registry location and note the `WinningProvider` GUID. This value confirms under which User GUID the policy is set.

```
HKLM\SOFTWARE\Microsoft\PolicyManager\current\{USER  
SID}\Experience:AllowWindowsSpotlight_WinningProvider
```

2. Navigate to the following registry location and confirm the value is set to 0.

```
HKLM\SOFTWARE\Microsoft\PolicyManager\Providers\{GUID}\Default\{USER  
SID}\Experience:AllowWindowsSpotlight
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Block`:

```
Experience\Allow Windows Spotlight (User)
```

Default Value:

Disabled. (Windows Spotlight features are allowed.)

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. | | ● | ● |

30.3 (L1) Ensure 'Do not show feedback notifications' is set to 'Feedback notifications are disabled' (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 third-party vendors in an enterprise managed environment.

Impact:

Users will no longer see feedback notifications through the Windows Feedback app.

Audit:

1. Navigate to the following registry location and note the *WinningProvider* GUID. This value confirms under which User GUID the policy is set.

```
HKLM\SOFTWARE\Microsoft\PolicyManager\current\device\Experience:DoNotShowFeedbackNotifications_WinningProvider
```

2. Navigate to the following registry location and confirm the value is set to 1.

```
HKLM\SOFTWARE\Microsoft\PolicyManager\Providers\{GUID}\Default\Device\Experience:DoNotShowFeedbackNotifications
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled:

```
Experience\Do not show feedback notifications
```

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 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| 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. | | ● | ● |

31 Exploit Guard

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

32 Federated Authentication

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

33 Feeds

This section contains recommendations for Feeds.

Note: This section is not viewable when browsing by category. A search for Feeds is necessary to view this section.

33.1 (L2) Ensure 'Enable news and interests' is set to 'Not Allowed' (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: Not Allowed.

Note: This setting only applies to Windows 10. When configured in settings catalog for a Windows 11 system an error will be generated in both Intune and the local event log.

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 third-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 with a REG_DWORD value of 0.

| |
|--|
| HKLM\SOFTWARE\Policies\Microsoft\Windows\Windows Feeds:EnableFeeds |
|--|

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Not Allowed:

Feeds\Enable news and interests

Note: At time of benchmark publication, the **Feeds** category was not visible when browsing by category. To find this setting, search for news and feeds, and the **Feeds** category will show.

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>

Additional Information:

Applies to Windows 10 **only**.

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. | ● | ● | ● |

34 File Explorer

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

35 Firewall

This section contains recommendations for Firewall.

35.1 (L1) Ensure 'Enable Domain Network Firewall' is set to 'True' (Automated)

Profile Applicability:

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

Description:

Select True (recommended) to have Windows Firewall with Advanced Security use the settings for this profile to filter network traffic. If you select False, 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: True.

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 following registry location and confirm the value is set to 1.

```
HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy  
\Mdm\DomainProfile:EnableFirewall
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to True:

```
Firewall\Enable Domain Network Firewall
```

Default Value:

On (recommended). (The Windows Firewall with Advanced Security will be active in this profile.)

References:

1. <https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/best-practices-configuring>
2. <https://learn.microsoft.com/en-us/windows/client-management/mdm/firewall-csp>

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | <p>4.5 <u>Implement and Manage a Firewall on End-User Devices</u></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 <u>Apply Host-based Firewalls or Port Filtering</u></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> | ● | ● | ● |

35.2 (L1) Ensure 'Enable Domain Network Firewall: Default Inbound Action for Domain Profile' is set to 'Block' (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.

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 following registry location and confirm the value is set to 1.

```
HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy  
\Mdm\DomainProfile:DefaultInboundAction
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Block:

```
Firewall\Enable Domain Network Firewall: Default Inbound Action for Domain  
Profile
```

Default Value:

Block (default). (The Windows Firewall with Advanced Security will block all inbound connections that do not match an inbound firewall rule in this profile.)

References:

1. <https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/best-practices-configuring>
2. <https://learn.microsoft.com/en-us/windows/client-management/mdm/firewall-csp>

CIS Controls:

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

35.3 (L1) Ensure 'Enable Domain Network Firewall: Disable Inbound Notifications' is set to 'True' (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: True.

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 following registry location and confirm the value is set to 1.

```
HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy  
\Mdm\DomainProfile:DisableNotifications
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to True:

```
Firewall\Enable Domain Network Firewall: Disable Inbound Notifications
```

Default Value:

Yes. (Windows Firewall with Advanced Security will display a notification when a program is blocked from receiving inbound connections.)

References:

1. <https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/best-practices-configuring>
2. <https://learn.microsoft.com/en-us/windows/client-management/mdm/firewall-csp>

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. | | ● | ● |

35.4 (L1) Ensure 'Enable Private Network Firewall' is set to 'True' (Automated)

Profile Applicability:

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

Description:

Select True (recommended) to have Windows Firewall with Advanced Security use the settings for this profile to filter network traffic. If you select False, 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: True (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 with a REG_DWORD value of 1.

HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy
\Mdm\StandardProfile:EnableFirewall

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to True (recommended):

Firewall\Enable Private Network Firewall

Default Value:

On (recommended). (The Windows Firewall with Advanced Security will be active in this profile.)

References:

1. <https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/best-practices-configuring>
2. <https://learn.microsoft.com/en-us/windows/client-management/mdm/firewall-csp>

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | <p>4.5 <u>Implement and Manage a Firewall on End-User Devices</u></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 <u>Apply Host-based Firewalls or Port Filtering</u></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> | ● | ● | ● |

35.5 (L1) Ensure 'Enable Private Network Firewall: Default Inbound Action for Private Profile' is set to 'Block' (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.

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 with a REG_DWORD value of 1.

```
HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy  
\Mdm\StandardProfile:DefaultInboundAction
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Block:

```
Firewall\Enable Private Network Firewall: Default Inbound Action for Private  
Profile
```

Default Value:

Block (default). (The Windows Firewall with Advanced Security will block all inbound connections that do not match an inbound firewall rule in this profile.)

References:

1. <https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/best-practices-configuring>
2. <https://learn.microsoft.com/en-us/windows/client-management/mdm/firewall-csp>

CIS Controls:

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

35.6 (L1) Ensure 'Enable Private Network Firewall: Disable Inbound Notifications' is set to 'True' (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: True.

Note: When the `Apply local firewall rules` setting is configured to No, it's recommended to also configure the `Display a notification` setting to No. Otherwise, users will continue to receive messages that ask if they want to unblock a restricted inbound connection, but the user's response will be ignored.

Rationale:

Firewall notifications can be complex and may confuse the end users, who would not be able to address the alert.

Impact:

Windows Firewall will not display a notification when a program is blocked from receiving inbound connections.

Audit:

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

```
HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy  
\Mdm\StandardProfile:DisableNotifications
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to True:

```
Firewall\Enable Private Network Firewall: Disable Inbound Notifications
```

Default Value:

Yes. (Windows Firewall with Advanced Security will display a notification when a program is blocked from receiving inbound connections.)

References:

1. <https://learn.microsoft.com/en-us/windows/client-management/mdm/firewall-csp>

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. | | ● | ● |

35.7 (L1) Ensure 'Enable Public Network Firewall' is set to 'True' (Automated)

Profile Applicability:

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

Description:

Select True (recommended) to have Windows Firewall with Advanced Security use the settings for this profile to filter network traffic. If you select False, 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: True (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 with a REG_DWORD value of 1.

```
HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy  
\Mdm\PublicProfile:EnableFirewall
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to True (recommended) :

```
Firewall\Enable Public Network Firewall
```

Default Value:

On (recommended). (The Windows Firewall with Advanced Security will be active in this profile.)

References:

1. <https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/best-practices-configuring>
2. <https://learn.microsoft.com/en-us/windows/client-management/mdm/firewall-csp>

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | <p>4.5 <u>Implement and Manage a Firewall on End-User Devices</u></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 <u>Apply Host-based Firewalls or Port Filtering</u></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> | ● | ● | ● |

35.8 (L1) Ensure 'Enable Public Network Firewall: Allow Local Ipsec Policy Merge' is set to 'False' (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: False.

Rationale:

Users with administrative privileges might create firewall rules that expose the system to remote attack.

Impact:

Administrators can still create local connection security rules, but the rules will not be applied.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a REG_DWORD value of 0.

HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy
\Mdm\PublicProfile:AllowLocalIPsecPolicyMerge

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to False:

Firewall\Enable Public Network Firewall: Allow Local Ipsec Policy Merge

Default Value:

Yes (default). (Local connection security rules created by administrators will be applied.)

References:

1. <https://learn.microsoft.com/en-us/windows/client-management/mdm/firewall-csp>

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> | | ● | ● |

35.9 (L1) Ensure 'Enable Public Network Firewall: Allow Local Policy Merge' is set to 'False' (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: False.

Note: When the Allow Local Policy Merge setting is configured to False, it's recommended to also configure the Disable Inbound Notifications setting to True. Otherwise, users will continue to receive messages that ask if they want to unblock a restricted inbound connection, but the user's response will be ignored.

Rationale:

When in the Public profile, there should be no special local firewall exceptions per computer. These settings should be managed by a centralized policy.

Impact:

Administrators can still create firewall rules, but the rules will not be applied.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a REG_DWORD value of 0.

```
HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy  
\Mdm\PublicProfile:AllowLocalPolicyMerge
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to False:

```
Firewall\Enable Public Network Firewall: Allow Local Policy Merge
```

Default Value:

Yes (default). (Firewall rules created by administrators will be applied.)

References:

1. <https://learn.microsoft.com/en-us/windows/client-management/mdm/firewall-csp>

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>11.3 Use Automated Tools to Verify Standard Device Configurations and Detect Changes</p> <p>Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviations are discovered.</p> | | ● | ● |

35.10 (L1) Ensure 'Enable Public Network Firewall: Default Inbound Action for Public Profile' is set to 'Block' (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.

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 with a REG_DWORD value of 1.

```
HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy  
\Mdm\PublicProfile:DefaultInboundAction
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Block:

```
Firewall\Enable Public Network Firewall: Default Inbound Action for Public  
Profile
```

Default Value:

Block (default). (The Windows Firewall with Advanced Security will block all inbound connections that do not match an inbound firewall rule in this profile.)

References:

1. <https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/best-practices-configuring>
2. <https://learn.microsoft.com/en-us/windows/client-management/mdm/firewall-csp>

CIS Controls:

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

35.11 (L1) Ensure 'Enable Public Network Firewall: Disable Inbound Notifications' is set to 'True' (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: True.

Rationale:

Some organizations may prefer to avoid alarming users when firewall rules block certain types of network activity. However, notifications can be helpful when troubleshooting network issues involving the firewall.

Impact:

Windows Firewall will not display a notification when a program is blocked from receiving inbound connections.

Audit:

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

HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy
\Mdm\PublicProfile:DisableNotifications

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to 'True':

Firewall\Enable Public Network Firewall: Disable Inbound Notifications

Default Value:

Yes. (Windows Firewall with Advanced Security will display a notification when a program is blocked from receiving inbound connections.)

References:

1. <https://learn.microsoft.com/en-us/windows/client-management/mdm/firewall-csp>

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> | | ● | ● |

36 FSLogix

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

37 Games

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

38 Handwriting

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

39 Human Presence

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

40 Kerberos

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

41 Kiosk Browser

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

42 Lanman Workstation

This section contains recommendations for Lanman Workstation.

42.1 (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 with a REG_DWORD value of 0.

HKLM\SOFTWARE\Policies\Microsoft\Windows\LanmanWorkstation:AllowInsecureGuestAuth

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to **Disabled**:

Lanman Workstation\Enable insecure guest logons

Default Value:

Windows 10 R1703 or older: Enabled. (The SMB client will allow insecure guest logons.)

Windows 10 R1709 or newer: Disabled. (The SMB client will reject insecure guest logons.)

References:

1. <https://learn.microsoft.com/en-us/troubleshoot/windows-server/networking/guest-access-in-smb2-is-disabled-by-default>

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| 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. | ● | ● | |

43 Licensing

This section contains recommendations for Licensing.

43.1 (L2) Ensure 'Disallow KMS Client Online AVS Validation' is set to 'Allow' (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: Allow.

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:

1. Navigate to the following registry location and note the *WinningProvider* GUID. This value confirms under which User GUID the policy is set.

```
HKLM\SOFTWARE\Microsoft\PolicyManager\current\device\Licensing:DisallowKMSClientOnlineAVSValidation_WinningProvider
```

2. Navigate to the following registry location and confirm the value is set to 1.

```
HKLM\SOFTWARE\Microsoft\PolicyManager\Providers\{GUID}\Default\Device\Licensing:DisallowKMSClientOnlineAVSValidation
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Allow`:

```
Licensing\Disallow KMS Client Online AVS Validation
```

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 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| 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. | | ● | ● |

44 List Sync

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

45 Local Policies Security Options

This section contains recommendations for Local Policies Security Options.

45.1 (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 with a REG_DWORD value of 3.

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System>NoConnectedUser

Remediation:

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

Local Policies Security Options\Accounts: Block Microsoft accounts

Default Value:

Users are able to use Microsoft accounts with Windows.

References:

1. <https://learn.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 |
|------------------|---|------|------|------|
| 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. | | ● | ● |

45.2 (L1) Ensure 'Accounts: Enable 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 configuration profiles, set the following Settings Catalog path to **Disabled**:

Local Policies Security Options\Accounts: Guest account status

Default Value:

Disabled.

References:

1. <https://learn.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. | ● | ● | ● |

45.3 (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 with a REG_DWORD value of 1.

HKLM\SYSTEM\CurrentControlSet\Control\Lsa:LimitBlankPasswordUse

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled:

Local Policies Security Options\Accounts: Limit local account use of blank passwords to console logon only

Default Value:

Enabled.

References:

1. <https://learn.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. | | ● | ● |

45.4 (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 configuration profiles, set the following Settings Catalog path:

Local Policies Security Options\Accounts: Rename administrator account

Default Value:

Administrator.

References:

1. <https://learn.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 | 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. | ● | ● | ● |

45.5 (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 configuration profiles, set the following Settings Catalog path:

Local Policies Security Options\Accounts: Rename guest account

Default Value:

Guest.

References:

1. <https://learn.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>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> | ● | ● | ● |

45.6 (L2) Ensure 'Devices: Prevent users from installing printer drivers when connecting to shared printers' is set to 'Enable' (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: Enable.

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 with a REG_DWORD value of 1.

| |
|---|
| HKLM\SYSTEM\CurrentControlSet\Control\Print\Providers\LanMan Print Services\Servers:AddPrinterDrivers |
|---|

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Enable`:

Local Policies Security Options\Devices: Prevent users from installing printer drivers when connecting to shared printers

Default Value:

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

References:

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

CIS Controls:

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

45.7 (L1) Ensure 'Interactive logon: Do not 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.

Warning: If the [Self Service Password Reset \(SSPR\)](#) feature is used in Microsoft Entra ID, an exception to this recommendation is needed as it's known to interfere with SSPR.

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 with a REG_DWORD value of 1.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:DontDisplayLastUserName
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled:

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

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. | ● | ● | ● |
| v7 | 5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software. | ● | ● | ● |

45.8 (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 with a REG_DWORD value of `0`.

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:DisableCAD

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to **Disabled**:

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

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| v7 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |

45.9 (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 with a REG_DWORD value of 900 or less, but not 0.

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:InactivityTimeoutSecs

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to 900 or fewer seconds, but not 0:

Local Policies Security Options\Interactive logon: Machine inactivity limit

Default Value:

0 seconds. (There is no inactivity limit.)

References:

1. <https://learn.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 | 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. | ● | ● | ● |

45.10 (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.

Warning: [Windows Autopilot - Policy Conflicts](#): Windows Autopilot pre-provisioning doesn't work when this GPO policy settings is enabled. An exception to this recommendation will be needed if Windows AutoPilot is used.

Audit:

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

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:LegalNoticeText

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to a value that is consistent with the security and operational requirements of your organization:

Local Policies Security Options\Interactive logon: Message text for users attempting to log on

Default Value:

No message.

References:

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

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| v7 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |

45.11 (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.

Warning: [Windows Autopilot - Policy Conflicts](#): Windows Autopilot pre-provisioning doesn't work when this GPO policy settings is enabled. An exception to this recommendation will be needed if Windows AutoPilot is used.

Audit:

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

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:LegalNoticeCaption

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to a value that is consistent with the security and operational requirements of your organization:

Local Policies Security Options\Interactive logon: Message title for users attempting to log on

Default Value:

No message.

References:

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

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| v7 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |

45.12 (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. This group policy setting is backed by the following registry location with a REG_SZ value of 1, 2 or 3.

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon:ScRemoveOption

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Lock Workstation (or, if applicable for your environment, Force Logoff or Disconnect if a Remote Desktop Services session):

Local Policies Security Options\Interactive logon: Smart card removal behavior

Default Value:

No action.

References:

1. <https://learn.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. | ● | ● | ● |

45.13 (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 with a REG_DWORD value of 1.

```
HKLM\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters:RequireSecuritySignature
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled:

```
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://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/microsoft-network-client-digital-sign-communications-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). | ● | ● | ● |

45.14 (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 with a REG_DWORD value of 1.

```
HKLM\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters:EnableSecuritySignature
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled:

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

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). | | ● | ● |

45.15 (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 with a REG_DWORD value of 0.

```
HKLM\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters:EnablePlainTextPassword
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

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://learn.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. | | ● | ● |

45.16 (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 with a REG_DWORD value of 1.

```
HKLM\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters:RequireSecuritySignature
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled:

```
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://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/microsoft-network-server-digital-sign-communications-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). | ● | ● | ● |

45.17 (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 with a REG_DWORD value of 1.

```
HKLM\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters:EnableSecurity  
Signature
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled:

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

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). | ● | ● | ● |

45.18 (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 with a REG_DWORD value of 1.

HKLM\SYSTEM\CurrentControlSet\Control\Lsa:RestrictAnonymousSAM

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled:

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

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| v7 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |

45.19 (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 with a REG_DWORD value of 1.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa:RestrictAnonymous

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled:

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

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| v7 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |

45.20 (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

`HKLM\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters`

registry key. This registry value toggles null session shares on or off to control whether the server service restricts unauthenticated clients' access to named resources.

The recommended state for this setting is: Enabled.

Rationale:

Null sessions are a weakness that can be exploited through shares (including the default shares) on computers in your environment.

Impact:

None - this is the default behavior. If you choose to enable this setting and are supporting Windows NT 4.0 domains, you should check if any of the named pipes are required to maintain trust relationships between the domains, and then add the pipe to the **Network access: Named pipes that can be accessed anonymously** list:

- COMNAP: SNA session access
- COMNODE: SNA session access
- SQL\QUERY: SQL instance access
- SPOOLSS: Spooler service
- LLSRPC: License Logging service
- NETLOGON: Net Logon service
- LSARPC: LSA access
- SAMR: Remote access to SAM objects
- BROWSER: Computer Browser service

Previous to the release of Windows Server 2003 with Service Pack 1 (SP1) these named pipes were allowed anonymous access by default, but with the increased hardening in Windows Server 2003 with SP1 these pipes must be explicitly added if needed.

Audit:

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

```
HKLM\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters:RestrictNullSe  
ssAccess
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled:

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

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| v7 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |

45.21 (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: This setting was originally only supported on Windows 10 R1607 or newer, then support for it was added to Windows 7 or newer via the March 2017 security patches.

Note #3: If your organization is using Microsoft Defender for Identity (formerly Azure Advanced Threat Protection (Azure ATP)), the (organization-named) Defender for Identity Directory Service Account (DSA), will also need to be granted the same Remote Access: Allow permission. For more information on adding the service account please see [Configure SAM-R to enable lateral movement path detection in Microsoft Defender for Identity | Microsoft Docs](#).

Rationale:

To ensure that an unauthorized user cannot anonymously list local account names or groups and use the information to attempt to guess passwords or perform social engineering attacks. (Social engineering attacks try to deceive users in some way to obtain passwords or some form of security information.)

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a REG_SZ value of O:BAG:BAD:(A;;RC;;;BA).

HKLM\SYSTEM\CurrentControlSet\Control\Lsa:restrictremotesam

O:BAG:BAD:(A;;RC;;;BA)

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Administrators: Remote Access: Allow:

Local Policies Security Options\Network access: Restrict clients allowed to make remote calls to SAM

Default Value:

Administrators: Remote Access: Allow.

References:

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

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| v7 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |

45.22 (L1) Ensure 'Network security: Allow Local System to use computer identity for NTLM' is set to 'Allow' (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: Allow.

Rationale:

When connecting to computers running versions of Windows earlier than Windows Vista or Windows Server 2008 (non-R2), services running as Local System and using SPNEGO (Negotiate) that revert to NTLM use the computer identity. In Windows 7, if you are connecting to a computer running Windows Server 2008 or Windows Vista, then a system service uses either the computer identity or a NULL session. When connecting with a NULL session, a system-generated session key is created, which provides no protection but allows applications to sign and encrypt data without errors. When connecting with the computer identity, both signing and encryption is supported in order to provide data protection.

Impact:

Services running as Local System that use Negotiate when reverting to NTLM authentication will use the computer identity. This might cause some authentication requests between Windows operating systems to fail and log an error.

Audit:

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

| |
|--|
| HKLM\SYSTEM\CurrentControlSet\Control\Lsa:UseMachineId |
|--|

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Allow:

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

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| v7 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |

45.23 (L1) Ensure 'Network Security: Allow PKU2U authentication requests' is set to 'Block' (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: Block.

Rationale:

The PKU2U protocol is a peer-to-peer authentication protocol - authentication should be managed centrally in most managed networks.

Impact:

None - this is the default configuration for domain-joined computers.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a REG_DWORD value of 0.

```
HKLM\SYSTEM\CurrentControlSet\Control\Lsa\pku2u:AllowOnlineID
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Block:

```
Local Policies Security Options\Network Security: Allow PKU2U authentication requests to this computer
```

Default Value:

Disabled. (Online identities will not be allowed to authenticate to a domain-joined machine.)

References:

1. <https://learn.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 |
|------------------|---|------|------|------|
| v8 | 4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. | ● | ● | ● |
| 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. | ● | ● | ● |

45.24 (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 with a REG_DWORD value of 1.

HKLM\SYSTEM\CurrentControlSet\Control\Lsa>NoLMHash

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled:

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://learn.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. | ● | ● | |

45.25 (L1) Ensure 'Network security: LAN Manager authentication level' is set to 'Send LM and NTLMv2 responses only. Refuse LM and 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 LM and NTLMv2 responses only.

Refuse LM and 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 with a REG_DWORD value of 5.

HKLM\SYSTEM\CurrentControlSet\Control\Lsa:LmCompatibilityLevel

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to: Send LM and NTLMv2 responses only. Refuse LM and NTLM:

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://learn.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. | | ● | ● |

45.26 (L1) Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' is set to 'Require NTLM and 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 with a REG_DWORD value of 537395200.

HKLM\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0:NTLMMinClientSec

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Require NTLMv2 session security, Require 128-bit encryption:

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://learn.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. | | ● | ● |

45.27 (L1) Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require NTLM and 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 with a REG_DWORD value of 537395200.

HKLM\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0:NTLMMinServerSec

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Require NTLMv2 session security, Require 128-bit encryption:

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://learn.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. | | ● | ● |

45.28 (L1) Ensure 'Network security: Restrict NTLM: Audit Incoming NTLM Traffic' is set to 'Enable auditing for all accounts' (Automated)

Profile Applicability:

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

Description:

This policy setting allows the auditing of incoming NTLM traffic. Events for this setting are recorded in the operational event log (e.g. Applications and Services Log\Microsoft\Windows\NTLM).

The recommended state for this setting is: Enable auditing for all accounts.

Rationale:

Auditing and monitoring NTLM traffic can assist in identifying systems using this outdated authentication protocol, so they can be remediated to using a more secure protocol, such as Kerberos. The log information gathered can also assist in forensic investigations after a malicious attack.

NTLM and NTLMv2 authentication is vulnerable to various attacks, including SMB relay, man-in-the-middle, and brute force attacks. Reducing and eliminating NTLM authentication in an environment reduces the risk of an attacker gaining access to systems on the network.

Impact:

The event log will contain information on incoming NTLM authentication traffic.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a REG_DWORD value of 2.

HKLM\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0:AuditReceivingNTLMTraffic

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Enable auditing for all accounts`:

```
Local Policies Security Options\Network security: Restrict NTLM: Audit  
Incoming NTLM Traffic
```

Default Value:

Disabled. (Incoming NTLM traffic is not logged.)

References:

1. <https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-restrict-ntlm-audit-incoming-ntlm-traffic>
2. <https://learn.microsoft.com/en-us/defender-for-identity/configure-windows-event-collection#event-id-8004>

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. | | ● | ● |

45.29 (L1) Ensure 'User Account Control: Behavior of the elevation prompt for administrators' is set to 'Prompt for consent on the secure desktop' or higher (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. Configuring this setting to Prompt for credentials on the secure desktop also conforms to the benchmark.

Rationale:

One of the risks that the UAC feature introduced with Windows Vista is trying to mitigate is that of malicious software running under elevated credentials without the user or administrator being aware of its activity. This setting raises awareness to the administrator of elevated privilege operations and permits the administrator to prevent a malicious program from elevating its privilege when the program attempts to do so.

Impact:

When an operation (including execution of a Windows binary) requires elevation of privilege, the user is prompted on the secure desktop to select either Permit or Deny. If the user selects Permit, the operation continues with the user's highest available privilege.

Warning: [Windows Autopilot - Policy Conflicts](#): This policy requires a reboot to apply. As a result, prompts may appear when modifying user account control (UAC) settings during the Out of the Box Experience (OOBE) using the device Enrollment Status Page (ESP). Increased prompts are more likely if the device reboots after policies are applied. To work around this issue, the policies can be targeted to users instead of devices so that they apply later in the process. An exception to this recommendation may be needed if Windows AutoPilot is used.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a REG_DWORD value of 1 or 2.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:ConsentPromptBehaviorAdmin
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Prompt for consent on the secure desktop or Prompt for credentials on the secure desktop:

```
Local Policies Security Options\User Account Control: Behavior of the elevation prompt for administrators
```

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://learn.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>

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| v7 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |

45.30 (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.

Note #2: When using third-party remote support tools, this recommendation could prevent Administrators from entering their administrative credentials. In this case, an exception to this recommendation will be needed.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a REG_DWORD value of 0.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:ConsentPromptBehaviorUser
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Automatically deny elevation requests:

```
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://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/user-account-control-behavior-of-the-elevation-prompt-for-standard-users>

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| v7 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |

45.31 (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 with a REG_DWORD value of 1.

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

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled:

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

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| v7 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |

45.32 (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 with a REG_DWORD value of 1.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:EnableSecureUIAPaths
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled:

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

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| v7 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |

45.33 (L1) Ensure 'User Account Control: Use 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 Admin Approval Mode for the built-in Administrator account.

The recommended state for this setting is: Enabled.

Rationale:

One of the risks that the User Account Control feature introduced with Windows Vista is trying to mitigate is that of malicious software running under elevated credentials without the user or administrator being aware of its activity. An attack vector for these programs was to discover the password of the account named "Administrator" because that user account was created for all installations of Windows. To address this risk, in Windows Vista or newer, the built-in Administrator account is now disabled by default. In a default installation of a new computer, accounts with administrative control over the computer are initially set up in one of two ways:

- If the computer is not joined to a domain, the first user account you create has the equivalent permissions as a local administrator.
- If the computer is joined to a domain, no local administrator accounts are created. The Enterprise or Domain Administrator must log on to the computer and create one if a local administrator account is warranted.

Once Windows is installed, the built-in Administrator account may be manually enabled, but we strongly recommend that this account remain disabled.

Impact:

The built-in Administrator account uses Admin Approval Mode. Users that log on using the local Administrator account will be prompted for consent whenever a program requests an elevation in privilege, just like any other user would.

Audit:

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

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:FilterAdministratorToken
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled:

```
Local Policies Security Options\User Account Control: Use Admin Approval Mode
```

Default Value:

Disabled. (The built-in Administrator account runs all applications with full administrative privilege.)

References:

1. <https://learn.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 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| v7 | 4.4 <u>Use Unique Passwords</u> 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. | | ● | ● |

45.34 (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 with a REG_DWORD value of 1.

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

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled:

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

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| v7 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |

45.35 (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 with a REG_DWORD value of 1.

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:EnableLUA

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled:

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://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/user-account-control-run-all-administrators-in-admin-approval-mode>

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| v7 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |

45.36 (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
- HKLM\SOFTWARE

The recommended state for this setting is: Enabled.

Rationale:

This setting reduces vulnerabilities by ensuring that legacy applications only write data to permitted locations.

Impact:

None - this is the default behavior.

Audit:

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

| |
|---|
| HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:EnableVirtualization |
|---|

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled:

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

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| v7 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |

46 Lock Down

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

47 Memory Dump

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

48 Microsoft App Store

This section contains recommendations for Microsoft App Store.

48.1 (L1) Ensure 'Allow apps from the Microsoft app store to auto update' is set to 'Allowed' (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: Allowed.

Rationale:

Keeping your system properly patched can help protect against 0 day vulnerabilities.

Impact:

None - this is the default behavior.

Audit:

1. Navigate to the following registry location and note the *WinningProvider* GUID. This value confirms under which User GUID the policy is set.

```
HKLM\SOFTWARE\Microsoft\PolicyManager\current\device\ApplicationManagement:AllowAppStoreAutoUpdate_WinningProvider
```

2. Navigate to the following registry location and confirm the value is set to 1.

```
HKLM\SOFTWARE\Microsoft\PolicyManager\Providers\{GUID}\Default\Device\ApplicationManagement:AllowAppStoreAutoUpdate
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Allowed:

```
Microsoft App Store\Allow apps from the Microsoft app store to auto update
```

Default Value:

2

References:

1. https://learn.microsoft.com/en-us/windows/client-management/mdm/policy-csp-ApplicationManagement?WT.mc_id=Portal-fx#allowappstoreautoupdate

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>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.</p> | | ● | ● |

48.2 (L1) Ensure 'Allow Game DVR' is set to 'Block' (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: Block.

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:

1. Navigate to the following registry location and note the *WinningProvider* GUID. This value confirms under which User GUID the policy is set.

```
HKLM\SOFTWARE\Microsoft\PolicyManager\current\device\ApplicationManagement:AllowGameDVR_WinningProvider
```

2. Navigate to the following registry location and confirm the value is set to 0.

```
HKLM\SOFTWARE\Microsoft\PolicyManager\Providers\{GUID}\Default\Device\ApplicationManagement:AllowGameDVR
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Block:

```
Microsoft App Store\Allow Game DVR
```

Default Value:

Enabled. (Recording and Broadcasting (streaming) is 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> | ● | ● | ● |

48.3 (L2) Ensure 'Disable Store Originated Apps' is set to 'Enabled' (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: Enabled.

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:

1. Navigate to the following registry location and note the *WinningProvider* GUID.
This value confirms under which User GUID the policy is set.

```
HKLM\SOFTWARE\Microsoft\PolicyManager\current\device\ApplicationManagement:DisableStoreOriginatedApps_WinningProvider
```

2. Navigate to the following registry location and confirm the value is set to 0.

```
HKLM\SOFTWARE\Microsoft\PolicyManager\Providers\{GUID}\Default\Device\ApplicationManagement:DisableStoreOriginatedApps
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled:

```
Microsoft App Store\Disable Store Originated Apps
```

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. | | ● | ● |

48.4 (L1) Ensure 'MSI 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 with a REG_DWORD value of 0.

| |
|--|
| HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer:EnableUserControl |
|--|

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft App Store\MSI Allow user control over installs
```

Default Value:

`Disabled`. (The security features of Windows Installer will prevent users from changing installation options typically reserved for system administrators, such as specifying the directory to which files are installed.)

References:

1. <https://learn.microsoft.com/en-us/windows/win32/msi/windows-installer-portal>

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| v7 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |

48.5 (L1) Ensure 'MSI 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 with a REG_DWORD value of 0.

HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer:AlwaysInstallElevated

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft App Store\MSI Always install with elevated privileges
```

Default Value:

Disabled. (Windows Installer will apply the current user's permissions when it installs programs that a system administrator does not distribute or offer. This will prevent standard users from installing applications that affect system-wide configuration items.)

References:

1. <https://learn.microsoft.com/en-us/windows/win32/msi/using-windows-installer-with-uac>

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| 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. | ● | ● | ● |

48.6 (L1) Ensure 'MSI Always install with elevated privileges (User)' 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 with a REG_DWORD value of 0.

```
HKU\[USER  
SID]\Software\Policies\Microsoft\Windows\Installer:AlwaysInstallElevated
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`:

Microsoft App Store\MSI Always install with elevated privileges (User)

Default Value:

Disabled. (Windows Installer will apply the current user's permissions when it installs programs that a system administrator does not distribute or offer. This will prevent standard users from installing applications that affect system-wide configuration items.)

References:

1. <https://learn.microsoft.com/en-us/windows/win32/msi/alwaysinstallelevated>

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| 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. | ● | ● | ● |

48.7 (L1) Ensure 'Require Private Store Only' is set to 'Only Private store is 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: Only Private store 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 with a REG_DWORD value of 1.

HKLM\SOFTWARE\Policies\Microsoft\WindowsStore:RequirePrivateStoreOnly

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Only Private store is enabled:

Microsoft App Store\Require Private Store Only

Default Value:

Disabled. (Users can access the retail catalog in the Microsoft Store.)

References:

1. <https://learn.microsoft.com/en-us/microsoft-store/manage-access-to-private-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. | ● | ● | |

49 Microsoft Defender for Endpoint

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

50 Mixed Reality

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

51 Network Isolation

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

52 Network List Manager

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

53 News and interests

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

54 Notifications

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

55 PDE

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

56 Power

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

57 Printer Provisioning

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

58 Privacy

This section contains recommendations for Privacy.

58.1 (L2) Ensure 'Allow Cross Device Clipboard' is set to 'Block' (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: Block.

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:

1. Navigate to the following registry location and note the *WinningProvider* GUID. This value confirms under which User GUID the policy is set.

```
HKLM\SOFTWARE\Microsoft\PolicyManager\current\device\Privacy:AllowCrossDeviceClipboard_WinningProvider
```

2. Navigate to the following registry location and confirm the value is set to 0.

```
HKLM\SOFTWARE\Microsoft\PolicyManager\Providers\{GUID}\Default\Device\Privacy:AllowCrossDeviceClipboard
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Block:

```
Privacy\Allow Cross Device Clipboard
```

Default Value:

Enabled. (Clipboard contents are allowed to be synchronized across devices logged in under the same Microsoft account or Azure AD account.)

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> | | ● | ● |

58.2 (L1) Ensure 'Allow Input Personalization' is set to 'Block' (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: Block.

Rationale:

If this setting is Enabled sensitive information could be stored in the cloud or sent to Microsoft.

Impact:

Automatic learning of speech, inking, and typing stops and users cannot change its value via PC Settings.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a REG_DWORD value of 0.

```
HKLM\SOFTWARE\Policies\Microsoft\InputPersonalization:AllowInputPersonalization
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Block:

```
Privacy\Allow Input Personalization
```

Default Value:

Enabled. (Automatic learning of speech, inking and typing is enabled, but users may change this value via PC Settings.)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|------|------|------|
| v8 | <p>4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.</p> | ● | ● | ● |
| v7 | <p>5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.</p> | ● | ● | ● |

58.3 (L2) Ensure 'Disable 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 with a REG_DWORD value of 1.

HKLM\SOFTWARE\Policies\Microsoft\Windows\AdvertisingInfo:DisabledByGroupPolicy

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled:

Privacy\Disable Advertising ID

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 |
|------------------|---|------|------|------|
| 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> | ● | ● | ● |

58.4 (L1) Ensure 'Let Apps Activate With Voice Above Lock' 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:

1. Navigate to the following registry location and note the *WinningProvider* GUID. This value confirms under which User GUID the policy is set.

```
HKLM\SOFTWARE\Microsoft\PolicyManager\current\device\Privacy:LetAppsActivateWithVoiceAboveLock_WinningProvider
```

2. Navigate to the following registry location and confirm the value is set to 2.

```
HKLM\SOFTWARE\Microsoft\PolicyManager\Providers\{GUID}\Default\Device\Privacy:LetAppsActivateWithVoiceAboveLock
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled: Force Deny:

```
Privacy\Let Apps Activate With Voice Above Lock
```

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 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| 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. | | ● | ● |

58.5 (L2) Ensure 'Upload 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 third-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:

1. Navigate to the following registry location and note the *WinningProvider* GUID. This value confirms under which User GUID the policy is set.

```
HKLM\SOFTWARE\Microsoft\PolicyManager\current\device\Privacy:UploadUserActivities_WinningProvider
```

2. Navigate to the following registry location and confirm the value is set to 0.

```
HKLM\SOFTWARE\Microsoft\PolicyManager\Providers\{GUID}\Default\Device\Privacy:UploadUserActivities
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to **Disabled**:

```
Privacy\Upload User Activities
```

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 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| 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. | | ● | ● |

59 Remote Desktop

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

60 Search

This section contains recommendations for Search.

60.1 (L2) Ensure 'Allow Cloud Search' is set to 'Not allowed' (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: Not allowed.

Rationale:

Due to privacy concerns, data should never be sent to any third-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:

1. Navigate to the following registry location and note the *WinningProvider* GUID. This value confirms under which User GUID the policy is set.

```
HKLM\SOFTWARE\Microsoft\PolicyManager\current\device\Search:AllowCloudSearch_WinningProvider
```

2. Navigate to the following registry location and confirm the value is set to 0.

```
HKLM\SOFTWARE\Microsoft\PolicyManager\Providers\{GUID}\Default\Device\Search:AllowCloudSearch
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Not allowed:

```
Search\Allow Cloud Search
```

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 <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> | ● | ● | ● |

60.2 (L1) Ensure 'Allow Indexing Encrypted Stores Or Items' is set to 'Block' (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: Block.

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:

1. Navigate to the following registry location and note the *WinningProvider* GUID. This value confirms under which User GUID the policy is set.

```
HKLM\SOFTWARE\Microsoft\PolicyManager\current\device\Search:AllowIndexingEncryptedStoresOrItems_WinningProvider
```

2. Navigate to the following registry location and confirm the value is set to 0.

```
HKLM\SOFTWARE\Microsoft\PolicyManager\Providers\{GUID}\Default\Device\Search:AllowIndexingEncryptedStoresOrItems
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Block:

```
Search\Allow Indexing Encrypted Stores Or Items
```

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 |
|------------------|---|------|------|------|
| v8 | 4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. | | ● | ● |
| v7 | 14.8 Encrypt Sensitive Information at Rest Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information. | | | ● |

60.3 (L1) Ensure 'Allow Search To Use Location' is set to 'Block' (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: Block.

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:

1. Navigate to the following registry location and note the *WinningProvider* GUID. This value confirms under which User GUID the policy is set.

```
HKLM\SOFTWARE\Microsoft\PolicyManager\current\device\Search:AllowSearchToUseLocation_WinningProvider
```

2. Navigate to the following registry location and confirm the value is set to 0.

```
HKLM\SOFTWARE\Microsoft\PolicyManager\Providers\{GUID}\Default\Device\Search:AllowSearchToUseLocation
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Block:

```
Search\Allow search to use location
```

Default Value:

Enabled. (Search and Cortana can access location information.)

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> | ● | ● | ● |

61 Security

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

62 Settings

This section contains recommendations for Settings.

62.1 (L2) Ensure 'Allow Online Tips' is set to 'Block' (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: Block.

Rationale:

Due to privacy concerns, data should never be sent to any third-party since this data could contain sensitive information.

Impact:

Settings will not contact Microsoft content services to retrieve tips and help content.

Audit:

1. Navigate to the following registry location and note the *WinningProvider* GUID. This value confirms under which User GUID the policy is set.

```
HKLM\SOFTWARE\Microsoft\PolicyManager\current\device\Settings:AllowOnlineTips  
_WinningProvider
```

2. Navigate to the following registry location and confirm the value is set to 0.

```
HKLM\SOFTWARE\Microsoft\PolicyManager\Providers\{GUID}\Default\Device\Settings:AllowOnlineTips
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Block.

```
Settings\Allow Online Tips
```

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 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| 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. | | ● | ● |

63 Shared PC

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

64 Smart Screen

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

65 Speech

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

66 Storage

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

67 System

This section contains recommendations for System.

67.1 (L1) Ensure 'Allow Telemetry' is set to 'Basic' (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:

The recommended state for this setting is: Basic or Security.

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 third-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 with a REG_DWORD value of 0 or 1.

| |
|---|
| HKLM\Software\Policies\Microsoft\Windows\DataCollection:AllowTelemetry_Policy Manager |
|---|

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Basic or Security:

System\Allow Telemetry

Default Value:

Basic. (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://learn.microsoft.com/en-us/windows/privacy/configure-windows-diagnostic-data-in-your-organization>
2. https://learn.microsoft.com/en-us/windows/client-management/mdm/policy-csp-System?WT.mc_id=Portal-fx#allowtelemetry

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| 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. | | ● | ● |

67.2 (L2) Ensure 'Allow Font Providers' is set to 'Not allowed' (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: Not allowed.

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:

1. Navigate to the following registry location and note the *WinningProvider* GUID. This value confirms under which User GUID the policy is set.

```
HKLM\SOFTWARE\Microsoft\PolicyManager\current\device\System:AllowFontProvider  
s_WinningProvider
```

2. Navigate to the following registry location and confirm the value is set to 0.

```
HKLM\SOFTWARE\Microsoft\PolicyManager\Providers\{GUID}\Default\Device\System:  
AllowFontProviders
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Not allowed:

```
System\Allow Font Providers
```

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 | <p>16.5 <u>Use Up-to-Date and Trusted Third-Party Software Components</u></p> <p>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.</p> | | ● | ● |
| v7 | <p>18.4 <u>Only Use Up-to-date And Trusted Third-Party Components</u></p> <p>Only use up-to-date and trusted third-party components for the software developed by the organization.</p> | | ● | ● |

67.3 (L2) Ensure 'Disable One Drive File Sync' is set to 'Sync Disabled' (Automated)

Profile Applicability:

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

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: Sync Disabled.

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 Microsoft 365, be aware that this setting will prevent users from saving files to OneDrive/SkyDrive.

- *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 with a REG_DWORD value of 1.

HKLM\SOFTWARE\Policies\Microsoft\Windows\OneDrive:DisableFileSyncNGSC

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Sync Disabled:

System\Disable One Drive File Sync

Default Value:

Disabled. (Apps and features can work with OneDrive file storage using the Next Generation Sync Client.)

References:

1. <https://learn.microsoft.com/en-us/office365/servicedescriptions/onedrive-for-business-service-description>

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>13.4 Only Allow Access to Authorized Cloud Storage or Email Providers</u> Only allow access to authorized cloud storage or email providers. | ● | | ● |

68 Task Manager

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

69 System Services

This section contains recommendations for System Services.

69.1 (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 with a REG_DWORD value of 4.

```
HKLM\SYSTEM\CurrentControlSet\Services\BTAGService:Start
```

Remediation:

Remediation of this service is currently not possible through Settings Catalog or a custom profile OMA-URI. Instead, it can be scripted and deployed through the Intune Scripts or Remediations blade or by other means.

To establish the recommended configuration via PowerShell, run the following cmdlet:

```
Set-Service -Name BTAGService -StartupType Disabled
```

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> | ● | ● | ● |

69.2 (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 with a REG_DWORD value of 4.

```
HKLM\SYSTEM\CurrentControlSet\Services\bthserv:Start
```

Remediation:

Remediation of this service is currently not possible through Settings Catalog or a custom profile OMA-URI. Instead, it can be scripted and deployed through the Intune Scripts or Remediations blade or by other means.

To establish the recommended configuration via PowerShell, run the following cmdlet:

```
Set-Service -Name bthserv -StartupType Disabled
```

Default Value:

Windows 7: Manual

Windows 8.0 or 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. | | ● | ● |

69.3 (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 with a REG_DWORD value of 4 or that the key does not exist.

| |
|--|
| HKLM\SYSTEM\CurrentControlSet\Services\Browser:Start |
|--|

Remediation:

To establish the recommended configuration, set the following Custom Configuration Policy to 4 or confirm that the service is Not installed:

```
Name: <Enter name>
Description: <Enter Description>
OMA-URI:
./Device/Vendor/MSFT/Policy/Config/SystemServices/ConfigureComputerBrowserServiceStartupMode
Data Type: Integer
Value: 4
```

Note: As of January 2024, despite its inclusion in Microsoft's official documentation, using an OMI-URI to configure a Windows Service Startup Mode via a custom profile will lead to an error in Intune. This error will be logged in the local event log as "The system cannot find the file specified." Currently, the most reliable method for remediation is through PowerShell.

The recommended configuration can also be established via PowerShell, by running the following cmdlet:

```
if(Test-Path -LiteralPath "HKLM:\SYSTEM\CurrentControlSet\Services\Browser")
{
    Set-ItemProperty -LiteralPath
    'HKLM:\SYSTEM\CurrentControlSet\Services\Browser' -Name 'Start' -Value 4 -Verbose
}
```

Note: This service is not installed in Windows 10 R1709 and newer. Running the cmdlet `Set-Service -Name 'Browser' -StartupType Disabled` will cause a inadvertent match against a similarly named service called `bowser` which coincidentally has the `DisplayName` of `Browser` and will then throw an error. `bowser` is actually the `NT Lan Manager Datagram Receiver Driver`. Using the literal registry path above avoids that error.

Default Value:

Windows 7: Manual

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

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

References:

1. <https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/>
2. https://learn.microsoft.com/en-us/windows/client-management/mdm/policy-csp-SystemServices?WT.mc_id=Portal-Microsoft_Intune_Workflows#configurecomputerbrowserservicestartupmode

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> | ● | ● | ● |

69.4 (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 third-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 with a REG_DWORD value of 4.

```
HKLM\SYSTEM\CurrentControlSet\Services\MapsBroker:Start
```

Remediation:

Remediation of this service is currently not possible through Settings Catalog or a custom profile OMA-URI. Instead, it can be scripted and deployed through the Intune Scripts or Remediations blade or by other means.

To establish the recommended configuration via PowerShell, run the following cmdlet:

```
Set-Service -Name MapsBroker -StartupType Disabled
```

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. | ● | ● | ● |

69.5 (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 with a REG_DWORD value of 4.

```
HKLM\SYSTEM\CurrentControlSet\Services\lfsvc:Start
```

Remediation:

Remediation of this service is currently not possible through Settings Catalog or a custom profile OMA-URI. Instead, it can be scripted and deployed through the Intune Scripts or Remediations blade or by other means.

To establish the recommended configuration via PowerShell, run the following cmdlet:

```
Set-Service -Name lfsvc -StartupType Disabled
```

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> | ● | ● | ● |

69.6 (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 with a REG_DWORD value of 4 or that the key does not exist.

| |
|---|
| HKLM\SYSTEM\CurrentControlSet\Services\IISADMIN:Start |
|---|

Remediation:

To establish the recommended configuration, set the following Custom Configuration Policy to 4 or confirm that the service is Not installed:

```
Name: <Enter name>
Description: <Enter Description>
OMA-URI:
./Device/Vendor/MSFT/Policy/Config/SystemServices/ConfigureIISAdminServiceStartMode
Data Type: Integer
Value: 4
```

Note: As of January 2024, despite its inclusion in Microsoft's official documentation, using an OMI-URI to configure a Windows Service Startup Mode via a custom profile will lead to an error in Intune. This error will be logged in the local event log as "The system cannot find the file specified." Currently, the most reliable method for remediation is through PowerShell.

The recommended configuration can also be established via PowerShell by running the following cmdlet:

```
Set-Service -Name IISADMIN -StartupType Disabled
```

Default Value:

Not Installed (Automatic when installed)

References:

1. https://learn.microsoft.com/en-us/windows/client-management/mdm/policy-csp-SystemServices?WT.mc_id=Portal-Microsoft_Intune_Workflows#configureiisadminservicestartupmode

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. | | ● | ● |

69.7 (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 with a REG_DWORD value of 4 or that the key does not exist.

HKLM\SYSTEM\CurrentControlSet\Services\irmon:Start

Remediation:

To establish the recommended configuration, set the following Custom Configuration Policy to 4 or confirm that the service is Not installed:

```
Name: <Enter name>
Description: <Enter Description>
OMA-URI:
./Device/Vendor/MSFT/Policy/Config/SystemServices/ConfigureInfraredMonitorServiceStartupMode
Data Type: Integer
Value: 4
```

Note: As of January 2024, despite its inclusion in Microsoft's official documentation, using an OMI-URI to configure a Windows Service Startup Mode via a custom profile will lead to an error in Intune. This error will be logged in the local event log as "The system cannot find the file specified." Currently, the most reliable method for remediation is through PowerShell.

The recommended configuration can also be established via PowerShell by running the following cmdlet:

```
Set-Service -Name irmon -StartupType Disabled
```

Default Value:

Windows 10 R1607 through Windows 10 R1809: Manual

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

References:

1. https://learn.microsoft.com/en-us/windows/client-management/mdm/policy-csp-SystemServices?WT.mc_id=Portal-Microsoft_Intune_Workflows#configureinfraredmonitorservicestartupmode

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. | | ● | ● |

69.8 (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 with a REG_DWORD value of 4.

| |
|---|
| HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess:Start |
|---|

Remediation:

To establish the recommended configuration, set the following Custom Configuration Policy to 4:

```
Name: <Enter name>
Description: <Enter Description>
OMA-URI:
./Device/Vendor/MSFT/Policy/Config/SystemServices/ConfigureInternetConnectionSharingServiceStartupMode
Data Type: Integer
Value: 4
```

Note: As of January 2024, despite its inclusion in Microsoft's official documentation, using an OMI-URI to configure a Windows Service Startup Mode via a custom profile will lead to an error in Intune. This error will be logged in the local event log as "The system cannot find the file specified." Currently, the most reliable method for remediation is through PowerShell.

The recommended configuration can also be established via PowerShell by running the following cmdlet:

```
Set-Service -Name SharedAccess -StartupType Disabled
```

Default Value:

Windows 7 through Windows 8.1: Disabled

Windows 10 R1507 and R1511: Manual

Windows 10 R1607 or newer: Manual (Trigger Start)

References:

1. https://learn.microsoft.com/en-us/windows/client-management/mdm/policy-csp-SystemServices?WT.mc_id=Portal-Microsoft_Intune_Workflows#configureinternetconnectionsharingservicestartupmode

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> | ● | ● | ● |

69.9 (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 with a REG_DWORD value of 4.

```
HKLM\SYSTEM\CurrentControlSet\Services\lltdsvc:Start
```

Remediation:

Remediation of this service is currently not possible through Settings Catalog or a custom profile OMA-URI. Instead, it can be scripted and deployed through the Intune Scripts or Remediations blade or by other means.

To establish the recommended configuration via PowerShell, run the following cmdlet:

```
Set-Service -Name lltdsvc -StartupType Disabled
```

Default Value:

Manual

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> | ● | ● | ● |

69.10 (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 with a REG_DWORD value of 4 or that the key does not exist.

| |
|--|
| HKLM\SYSTEM\CurrentControlSet\Services\LxssManager:Start |
|--|

Remediation:

To establish the recommended configuration, set the following Custom Configuration Policy to 4 or confirm that the service is Not installed:

```
Name: <Enter name>
Description: <Enter Description>
OMA-URI:
./Device/Vendor/MSFT/Policy/Config/SystemServices/ConfigureLxssManagerService
StartupMode
Data Type: Integer
Value: 4
```

Note: As of January 2024, despite its inclusion in Microsoft's official documentation, using an OMI-URI to configure a Windows Service Startup Mode via a custom profile will lead to an error in Intune. This error will be logged in the local event log as "The system cannot find the file specified." Currently, the most reliable method for remediation is through PowerShell.

The recommended configuration can also be established via PowerShell by running the following cmdlet:

```
Set-Service -Name LxssManager -StartupType Disabled
```

Default Value:

Not Installed (Manual when installed)

References:

1. https://learn.microsoft.com/en-us/windows/client-management/mdm/policy-csp-SystemServices?WT.mc_id=Portal-Microsoft_Intune_Workflows#configurelxssmanagerservicestartupmode

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. | | ● | ● |

69.11 (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 with a REG_DWORD value of 4 or that the key does not exist.

HKLM\SYSTEM\CurrentControlSet\Services\FTPSVC:Start

Remediation:

To establish the recommended configuration, set the following Custom Configuration Policy to 4 or confirm that the service is Not installed:

```
Name: <Enter name>
Description: <Enter Description>
OMA-URI:
./Device/Vendor/MSFT/Policy/Config/SystemServices/ConfigureMicrosoftFTPServic
eStartupMode
Data Type: Integer
Value: 4
```

Note: As of January 2024, despite its inclusion in Microsoft's official documentation, using an OMI-URI to configure a Windows Service Startup Mode via a custom profile will lead to an error in Intune. This error will be logged in the local event log as "The system cannot find the file specified." Currently, the most reliable method for remediation is through PowerShell.

The recommended configuration can also be established via PowerShell by running the following cmdlet:

```
Set-Service -Name FTPSVC -StartupType Disabled
```

Default Value:

Not Installed (Automatic when installed)

References:

1. https://learn.microsoft.com/en-us/windows/client-management/mdm/policy-csp-SystemServices?WT.mc_id=Portal-Microsoft_Intune_Workflows#configuremicrosoftftpservicestartupmode

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. | | ● | ● |

69.12 (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 with a REG_DWORD value of 4.

```
HKLM\SYSTEM\CurrentControlSet\Services\MSiSCSI:Start
```

Remediation:

Remediation of this service is currently not possible through Settings Catalog or a custom profile OMA-URI. Instead, it can be scripted and deployed through the Intune Scripts or Remediations blade or by other means.

To establish the recommended configuration via PowerShell, run the following cmdlet:

```
Set-Service -Name MSiSCSI -StartupType Disabled
```

Default Value:

Manual

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> | ● | ● | ● |

69.13 (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 with a REG_DWORD value of 4 or that the key does not exist.

HKLM\SYSTEM\CurrentControlSet\Services\sshd:Start

Remediation:

Remediation of this service is currently not possible through Settings Catalog or a custom profile OMA-URI. Instead, it can be scripted and deployed through the Intune Scripts **or** Remediations blade or by other means.

To establish the recommended configuration via PowerShell, run the following cmdlet:

Set-Service -Name sshd -StartupType Disabled

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> | ● | ● | ● |

69.14 (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 with a REG_DWORD value of 4.

```
HKLM\SYSTEM\CurrentControlSet\Services\PNRPsvc:Start
```

Remediation:

Remediation of this service is currently not possible through Settings Catalog or a custom profile OMA-URI. Instead, it can be scripted and deployed through the Intune Scripts or Remediations blade or by other means.

To establish the recommended configuration via PowerShell, run the following cmdlet:

```
Set-Service -Name PNRPsvc -StartupType Disabled
```

Default Value:

Manual

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> | ● | ● | ● |

69.15 (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 with a REG_DWORD value of 4.

```
HKLM\SYSTEM\CurrentControlSet\Services\p2psvc:Start
```

Remediation:

Remediation of this service is currently not possible through Settings Catalog or a custom profile OMA-URI. Instead, it can be scripted and deployed through the Intune Scripts or Remediations blade or by other means.

To establish the recommended configuration via PowerShell, run the following cmdlet:

```
Set-Service -Name p2psvc -StartupType Disabled
```

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. | ● | ● | ● |

69.16 (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 with a REG_DWORD value of 4.

```
HKLM\SYSTEM\CurrentControlSet\Services\p2pimsvc:Start
```

Remediation:

Remediation of this service is currently not possible through Settings Catalog or a custom profile OMA-URI. Instead, it can be scripted and deployed through the Intune Scripts or Remediations blade or by other means.

To establish the recommended configuration via PowerShell, run the following cmdlet:

```
Set-Service -Name p2pimsvc -StartupType Disabled
```

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. | ● | ● | ● |

69.17 (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 with a REG_DWORD value of 4.

```
HKLM\SYSTEM\CurrentControlSet\Services\PNRPAutoReg:Start
```

Remediation:

Remediation of this service is currently not possible through Settings Catalog or a custom profile OMA-URI. Instead, it can be scripted and deployed through the Intune Scripts or Remediations blade or by other means.

To establish the recommended configuration via PowerShell, run the following cmdlet:

```
Set-Service -Name PNRPAutoReg -StartupType Disabled
```

Default Value:

Manual

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> | ● | ● | ● |

69.18 (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 with a REG_DWORD value of 4.

```
HKLM\SYSTEM\CurrentControlSet\Services\Spooler:Start
```

Remediation:

Remediation of this service is currently not possible through Settings Catalog or a custom profile OMA-URI. Instead, it can be scripted and deployed through the Intune Scripts or Remediations blade or by other means.

To establish the recommended configuration via PowerShell, run the following cmdlet:

```
Set-Service -Name Spooler -StartupType Disabled
```

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 | <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> | ● | ● | ● |

69.19 (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 with a REG_DWORD value of 4.

```
HKLM\SYSTEM\CurrentControlSet\Services\wercplsupport:Start
```

Remediation:

Remediation of this service is currently not possible through Settings Catalog or a custom profile OMA-URI. Instead, it can be scripted and deployed through the Intune Scripts or Remediations blade or by other means.

To establish the recommended configuration via PowerShell, run the following cmdlet:

```
Set-Service -Name wercplsupport -StartupType Disabled
```

Default Value:

Manual

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> | ● | ● | ● |

69.20 (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 with a REG_DWORD value of 4.

```
HKLM\SYSTEM\CurrentControlSet\Services\RasAuto:Start
```

Remediation:

Remediation of this service is currently not possible through Settings Catalog or a custom profile OMA-URI. Instead, it can be scripted and deployed through the Intune Scripts or Remediations blade or by other means.

To establish the recommended configuration via PowerShell, run the following cmdlet:

```
Set-Service -Name RasAuto -StartupType Disabled
```

Default Value:

Manual

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> | ● | ● | ● |

69.21 (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 with a REG_DWORD value of 4.

```
HKLM\SYSTEM\CurrentControlSet\Services\SessionEnv:Start
```

Remediation:

Remediation of this service is currently not possible through Settings Catalog or a custom profile OMA-URI. Instead, it can be scripted and deployed through the Intune Scripts or Remediations blade or by other means.

To establish the recommended configuration via PowerShell, run the following cmdlet:

```
Set-Service -Name SessionEnv -StartupType Disabled
```

Default Value:

Manual

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> | ● | ● | ● |

69.22 (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 with a REG_DWORD value of 4.

```
HKLM\SYSTEM\CurrentControlSet\Services\TermService:Start
```

Remediation:

Remediation of this service is currently not possible through Settings Catalog or a custom profile OMA-URI. Instead, it can be scripted and deployed through the Intune Scripts or Remediations blade or by other means.

To establish the recommended configuration via PowerShell, run the following cmdlet:

```
Set-Service -Name TermService -StartupType Disabled
```

Default Value:

Manual

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> | ● | ● | ● |

69.23 (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 with a REG_DWORD value of 4.

```
HKLM\SYSTEM\CurrentControlSet\Services\UmRdpService:Start
```

Remediation:

Remediation of this service is currently not possible through Settings Catalog or a custom profile OMA-URI. Instead, it can be scripted and deployed through the Intune Scripts or Remediations blade or by other means.

To establish the recommended configuration via PowerShell, run the following cmdlet:

```
Set-Service -Name UmRdpService -StartupType Disabled
```

Default Value:

Manual

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> | ● | ● | ● |

69.24 (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 or 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 with a REG_DWORD value of 4.

| |
|---|
| HKLM\SYSTEM\CurrentControlSet\Services\RpcLocator:Start |
|---|

Remediation:

To establish the recommended configuration, set the following Custom Configuration Policy to 4:

```
Name: <Enter name>
Description: <Enter Description>
OMA-URI:
./Device/Vendor/MSFT/Policy/Config/SystemServices/ConfigureRemoteProcedureCal
lLocatorServiceStartupMode
Data Type: Integer
Value: 4
```

Note: As of January 2024, despite its inclusion in Microsoft's official documentation, using an OMI-URI to configure a Windows Service Startup Mode via a custom profile will lead to an error in Intune. This error will be logged in the local event log as "The system cannot find the file specified." Currently, the most reliable method for remediation is through PowerShell.

The recommended configuration can also be established via PowerShell by running the following cmdlet:

```
Set-Service -Name RpcLocator -StartupType Disabled
```

Default Value:

Manual

References:

1. <https://learn.microsoft.com/en-us/windows/client-management/mdm/policy-csp-systemservices#configureremoteprocedurecallocatorservicestartupmode>

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. | ● | ● | |

69.25 (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 with a REG_DWORD value of 4.

```
HKLM\SYSTEM\CurrentControlSet\Services\RemoteRegistry:Start
```

Remediation:

Remediation of this service is currently not possible through Settings Catalog or a custom profile OMA-URI. Instead, it can be scripted and deployed through the Intune Scripts or Remediations blade or by other means.

To establish the recommended configuration via PowerShell, run the following cmdlet:

```
Set-Service -Name RemoteRegistry -StartupType Disabled
```

Default Value:

Windows 7: Manual

Windows 8.0 or newer: Disabled

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> | ● | ● | ● |

69.26 (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 with a REG_DWORD value of 4.

| |
|---|
| HKLM\SYSTEM\CurrentControlSet\Services\RemoteAccess:Start |
|---|

Remediation:

To establish the recommended configuration, set the following Custom Configuration Policy to 4:

```
Name: <Enter name>
Description: <Enter Description>
OMA-URI:
./Device/Vendor/MSFT/Policy/Config/SystemServices/ConfigureRoutingAndRemoteAccessServiceStartupMode
Data Type: Integer
Value: 4
```

Note: As of January 2024, despite its inclusion in Microsoft's official documentation, using an OMI-URI to configure a Windows Service Startup Mode via a custom profile will lead to an error in Intune. This error will be logged in the local event log as "The system cannot find the file specified." Currently, the most reliable method for remediation is through PowerShell.

The recommended configuration can also be established via PowerShell by running the following cmdlet:

```
Set-Service -Name RemoteAccess -StartupType Disabled
```

Default Value:

Disabled

References:

1. <https://learn.microsoft.com/en-us/windows/client-management/mdm/policy-csp-systemservices#configureroutingandremoteaccessservicestartupmode>

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. | ● | ● | |

69.27 (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 with a REG_DWORD value of 4.

```
HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer:Start
```

Remediation:

Remediation of this service is currently not possible through Settings Catalog or a custom profile OMA-URI. Instead, it can be scripted and deployed through the Intune Scripts or Remediations blade or by other means.

To establish the recommended configuration via PowerShell, run the following cmdlet:

```
Set-Service -Name LanmanServer -StartupType Disabled
```

Default Value:

Windows 7 through Windows 10 R1703: Automatic

Windows 10 R1709 or newer: Automatic (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> | ● | ● | ● |

69.28 (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 TCP/IP 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 with a REG_DWORD value of 4 or that the key does not exist.

| |
|--|
| HKLM\SYSTEM\CurrentControlSet\Services\simptcp:Start |
|--|

Remediation:

To establish the recommended configuration, set the following Custom Configuration Policy to 4 or confirm that the service is Not installed:

```
Name: <Enter name>
Description: <Enter Description>
OMA-URI:
./Device/Vendor/MSFT/Policy/Config/SystemServices/ConfigureSimpleTCPIPService
sStartupMode
Data Type: Integer
Value: 4
```

Note: As of January 2024, despite its inclusion in Microsoft's official documentation, using an OMI-URI to configure a Windows Service Startup Mode via a custom profile will lead to an error in Intune. This error will be logged in the local event log as "The system cannot find the file specified." Currently, the most reliable method for remediation is through PowerShell.

The recommended configuration can also be established via PowerShell by running the following cmdlet:

```
Set-Service -Name simptcp -StartupType Disabled
```

Default Value:

Not Installed (Automatic when installed)

References:

1. [https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-r2-and-2008/cc725973\(v=ws.10\)](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-r2-and-2008/cc725973(v=ws.10))
2. <https://learn.microsoft.com/en-us/windows/client-management/mdm/policy-csp-systemservices#configuresimpletcpipservicesstartupmode>

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. | | ● | ● |

69.29 (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 with a REG_DWORD value of 4 or that the key does not exist.

```
HKLM\SYSTEM\CurrentControlSet\Services\SNMP:Start
```

Remediation:

Remediation of this service is currently not possible through Settings Catalog or a custom profile OMA-URI. Instead, it can be scripted and deployed through the Intune Scripts **or** Remediations blade or by other means.

To establish the recommended configuration via PowerShell, run the following cmdlet:

```
Set-Service -Name SNMP -StartupType Disabled
```

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. | ● | ● | ● |

69.30 (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 with a REG_DWORD value of 4 or that the key does not exist.

| |
|---|
| HKLM\SYSTEM\CurrentControlSet\Services\sacsrv:Start |
|---|

Remediation:

To establish the recommended configuration, set the following Custom Configuration Policy to 4 or confirm that the service is Not installed:

```
Name: <Enter name>
Description: <Enter Description>
OMA-URI:
./Device/Vendor/MSFT/Policy/Config/SystemServices/ConfigureSpecialAdministrationConsoleHelperServiceStartupMode
Data Type: Integer
Value: 4
```

Note: As of January 2024, despite its inclusion in Microsoft's official documentation, using an OMI-URI to configure a Windows Service Startup Mode via a custom profile will lead to an error in Intune. This error will be logged in the local event log as "The system cannot find the file specified." Currently, the most reliable method for remediation is through PowerShell.

The recommended configuration can also be established via PowerShell by running the following cmdlet:

```
Set-Service -Name sacsrv -StartupType Disabled
```

Default Value:

Not Installed (Manual when installed)

References:

1. <https://learn.microsoft.com/en-us/windows/client-management/mdm/policy-csp-systemservices#configurespecialadministrationconsolehelperservicestartupmode>

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. | | ● | ● |

69.31 (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 with a REG_DWORD value of 4.

HKLM\SYSTEM\CurrentControlSet\Services\SSDPSRV:Start

Remediation:

To establish the recommended configuration, set the following Custom Configuration Policy to 4:

```
Name: <Enter name>
Description: <Enter Description>
OMA-URI:
./Device/Vendor/MSFT/Policy/Config/SystemServices/ConfigureSSDPDiscoveryServiceStartupMode
Data Type: Integer
Value: 4
```

Note: As of January 2024, despite its inclusion in Microsoft's official documentation, using an OMI-URI to configure a Windows Service Startup Mode via a custom profile will lead to an error in Intune. This error will be logged in the local event log as "The system cannot find the file specified." Currently, the most reliable method for remediation is through PowerShell.

The recommended configuration can also be established via PowerShell by running the following cmdlet:

```
Set-Service -Name SSDPSRV -StartupType Disabled
```

Default Value:

Manual

References:

1. <https://learn.microsoft.com/en-us/windows/client-management/mdm/policy-csp-systemservices#configuressdpdiscoveryservicestartupmode>

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. | ● | ● | |

69.32 (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 with a REG_DWORD value of 4.

| |
|---|
| HKLM\SYSTEM\CurrentControlSet\Services\upnphost:Start |
|---|

Remediation:

To establish the recommended configuration, set the following Custom Configuration Policy to 4:

```
Name: <Enter name>
Description: <Enter Description>
OMA-URI:
./Device/Vendor/MSFT/Policy/Config/SystemServices/ConfigureUPnPDeviceHostServiceStartupMode
Data Type: Integer
Value: 4
```

Note: As of January 2024, despite its inclusion in Microsoft's official documentation, using an OMI-URI to configure a Windows Service Startup Mode via a custom profile will lead to an error in Intune. This error will be logged in the local event log as "The system cannot find the file specified." Currently, the most reliable method for remediation is through PowerShell.

The recommended configuration can also be established via PowerShell by running the following cmdlet:

```
Set-Service -Name upnphost -StartupType Disabled
```

Default Value:

Manual

References:

1. <https://learn.microsoft.com/en-us/windows/client-management/mdm/policy-csp-systemservices#configureupnpdevicehostservicestartupmode>

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. | ● | ● | |

69.33 (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 with a REG_DWORD value of 4 or that the key does not exist.

| |
|--|
| HKLM\SYSTEM\CurrentControlSet\Services\WMSvc:Start |
|--|

Remediation:

To establish the recommended configuration, set the following Custom Configuration Policy to 4 or confirm that the service is Not installed:

```
Name: <Enter name>
Description: <Enter Description>
OMA-URI:
./Device/Vendor/MSFT/Policy/Config/SystemServices/ConfigureWebManagementServiceStartupMode
Data Type: Integer
Value: 4
```

Note: As of January 2024, despite its inclusion in Microsoft's official documentation, using an OMI-URI to configure a Windows Service Startup Mode via a custom profile will lead to an error in Intune. This error will be logged in the local event log as "The system cannot find the file specified." Currently, the most reliable method for remediation is through PowerShell.

The recommended configuration can also be established via PowerShell by running the following cmdlet:

```
Set-Service -Name WMSvc -StartupType Disabled
```

Default Value:

Not Installed (Manual when installed)

References:

1. <https://learn.microsoft.com/en-us/windows/client-management/mdm/policy-csp-systemservices#configurewebmanagementservicestartupmode>

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. | ● | ● | |

69.34 (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 with a REG_DWORD value of 4.

```
HKLM\SYSTEM\CurrentControlSet\Services\WerSvc:Start
```

Remediation:

Remediation of this service is currently not possible through Settings Catalog or a custom profile OMA-URI. Instead, it can be scripted and deployed through the Intune Scripts or Remediations blade or by other means.

To establish the recommended configuration via PowerShell, run the following cmdlet:

```
Set-Service -Name WerSvc -StartupType Disabled
```

Default Value:

Windows 7: Manual

Windows 8.0 or newer: 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> | ● | ● | ● |

69.35 (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 with a REG_DWORD value of 4.

```
HKLM\SYSTEM\CurrentControlSet\Services\Wecsvc:Start
```

Remediation:

Remediation of this service is currently not possible through Settings Catalog or a custom profile OMA-URI. Instead, it can be scripted and deployed through the Intune Scripts or Remediations blade or by other means.

To establish the recommended configuration via PowerShell, run the following cmdlet:

```
Set-Service -Name Wecsvc -StartupType Disabled
```

Default Value:

Manual

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> | ● | ● | ● |

69.36 (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 with a REG_DWORD value of 4 or that the key does not exist.

| |
|--|
| HKLM\SYSTEM\CurrentControlSet\Services\WMPNetworkSvc:Start |
|--|

Remediation:

To establish the recommended configuration, set the following Custom Configuration Policy to 4 or confirm that the service is Not installed:

```
Name: <Enter name>
Description: <Enter Description>
OMA-URI:
./Device/Vendor/MSFT/Policy/Config/SystemServices/ConfigureWindowsMediaPlayer
NetworkSharingServiceStartupMode
Data Type: Integer
Value: 4
```

Note: As of January 2024, despite its inclusion in Microsoft's official documentation, using an OMI-URI to configure a Windows Service Startup Mode via a custom profile will lead to an error in Intune. This error will be logged in the local event log as "The system cannot find the file specified." Currently, the most reliable method for remediation is through PowerShell.

The recommended configuration can also be established via PowerShell by running the following cmdlet:

```
Set-Service -Name WMPNetworkSvc -StartupType Disabled
```

Default Value:

Manual

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. | | ● | ● |

69.37 (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 with a REG_DWORD value of 4.

HKLM\SYSTEM\CurrentControlSet\Services\icssvc:Start

Remediation:

To establish the recommended configuration, set the following Custom Configuration Policy to 4 or confirm that the service is Not installed:

```
Name: <Enter name>
Description: <Enter Description>
OMA-URI:
./Device/Vendor/MSFT/Policy/Config/SystemServices/ConfigureWindowsMobileHotspotServiceStartupMode
Data Type: Integer
Value: 4
```

Note: As of January 2024, despite its inclusion in Microsoft's official documentation, using an OMI-URI to configure a Windows Service Startup Mode via a custom profile will lead to an error in Intune. This error will be logged in the local event log as "The system cannot find the file specified." Currently, the most reliable method for remediation is through PowerShell.

The recommended configuration can also be established via PowerShell by running the following cmdlet:

```
Set-Service -Name icssvc -StartupType Disabled
```

Default Value:

Manual (Trigger Start)

References:

1. <https://learn.microsoft.com/en-us/windows/client-management/mdm/policy-csp-systemservices#configurewindowsmobilehotspotservicestartupmode>

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. | ● | ● | |

69.38 (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 third-party notifications and updates from the cloud/Internet. In a high security environment, external systems, especially those hosted outside the organization, should be prevented from having an impact on the secure workstations.

Impact:

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 with a REG_DWORD value of 4.

```
HKLM\SYSTEM\CurrentControlSet\Services\WpnService:Start
```

Remediation:

Remediation of this service is currently not possible through Settings Catalog or a custom profile OMA-URI. Instead, it can be scripted and deployed through the Intune Scripts or Remediations blade or by other means.

To establish the recommended configuration via PowerShell, run the following cmdlet:

```
Set-Service -Name WpnService -StartupType Disabled
```

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> | ● | ● | ● |

69.39 (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 with a REG_DWORD value of 4.

```
HKLM\SYSTEM\CurrentControlSet\Services\PushToInstall:Start
```

Remediation:

Remediation of this service is currently not possible through Settings Catalog or a custom profile OMA-URI. Instead, it can be scripted and deployed through the Intune Scripts or Remediations blade or by other means.

To establish the recommended configuration via PowerShell, run the following cmdlet:

```
Set-Service -Name PushToInstall -StartupType Disabled
```

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> | ● | ● | ● |

69.40 (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 with a REG_DWORD value of 4.

```
HKLM\SYSTEM\CurrentControlSet\Services\WinRM:Start
```

Remediation:

Remediation of this service is currently not possible through Settings Catalog or a custom profile OMA-URI. Instead, it can be scripted and deployed through the Intune Scripts or Remediations blade or by other means.

To establish the recommended configuration via PowerShell, run the following cmdlet:

```
Set-Service -Name WinRM -StartupType Disabled
```

Default Value:

Manual

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> | ● | ● | ● |

69.41 (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 with a REG_DWORD value of 4 or that the key does not exist.

HKLM\SYSTEM\CurrentControlSet\Services\W3SVC:Start

Remediation:

To establish the recommended configuration, set the following Custom Configuration Policy to 4 or confirm that the service is Not installed:

```
Name: <Enter name>
Description: <Enter Description>
OMA-URI:
./Device/Vendor/MSFT/Policy/Config/SystemServices/ConfigureWorldWideWebPublishingServiceStartupMode
Data Type: Integer
Value: 4
```

Note: As of January 2024, despite its inclusion in Microsoft's official documentation, using an OMI-URI to configure a Windows Service Startup Mode via a custom profile will lead to an error in Intune. This error will be logged in the local event log as "The system cannot find the file specified." Currently, the most reliable method for remediation is through PowerShell.

The recommended configuration can also be established via PowerShell by running the following cmdlet:

```
Set-Service -Name W3SVC -StartupType Disabled
```

Default Value:

Not Installed (Automatic when installed)

References:

1. <https://learn.microsoft.com/en-us/windows/client-management/mdm/policy-csp-systemservices#configureworldwidewebpublishingservicestartupmode>

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. | ● | ● | |

69.42 (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 with a REG_DWORD value of 4.

HKLM\SYSTEM\CurrentControlSet\Services\XboxGipSvc:Start

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`.

System Services\Xbox Accessory Management Service

Default Value:

Windows 10 R1703: Manual

Windows 10 R1709 or newer: Manual (Trigger Start)

References:

1. <https://www.cisecurity.org/insights/blog/update-cis-microsoft-windows-10-enterprise-release-1703-benchmark-v1-0-0>

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> | ● | ● | ● |

69.43 (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 with a REG_DWORD value of 4.

HKLM\SYSTEM\CurrentControlSet\Services\XblAuthManager:Start

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Disabled.

System Services\Xbox Live Auth Manager

Default Value:

Manual

References:

1. <https://www.cisecurity.org/insights/blog/update-cis-microsoft-windows-10-enterprise-release-1703-benchmark-v1-0-0>

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> | ● | ● | ● |

69.44 (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 with a REG_DWORD value of 4.

HKLM\SYSTEM\CurrentControlSet\Services\XblGameSave:Start

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `Disabled`.

System Services\Xbox Live Game Save

Default Value:

Windows 10 R1507 and R1511: Manual

Windows 10 R1607 or newer: Manual (Trigger Start)

References:

1. <https://www.cisecurity.org/insights/blog/update-cis-microsoft-windows-10-enterprise-release-1703-benchmark-v1-0-0>

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> | ● | ● | ● |

69.45 (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 with a REG_DWORD value of 4.

HKLM\SYSTEM\CurrentControlSet\Services\XboxNetApiSvc:Start

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Disabled.

System Services\Xbox Live Networking Service

Default Value:

Manual

References:

1. <https://www.cisecurity.org/insights/blog/update-cis-microsoft-windows-10-enterprise-release-1703-benchmark-v1-0-0>

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. | ● | ● | ● |

70 Task Scheduler

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

71 Text Input

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

72 Time Language Settings

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

73 Troubleshooting

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

74 User Rights

This section contains recommendations for User Rights assignments.

74.1 (L1) Ensure 'Access Credential Manager As 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 Local Security Policy and confirm it is set as prescribed.

Security Settings\Local Policies\User Rights Assignment\Access Credential Manager as a trusted caller

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to (<! [CDATA[]]>) which represents No One.

User Rights\Access Credential Manager As Trusted Caller

Note: Using (<! [CDATA[]]>) to represent a blank value or No One is recommended by Microsoft. However, there is a known issue where an error occurs in Endpoint Manager (Intune) but this does not affect the policy setting from being applied properly to the system.

Default Value:

No one.

References:

1. <https://learn.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 |
|------------------|---|------|------|------|
| v8 | <p>6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.</p> | | | ● |
| v7 | <p>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.</p> | | ● | ● |

74.2 (L1) Ensure 'Access From 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.

Note: If your organization is using Microsoft Defender for Identity (formerly Azure Advanced Threat Protection (Azure ATP)), the (organization-named) Defender for Identity Directory Service Account (DSA), will also need to be granted the same ^{Access} from network User Right Assignment. For more information on adding the service account please see [Make sure the DSA is allowed to access computers from the network in Microsoft Defender for Identity | Microsoft Docs](#).

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 Local Security Policy and confirm it is set as prescribed.

Security Settings\Local Policies\User Rights Assignment\Access this computer from the network

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to **Administrators, Remote Desktop Users**.

User Rights\Access From Network

Note: Include only one User or Group per line in the Settings Catalog configuration screen.

Default Value:

Administrators, Backup Operators, Everyone, Users.

References:

1. <https://learn.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 |
|------------------|---|------|------|------|
| v8 | <p>6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.</p> | | | ● |
| v7 | <p>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.</p> | | ● | ● |

74.3 (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 Local Security Policy and confirm it is set as prescribed.

Security Settings\Local Policies\User Rights Assignment\Act as part of the operating system

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to (<! [CDATA[]]>) which equals No One.

User Rights\Act As Part Of The Operating System

Note: Using (<! [CDATA[]]>) to represent a blank value or No One is recommended by Microsoft. However, there is a known issue where an error occurs in Endpoint Manager (Intune) but does not affect the policy setting from being applied to the system properly.

Default Value:

No one.

References:

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

CIS Controls:

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

74.4 (L1) Ensure 'Allow Local Log On' 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 Local Security Policy and confirm it is set as prescribed.

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

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Administrators, Users.

User Rights\Allow Local Log On

Note: Include only one User or Group per line in the Settings Catalog configuration screen.

Default Value:

Administrators, Backup Operators, Guest, Users.

References:

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

CIS Controls:

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

74.5 (L1) Ensure 'Backup 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 Local Security Policy and confirm it is set as prescribed.

Security Settings\Local Policies\User Rights Assignment\Back up files and directories

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Administrators.

User Rights\Backup Files And Directories

Note: Include only one User or Group per line in the Settings Catalog configuration screen.

Default Value:

Administrators, Backup Operators.

References:

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

CIS Controls:

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

74.6 (L1) Ensure 'Change 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 Local Security Policy and confirm it is set as prescribed.

Security Settings\Local Policies\User Rights Assignment\Change the system time

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Administrators, LOCAL SERVICE.

User Rights\Change System Time

Note: Include only one User or Group per line in the Settings Catalog configuration screen.

Default Value:

Administrators, LOCAL SERVICE.

References:

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

CIS Controls:

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

74.7 (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 Local Security Policy and confirm it is set as prescribed.

Security Settings\Local Policies\User Rights Assignment>Create global objects

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE.

User Rights\Create Global Objects

Note: Include only one User or Group per line in the Settings Catalog configuration screen.

Default Value:

Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE.

References:

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

CIS Controls:

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

74.8 (L1) Ensure 'Create Page File' 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 Local Security Policy and confirm it is set as prescribed.

Security Settings\Local Policies\User Rights Assignment>Create a pagefile

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Administrators.

User Rights\Create Page File

Note: Include only one User or Group per line in the Settings Catalog configuration screen.

Default Value:

Administrators.

References:

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

CIS Controls:

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

74.9 (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 Local Security Policy and confirm it is set as prescribed.

Security Settings\Local Policies\User Rights Assignment>Create Permanent Shared Objects

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to (<! [CDATA[]]>) which equals No One.

User Rights\Create Permanent Shared Objects

Note: Using (<! [CDATA[]]>) to represent a blank value or No One is recommended by Microsoft. However, there is a known issue where an error occurs in Endpoint Manager (Intune) but does not affect the policy setting from being applied to the system properly.

Default Value:

No one.

References:

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

CIS Controls:

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

74.10 (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 Local Security Policy and confirm it is set as prescribed.

Security Settings\Local Policies\User Rights Assignment\Create Symbolic Links

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Administrators and (when the Hyper-V feature is installed) NT VIRTUAL MACHINE\Virtual Machines.

User Rights\Create Symbolic Links

Note: Include only one User or Group per line in the Settings Catalog configuration screen.

Default Value:

Administrators.

References:

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

CIS Controls:

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

74.11 (L1) Ensure 'Create Token' 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 Local Security Policy and confirm it is set as prescribed.

Security Settings\Local Policies\User Rights Assignment>Create a token object

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to (<! [CDATA[]]>) which equals No One.

User Rights\Create Token

Note: Using (<! [CDATA[]]>) to represent a blank value or No One is recommended by Microsoft. However, there is a known issue where an error occurs in Endpoint Manager (Intune) but does not affect the policy setting from being applied to the system properly.

Default Value:

No one.

References:

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

CIS Controls:

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

74.12 (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 Local Security Policy and confirm it is set as prescribed.

Security Settings\Local Policies\User Rights Assignment\Debug Programs

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Administrators.

User Rights\Debug Programs

Note: Include only one User or Group per line in the Settings Catalog configuration screen.

Default Value:

Administrators.

References:

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

CIS Controls:

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

74.13 (L1) Ensure 'Deny Access From 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 Computer From 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 Local Security Policy and confirm it is set as prescribed.

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

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Guests, Local account.

User Rights\Deny Access From Network

Note: Include only one User or Group per line in the Settings Catalog configuration screen.

Default Value:

Guest.

References:

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

CIS Controls:

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

74.14 (L1) Ensure 'Deny Local Log On' 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.

Warning: The help text in Intune associated with this recommendation is for the setting, *Deny log on as a service* and not this setting.

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 configuration profiles, set the following Settings Catalog path to Guests.

User Rights\Deny Local Log On

Note: Include only one User or Group per line in the Settings Catalog configuration screen.

Default Value:

Guest.

References:

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

CIS Controls:

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

74.15 (L1) Ensure 'Deny Remote Desktop Services Log On' 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 Local Security Policy and confirm it is set as prescribed.

Security Settings\Local Policies\User Rights Assignment\Deny log on through Remote Desktop Services

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Guests, Local account.

User Rights\Deny Remote Desktop Services Log On

Note: Include only one User or Group per line in the Settings Catalog configuration screen.

Default Value:

No one.

References:

1. <https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/deny-log-on-through-remote-desktop-services>

CIS Controls:

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

74.16 (L1) Ensure 'Enable 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 Local Security Policy and confirm it is set as prescribed.

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

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to (<! [CDATA[]]>) which equals No One.

User Rights\Enable Delegation

Note: Using (<! [CDATA[]]>) to represent a blank value or No One is recommended by Microsoft. However, there is a known issue where an error occurs in Endpoint Manager (Intune) but does not affect the policy setting from being applied to the system properly.

Default Value:

No one.

References:

1. <https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/enable-computer-and-user-accounts-to-be-trusted-for-delegation>

CIS Controls:

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

74.17 (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 Local Security Policy and confirm it is set as prescribed.

Security Settings\Local Policies\User Rights Assignment\Generate security audits

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to LOCAL SERVICE, NETWORK SERVICE.

User Rights\Generate security audits

Note: Include only one User or Group per line in the Settings Catalog configuration screen.

Default Value:

LOCAL SERVICE, NETWORK SERVICE.

References:

1. <https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/generate-security-audits>

CIS Controls:

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

74.18 (L1) Ensure 'Impersonate Client' 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 Local Security Policy and confirm it is set as prescribed.

Security Settings\Local Policies\User Rights Assignment\Impersonate a client after authentication

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE.

User Rights\Impersonate Client

Note: Include only one User or Group per line in the Settings Catalog configuration screen.

Default Value:

Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE.

References:

1. <https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/impersonate-a-client-after-authentication>

CIS Controls:

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

74.19 (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 Local Security Policy and confirm it is set as prescribed.

Security Settings\Local Policies\User Rights Assignment\Increase scheduling priority

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Administrators, Window Manager\Window Manager Group.

User Rights\Increase scheduling priority

Note: Include only one User or Group per line in the Settings Catalog configuration screen.

Default Value:

On Windows 10 R1607 or older: Administrators.

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

References:

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

CIS Controls:

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

74.20 (L1) Ensure 'Load 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 Local Security Policy and confirm it is set as prescribed.

Security Settings\Local Policies\User Rights Assignment\Load and unload device drivers

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to **Administrators**.

User Rights\Load Unload Device Drivers

Note: Include only one User or Group per line in the Settings Catalog configuration screen.

Default Value:

Administrators.

References:

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

CIS Controls:

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

74.21 (L1) Ensure 'Lock 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 Local Security Policy and confirm it is set as prescribed.

Security Settings\Local Policies\User Rights Assignment\Lock pages in memory

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to (<! [CDATA[]]>) which equals No One.

User Rights\Lock Memory

Note: Using (<! [CDATA[]]>) to represent a blank value or No One is recommended by Microsoft. However, there is a known issue where an error occurs in Endpoint Manager (Intune) but does not affect the policy setting from being applied to the system properly.

Default Value:

No one.

References:

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

CIS Controls:

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

74.22 (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 Local Security Policy and confirm it is set as prescribed.

Security Settings\Local Policies\User Rights Assignment\Manage auditing and security log

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Administrators.

User Rights\Manage auditing and security log

Note: Include only one User or Group per line in the Settings Catalog configuration screen.

Default Value:

Administrators.

References:

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

CIS Controls:

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

74.23 (L1) Ensure 'Manage Volume' 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 Local Security Policy and confirm it is set as prescribed.

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

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Administrators.

```
User Rights\Manage Volume
```

Note: Include only one User or Group per line in the Settings Catalog configuration screen.

\

Default Value:

Administrators.

References:

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

CIS Controls:

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

74.24 (L1) Ensure 'Modify Firmware Environment' 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 and 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 Local Security Policy and confirm it is set as prescribed.

Security Settings\Local Policies\User Rights Assignment\Modify firmware environment values

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Administrators.

User Rights\Modify Firmware Environment

Note: Include only one User or Group per line in the Settings Catalog configuration screen.

Default Value:

Administrators.

References:

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

CIS Controls:

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

74.25 (L1) Ensure 'Modify 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 Local Security Policy and confirm it is set as prescribed.

Security Settings\Local Policies\User Rights Assignment\Modify an object label

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to (<! [CDATA[]]>) which equals No One.

User Rights\Modify Object Label

Note: Using (<! [CDATA[]]>) to represent a blank value or No One is recommended by Microsoft. However, there is a known issue where an error occurs in Endpoint Manager (Intune) but does not affect the policy setting from being applied to the system properly.

Default Value:

No one.

References:

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

CIS Controls:

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

74.26 (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 Local Security Policy and confirm it is set as prescribed.

Security Settings\Local Policies\User Rights Assignment\Profile single process

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Administrators.

User Rights\Profile single process

Note: Include only one User or Group per line in the Settings Catalog configuration screen.

Default Value:

Administrators.

References:

1. <https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/profile-single-process>

CIS Controls:

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

74.27 (L1) Ensure 'Remote Shutdown' 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 or newer computers from remote locations on the network. Anyone who has been assigned this user right can cause a denial of service (DoS) condition, which would make the computer unavailable to service user requests. Therefore, it is recommended that only highly trusted administrators be assigned this user right.

The recommended state for this setting is: Administrators.

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 Local Security Policy and confirm it is set as prescribed.

Security Settings\Local Policies\User Rights Assignment\Force shutdown from a remote system

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Administrators.

User Rights\Remote Shutdown

Note: Include only one User or Group per line in the Settings Catalog configuration screen.

Default Value:

Administrators.

References:

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

CIS Controls:

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

74.28 (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 Local Security Policy and confirm it is set as prescribed.

Security Settings\Local Policies\User Rights Assignment\Restore files and directories

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Administrators.

User Rights\Restore files and directories

Note: Include only one User or Group per line in the Settings Catalog configuration screen.

Default Value:

Administrators, Backup Operators.

References:

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

CIS Controls:

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

74.29 (L1) Ensure 'Take Ownership' 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 Local Security Policy and confirm it is set as prescribed.

Security Settings\Local Policies\User Rights Assignment\Take ownership of files or other objects

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Administrators.

User Rights\Take Ownership

Note: Include only one User or Group per line in the Settings Catalog configuration screen.

Default Value:

Administrators.

References:

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

CIS Controls:

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

75 Virtualization Based Technology

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

76 Wi-Fi Settings

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

77 Widgets

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

78 Windows Defender Security Center

This section contains recommendations for Windows Defender Security Center.

78.1 (L1) Ensure 'Disallow Exploit Protection Override' is set to '(Enable)' (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: (Enable).

Rationale:

Only authorized IT staff should be able to make changes to the exploit protection settings in order to ensure the organizations specific configuration is not modified.

Impact:

Local users cannot make changes in the Exploit protection settings area.

Audit:

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

HKLM\SOFTWARE\Policies\Microsoft\Windows Defender Security Center\App and Browser protection:DisallowExploitProtectionOverride

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to (Enable).

Windows Defender Security Center\Disallow Exploit Protection Override

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 | <p>10.5 <u>Enable Anti-Exploitation Features</u></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 <u>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> | | ● | ● |

79 Windows Hello For Business

This section contains recommendations for Windows Hello For Business.

Windows Hello for Business is designed to be managed by group policy or MDM, but not a combination of both. Avoid mixing group policy and MDM policy settings for Windows Hello for Business. If you mix group policy and MDM policy settings, the MDM settings are ignored until all group policy settings are cleared.

79.1 (L1) Ensure 'Facial Features Use Enhanced Anti Spoofing' is set to 'true' (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: true.

Rationale:

Enterprise managed environments are now supporting a wider range of mobile devices, increasing the security on these devices will help protect against unauthorized access on your network.

Impact:

Windows will require all users on the device to use anti-spoofing for facial features, on devices which support it.

Audit:

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

HKLM\SOFTWARE\Microsoft\Policies\PassportForWork\Biometrics:FacialFeaturesUseEnhancedAntiSpoofing

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to true.

Windows Hello For Business\Facial Features Use Enhanced Anti Spoofing

Default Value:

Users are able to choose whether or not to use enhanced anti-spoofing on supported devices.

References:

1. <https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-biometrics-in-enterprise>

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| 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. | | ● | ● |

79.2 (L1) Ensure 'Minimum PIN Length' is set to '6 more character(s)' (Automated)

Profile Applicability:

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

Description:

Minimum PIN length configures the minimum number of characters required for the PIN. The lowest number you can configure for this policy setting is 4. The largest number you can configure must be less than the number configured in the Maximum PIN length policy setting or the number 127, whichever is the lowest.

The recommended state for this setting is: 6 more character(s).

Rationale:

Windows Hello for Business utilizes key-based or certificate-based authentication and makes credential theft extremely difficult.

When backed with a TPM chip multiple physical security mechanisms are added in order to make it tamper resistant.

Impact:

PIN theft is possible through shoulder surfing or other means of reconnaissance. Although this threat applies to passwords as well it is reduced with passphrases which involve complexity and length.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a REG_DWORD value of 6 (or higher).

HKLM\SOFTWARE\Microsoft\Policies\PassportForWork\<Tenant-ID>\Device\Policies\PINComplexity:MinimumPINLength

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to 6 (or more character(s)):

Windows Hello For Business\Minimum PIN Length

Default Value:

4

References:

1. <https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-why-pin-is-better-than-password>
2. https://learn.microsoft.com/en-us/windows/client-management/mdm/passportforwork-csp?WT.mc_id=Portal-fx#devicetenantidpoliciespincomplexityminimumpinlength

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. | | ● | ● |

79.3 (L1) Ensure 'Require Security Device' is set to 'true' (Automated)

Profile Applicability:

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

Description:

This policy controls whether a Trusted Platform Module (TPM) is required to provision Windows Hello for Business.

- If you enable this policy setting, only devices with a usable TPM provision Windows Hello for Business.
- If you disable or don't configure this policy setting, the TPM is still preferred, but all devices provision Windows Hello for Business using software if the TPM is non-functional or unavailable.

The recommended state for this setting is: true.

Rationale:

Windows Hello for Business utilizes key-based or certificate-based authentication and makes credential theft extremely difficult.

When backed with a TPM chip multiple physical security mechanisms are added in order to make it tamper resistant.

Impact:

If the TPM chip unexpectedly fails the user would be unable to authenticate using their PIN but would still be able to sign-in with their EntralID account 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 with a REG_DWORD value of 1.

```
HKLM\SOFTWARE\Microsoft\Policies\PassportForWork\<Tenant-ID>\Device\Policies:RequireSecurityDevice
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to `true`:

| |
|--|
| Windows Hello For Business\Require Security Device |
|--|

Default Value:

false (Disabled)

References:

1. <https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-why-pin-is-better-than-password>
2. https://learn.microsoft.com/en-us/windows/client-management/mdm/passportforwork-csp?WT.mc_id=Portal-Microsoft_Intune_Workflows#usertenantidpoliciesrequiresecuritydevice

Additional Information:

Applies to **Windows 11** only.

80 Windows Ink Workspace

This section contains recommendations for Windows Ink Workspace.

80.1 (L2) Ensure 'Allow suggested apps in Windows Ink Workspace' is set to 'Block' (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: Block.

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:

1. Navigate to the following registry location and note the *WinningProvider* GUID. This value confirms under which User GUID the policy is set.

```
HKLM\SOFTWARE\Microsoft\PolicyManager\current\device\WindowsInkWorkspace:AllowSuggestedAppsInWindowsInkWorkspace_WinningProvider
```

2. Navigate to the following registry location and confirm the value is set to 0.

```
HKLM\SOFTWARE\Microsoft\PolicyManager\Providers\{GUID}\Default\Device\WindowsInkWorkspace:AllowSuggestedAppsInWindowsInkWorkspace
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Block.

```
Windows Ink Workspace\Allow suggested apps in Windows Ink Workspace
```

Default Value:

Enabled. (The suggested apps in Windows Ink Workspace will be allowed.)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| 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. | | ● | ● |

**80.2 (L1) Ensure 'Allow Windows Ink Workspace' is set to
'Enabled: but the user can't access it above the lock screen' OR
'Disabled' (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: Ink workspace is enabled (feature is turned on), but the user can't access it above the lock screen **OR** Access to ink workspace is disabled. The feature is turned off.

Rationale:

Allowing any apps to be accessed while system is locked is not recommended. If this feature is permitted, it should only be accessible once a user authenticates with the proper credentials.

Impact:

Windows Ink Workspace will not be permitted above the lock screen.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a REG_DWORD value of 0 or 1.

HKLM\SOFTWARE\Microsoft\PolicyManager\current\device\WindowsInkWorkspace:AllowWindowsInkWorkspace

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Ink workspace is enabled (feature is turned on), but the user can't access it above the lock screen **OR** Access to ink workspace is disabled. The feature is turned off.

Windows Ink Workspace\Allow Windows Ink Workspace

Default Value:

Enabled. (Windows Ink Workspace is permitted above the lock screen.)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| 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. | | ● | ● |

81 Windows Logon

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

82 Windows Subsystem For Linux

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

83 Windows Update For Business

This section contains recommendations for Windows Update For Business.

83.1 (L1) Ensure 'Allow Auto Update' 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 this this policy setting is set to Enabled, select one of the following options in the Configure Automatic Updates Properties dialog box to specify how the service will work:

- 2 - Auto install and restart.
- 3 - Auto install and restart at a specified time. (Default)
- 4 - Auto install and restart without end-user control.

The recommended state for this setting is: `Enabled` and never "Turn off automatic updates"

Note: The sub-setting "*Allow Auto Update*:" has 6 possible values – not all of them are valid depending on specific organizational needs, however if feasible we suggest using a value of 2, 3, or 4. The only scored requirement is to not turn off automatic updates (5).

Note #2: Organizations that utilize a third--party solution for patching may choose to exempt themselves from this recommendation, and instead configure it to `Disabled` so that the native Windows Update mechanism does not interfere with the third--party patching process.

Warning: If option 3 or 4 is not selected, then the `ScheduledInstallDay` recommendation will not take effect and an exception to that recommendation will be needed.

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.

HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU:NoAutoUpdate

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to anything other than "Turn off automatic updates".

Windows Update For Business\Allow Auto Update

Default Value:

Enabled: 2 - Auto install and restart. (Updates are downloaded automatically on non-metered networks and installed during "Automatic Maintenance" when the device isn't in use and isn't running on battery power.)

References:

1. https://learn.microsoft.com/en-us/windows/client-management/mdm/policy-csp-Update?WT.mc_id=Portal-fx#allowautoupdate

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. | ● | ● | ● |

83.2 (L1) Ensure 'Defer Feature Updates Period in Days' 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 with a REG_DWORD value of 180 or more.

HKLM\SOFTWARE\Microsoft\PolicyManager\current\device\Update:DeferFeatureUpdatesPeriodInDays

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled: 180 or more days.

Windows Update for Business\Defer Feature Updates Period in Days

Default Value:

Disabled. (Feature Update cadence will not be enforced.)

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 | 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. | | ● | ● |

83.3 (L1) Ensure 'Defer Quality Updates Period (Days)' is set to 'Enabled: 0 days' (Automated)

Profile Applicability:

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

Description:

This policy setting controls when Quality Updates are received.

The recommended state for this setting is: Enabled: 0 days.

Note: If the "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 with a REG_DWORD value of 0.

HKLM\SOFTWARE\Microsoft\PolicyManager\current\device\Update:DeferQualityUpdatesPeriodInDays

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Enabled: 0 days.

| |
|---|
| Windows Update for Business\Defer Quality Updates Period (Days) |
|---|

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 | 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. | ● | ● | ● |

83.4 (L1) Ensure 'Manage preview builds' is set to 'Disable Preview builds' (Automated)

Profile Applicability:

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

Description:

This policy setting manages which updates that are received prior to the update being released.

Dev Channel: Ideal for highly technical users. Insiders in the Dev Channel will receive builds from our active development branch that is earliest in a development cycle. These builds are not matched to a specific Windows 10 release.

Beta Channel: Ideal for feature explorers who want to see upcoming Windows 10 features. Your feedback will be especially important here as it will help our engineers ensure key issues are fixed before a major release.

Release Preview Channel (default): Insiders in the Release Preview Channel will have access to the upcoming release of Windows 10 prior to it being released to the world. These builds are supported by Microsoft. The Release Preview Channel is where we recommend companies preview and validate upcoming Windows 10 releases before broad deployment within their organization.

The recommended state for this setting is: Disable Preview builds.

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 with a REG_DWORD value of 0.

HKLM\SOFTWARE\Microsoft\PolicyManager\current\device\Update:ManagePreviewBuilds

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Disable Preview builds.

Windows Update For Business\Manage preview builds

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://learn.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 | ● | ● | ● |

83.5 (L1) Ensure 'Scheduled Install Day' is set to '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: Every day.

Note: This setting is only applicable if the option of 3 or 4 is selected in the recommendation 'Allow Auto Update'. 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 option 3 or 4 is selected in recommendation 'Allow Auto Update', critical operating system updates and service packs will automatically download every day (at 3:00 A.M., by default).

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a REG_DWORD value of 0.

HKLM\SOFTWARE\Microsoft\PolicyManager\current\device\Update:ScheduledInstallDay

Remediation:

To establish the recommended configuration via configuration profiles, set the following Settings Catalog path to Every day.

Windows Update For Business\Scheduled Install Day

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> | ● | ● | ● |

83.6 (L1) Ensure 'Block "Pause Updates" ability' is set to 'Block' (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: Block.

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 with a REG_DWORD value of 1.

HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate:SetDisablePauseUXAccess

Remediation:

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

Windows Update For Business\Block "Pause Updates" ability

Default Value:

Disabled. (Users have access to the "Pause updates" feature.)

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> | ● | ● | ● |

84 Wireless Display

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

85 Windows LAPS

This section contains recommendations for Windows Local Administrator Password Solution (LAPS) settings.

Settings in this section are not available in Settings Catalog, instead need to be configured in [Endpoint security > Account Protection](#).

85.1 (L1) Ensure 'Backup Directory' is set to 'Backup the password to Azure AD only' (Automated)

Profile Applicability:

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

Description:

This policy setting configures which directory Windows LAPS will use to back up the local admin account password.

The recommended state for this setting is: Backup the password to Azure AD only.

Note: Organizations that utilize third-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations.

- Windows LAPS does not support standalone computers - they must be joined to an Active Directory domain or Entra ID (formerly Azure Active Directory).
- Windows LAPS does not support simultaneous storage of the local admin password in both directory types.
- If the setting is configured and the managed device is not joined to the configured directory type, the local administrator password will not be managed by Windows LAPS.

Important: An organization wishing to use Active Directory to backup the LAPS password may make an exception for this recommendation. To implement Active Directory backup see the latest on-premises CIS Benchmark for Windows 10/11. When backing up with Active Directory there are 2 additional security controls to be considered in the benchmark which are not available when using Azure AD for backup. These were excluded from the Intune benchmark as they cannot be selected unless Active Directory is selected as the backup location.

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 passwords managed by Windows LAPS will only be retrievable from the configured directory type.

Audit:

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

HKLM\SOFTWARE\Microsoft\Policies\LAPS:BackupDirectory

Remediation:

To establish the recommended configuration from Microsoft Intune Admin Center:

1. Navigate to Endpoint security > Account protection.
2. Create or edit a LAPS policy of the type Local admin password solution (Windows LAPS).
3. Set Backup Directory to Backup the password to Azure AD only.

Default Value:

Disabled. (The local administrator password is not managed by Windows LAPS.)

References:

1. <https://learn.microsoft.com/en-us/windows-server/identity/laps/laps-scenarios-azure-active-directory>
2. https://learn.microsoft.com/en-us/windows/client-management/mdm/laps-csp?WT.mc_id=Portal-fx#policiesbackupdirectory

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| v7 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |

85.2 (L1) Ensure 'Password Age Days' is set to 'Configured: 30 or fewer' (Automated)

Profile Applicability:

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

Description:

This policy setting configures the Windows LAPS Password Settings policy for password length.

Each additional character in a password increases its complexity exponentially. For instance, a seven-character, all lower-case alphabetic password would have 26 to the power of 7 (approximately 8×10 to the power of 9 or 8 billion) possible combinations. At 1,000,000 attempts per second (a capability of many password-cracking utilities), it would only take 133 minutes to crack. A seven-character case-sensitive alphanumeric password without punctuation has 627 combinations. An eight-character password has 26 to the power of 8 (or 2×10 to the power of 11) possible combinations. Although this might seem to be a large number, at 1,000,000 attempts per second it would take only 59 hours to try all possible passwords. Remember, these times will significantly increase for passwords that use ALT characters and other special keyboard characters such as "!" or "@". Proper use of the password settings can help make it difficult to mount a brute force attack.

The recommended state for this setting is: Configured: 30 or fewer.

Note: Organizations that utilize third-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations.

Note #2: Windows LAPS does not support standalone computers - they must be joined to an Active Directory domain or Entra ID (formerly Azure Active Directory).

Rationale:

Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or Member Servers when deploying them. This creates a serious attack surface security risk because if 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:

None - this is the default behavior, unless set to fewer than 30 days.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a REG_DWORD value of 30.

HKLM\SOFTWARE\Microsoft\Policies\LAPS:PasswordAgeDays

Remediation:

To establish the recommended configuration from Microsoft Intune Admin Center:

1. Navigate to Endpoint security > Account protection.
2. Create or edit a LAPS policy type Local admin password solution (Windows LAPS).
3. Set Password Age Days to Configured: 30 (or fewer)

Default Value:

30 days.

References:

1. https://learn.microsoft.com/en-us/windows/client-management/mdm/laps-csp?WT.mc_id=Portal-fx#policiespasswordagedays

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. | ● | ● | ● |

85.3 (L1) Ensure 'Password Complexity' is set to 'Large letters + small letters + numbers + special characters' (Automated)

Profile Applicability:

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

Description:

This policy setting configures the Windows LAPS Password Settings policy for password complexity.

Each additional character in a password increases its complexity exponentially. For instance, a seven-character, all lower-case alphabetic password would have 26 to the power of 7 (approximately 8×10 to the power of 9 or 8 billion) possible combinations. At 1,000,000 attempts per second (a capability of many password-cracking utilities), it would only take 133 minutes to crack. A seven-character case-sensitive alphanumeric password without punctuation has 627 combinations. An eight-character password has 26 to the power of 8 (or 2×10 to the power of 11) possible combinations. Although this might seem to be a large number, at 1,000,000 attempts per second it would take only 59 hours to try all possible passwords. Remember, these times will significantly increase for passwords that use ALT characters and other special keyboard characters such as "!" or "@". Proper use of the password settings can help make it difficult to mount a brute force attack.

The recommended state for this setting is: Large letters + small letters + numbers + special characters.

Note: Organizations that utilize third-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations.

Note #2: Windows LAPS does not support standalone computers - they must be joined to an Active Directory domain or Entra ID (formerly Azure Active Directory).

Rationale:

Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or Member Servers when deploying them. This creates a serious attack surface security risk because if 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:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a REG_DWORD value of 4.

HKLM\SOFTWARE\Microsoft\Policies\LAPS:PasswordComplexity

Remediation:

To establish the recommended configuration from Microsoft Intune Admin Center:

1. Navigate to Endpoint security > Account protection.
2. Create or edit a LAPS policy type Local admin password solution (Windows LAPS).
3. Set Password Complexity to Large letters + small letters + numbers + special characters.

Default Value:

Large letters + small letters + numbers + special characters.

References:

1. https://learn.microsoft.com/en-us/windows/client-management/mdm/laps-csp?WT.mc_id=Portal-fx#policiespasswordcomplexity

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. | | ● | ● |

85.4 (L1) Ensure 'Password Length' is set to 'Configured: 15 or more' (Automated)

Profile Applicability:

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

Description:

This policy setting configures the Windows LAPS Password Settings policy for password length.

Each additional character in a password increases its complexity exponentially. For instance, a seven-character, all lower-case alphabetic password would have 26 to the power of 7 (approximately 8×10 to the power of 9 or 8 billion) possible combinations. At 1,000,000 attempts per second (a capability of many password-cracking utilities), it would only take 133 minutes to crack. A seven-character case-sensitive alphanumeric password without punctuation has 627 combinations. An eight-character password has 26 to the power of 8 (or 2×10 to the power of 11) possible combinations. Although this might seem to be a large number, at 1,000,000 attempts per second it would take only 59 hours to try all possible passwords. Remember, these times will significantly increase for passwords that use ALT characters and other special keyboard characters such as "!" or "@". Proper use of the password settings can help make it difficult to mount a brute force attack.

The recommended state for this setting is: Configured: 15 or more.

Note: Organizations that utilize third-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations.

Note #2: Windows LAPS does not support standalone computers - they must be joined to an Active Directory domain or Entra ID (formerly Azure Active Directory).

Rationale:

Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or Member Servers when deploying them. This creates a serious attack surface security risk because if 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:

Windows LAPS-generated passwords will be required to have a length of 15 characters (or more, if selected).

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a REG_DWORD value of 15.

HKLM\SOFTWARE\Microsoft\Policies\LAPS:PasswordLength

Remediation:

To establish the recommended configuration from Microsoft Intune Admin Center:

1. Navigate to Endpoint security > Account protection.
2. Create or edit a LAPS policy type Local admin password solution (Windows LAPS).
3. Set Password Length to Configured: 15 (or more).

Default Value:

14 characters.

References:

1. https://learn.microsoft.com/en-us/windows/client-management/mdm/laps-csp?WT.mc_id=Portal-fx#policiespasswordlength

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. | ● | ● | ● |

85.5 (L1) Ensure 'Post-authentication actions' is set to 'Reset the password and logoff the managed account' or higher (Automated)

Profile Applicability:

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

Description:

This policy setting configures post-authentication actions which will be executed after detecting an authentication by the LAPS managed account. The `Action` refers to actions to take upon expiry of the grace period before executing the specified post-authentication actions.

Post-authentication actions:

- `Reset password`: upon expiry of the grace period, the managed account password will be reset.
- `Reset the password and logoff the managed account`: upon expiry of the grace period, the managed account password will be reset and any interactive logon sessions using the managed account will terminate.
- `Reset the password and reboot the device`: upon expiry of the grace period, the managed account password will be reset and the managed device will be immediately rebooted.

Warning: After an interactive logon session is terminated, other authenticated sessions using the Windows LAPS managed account may still be active. The only way to ensure that the previous password is no longer in use is to reboot the OS.

The recommended state for this setting is: `Reset the password and logoff the managed account or higher`.

Note: Organizations that utilize third-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations.

Note #2: Windows LAPS does not support standalone computers - they must be joined to an Active Directory domain or Entra ID (formerly Azure Active Directory).

Rationale:

Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or Member Servers when deploying them. This creates a serious attack surface security risk because if 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:

After the grace period expires, the Windows LAPS managed account password will be reset and logged off the system or the OS will be restarted.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a REG_DWORD value of 3 or 5.

HKLM\SOFTWARE\Microsoft\Policies\LAPS:PostAuthenticationActions

Remediation:

To establish the recommended configuration from Microsoft Intune Admin Center:

1. Navigate to Endpoint security > Account protection.
2. Create or edit a LAPS policy type Local admin password solution (Windows LAPS).
3. Set Post Authentication Actions to Reset the password and logoff the managed account (or higher).

Note: Both Reset the password and logoff the managed account and Reset the password and reboot are considered passing states.

Default Value:

Disabled. (Reset the password and logoff the managed account after the specified grace period.)

References:

1. https://learn.microsoft.com/en-us/windows/client-management/mdm/laps-csp?WT.mc_id=Portal-fx#policiespostauthenticationactions

85.6 (L1) Ensure 'Post Authentication Reset Delay' is set to 'Configured: 8 or fewer hours, but not 0' (Automated)

Profile Applicability:

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

Description:

This policy setting configures post-authentication actions which will be executed after detecting an authentication by the Windows LAPS managed account. The Grace period refers to the amount of time (hours) to wait after an authentication before executing the specified post-authentication actions.

The recommended state for this setting is: Configured: 8 or fewer hours, but not 0.

Note: Organizations that utilize third-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations.

Note #2: Windows LAPS does not support standalone computers - they must be joined to an Active Directory domain or Entra ID (formerly Azure Active Directory).

Note #3: If this policy is set to 0 it prevents all post-authentication actions from occurring.

Rationale:

Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or Member Servers when deploying them. This creates a serious attack surface security risk because if 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:

After 8 hours, the Windows LAPS managed account password will be reset and log off the system.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location with a REG_DWORD value of 8 or less, but not 0.

HKLM\SOFTWARE\Microsoft\Policies\LAPS:PostAuthenticationResetDelay

Remediation:

To establish the recommended configuration from Microsoft Intune Admin Center:

1. Navigate to Endpoint security > Account protection.
2. Create or edit a **LAPS** policy type Local admin password solution (Windows LAPS).
3. Set Post Authentication Reset Delay to Configured: 8 (or fewer hours, but not 0).

Default Value:

Disabled. (Specified post-authentication actions will be executed after a default 24-hour grace period.)

References:

1. https://learn.microsoft.com/en-us/windows/client-management/mdm/laps-csp?WT.mc_id=Portal-fx#policiespostauthenticationresetdelay

86 Miscellaneous Recommendations

This section contains settings that are supported by other non-settings catalog configuration profiles. Ex.: Custom

Settings contained within this section are **not** included in the CIS Intune Build Kit. Separate configuration profiles will need to be created manually for these settings.

86.1 Custom Profile

This section contains recommendations that are configured in the Custom Profile.

86.1.1 (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:

1. Navigate to the following registry location and note the *WinningProvider* GUID. This value confirms under which User GUID the policy is set.

```
HKLM\SOFTWARE\Microsoft\PolicyManager\current\device\ApplicationManagement:AllowSharedUserAppData_WinningProvider
```

2. Navigate to the following registry location and confirm the value is set to 0.

```
HKLM\SOFTWARE\Microsoft\PolicyManager\Providers\{GUID}\Default\Device\ApplicationManagement:AllowSharedUserAppData
```

Remediation:

To establish the recommended configuration, set the following Custom Configuration Policy to 0:

```
Name: <Enter name>
Description: <Enter Description>
OMA-URI:
./Device/Vendor/MSFT/Policy/Config/ApplicationManagement/AllowSharedUserAppData
Data type: Integer
Value: 0
```

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 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| v7 | 14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. | ● | ● | ● |

86.1.2 (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:

1. Navigate to the following registry location and note the *WinningProvider* GUID.
This value confirms under which User GUID the policy is set.

```
HKLM\SOFTWARE\Microsoft\PolicyManager\current\device\Wifi:AllowAutoConnectToWiFiSenseHotspots_ProviderSet
```

2. Navigate to the following registry location and confirm the value is set to 0.

```
HKLM\SOFTWARE\Microsoft\PolicyManager\Providers\{GUID}\Default\Device\Wifi:AllowAutoConnectToWiFiSenseHotspots
```

Remediation:

To establish the recommended configuration, set the following Custom Configuration Policy to 0:

```
Name: <Enter name>
Description: <Enter Description>
OMA-URI:
./Device/Vendor/MSFT/Policy/Config/Wifi/AllowAutoConnectToWiFiSenseHotspots
Data type: Integer
Value: 0
```

Default Value:

Enabled. (Users can choose to enable or disable either "Connect to suggested open hotspots" or "Connect to networks shared by my contacts".)

References:

1. <https://learn.microsoft.com/en-us/windows/configuration/manage-wifi-sense-in-enterprise>

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|------|------|------|
| v8 | 4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. | | ● | ● |
| v7 | 15.5 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. | | | ● |

86.1.3 (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 third-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:

1. Navigate to the following registry location and note the *WinningProvider* GUID. This value confirms under which User GUID the policy is set.

```
HKLM\SOFTWARE\Microsoft\PolicyManager\current\device\System:DisableEnterpriseAuthProxy_WinningProvider
```

2. Navigate to the following registry location and confirm the value is set to 1.

```
HKLM\SOFTWARE\Microsoft\PolicyManager\Providers\{GUID}\Default\Device\System:DisableEnterpriseAuthProxy
```

Remediation:

To establish the recommended configuration, set the following Custom Configuration Policy to 1:

```
Name: <Enter name>
Description: <Enter Description>
OMA-URI:
./Device/Vendor/MSFT/Policy/Config/System/DisableEnterpriseAuthProxy
Data type: Integer
Value: 1
```

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 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| 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. | | ● | ● |

86.1.4 (BL) Ensure 'Enumeration policy for external devices incompatible with Kernel DMA Protection' is set to 'Enabled: Block All' (Automated)

Profile Applicability:

- BitLocker (BL)

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 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:

1. Navigate to the following registry location and note the *WinningProvider* GUID.
This value confirms under which User GUID the policy is set.

```
HKLM\SOFTWARE\Microsoft\PolicyManager\current\device\DeviceEnumerationPolicy_WinningProvider
```

2. Navigate to the following registry location and confirm the value is set to 0.

```
HKLM\SOFTWARE\Microsoft\PolicyManager\Providers\{GUID}\Default\Device\DeviceEnumerationPolicy
```

Remediation:

To establish the recommended configuration via configuration profiles, set the following *Custom* profile path to `Enabled: Block All`:

```
Name: <Enter name>
Description: <Enter Description>
OMA-URL:
./Device/Vendor/MSFT/Policy/Config/DmaGuard/DeviceEnumerationPolicy
Data Type: Integer
Value: 0
```

Default Value:

Windows 10 R1803 or 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 |
|------------------|--|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| v7 | 1.4 <u>Maintain Detailed Asset Inventory</u> 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. | ● | ● | ● |

86.1.5 (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.

Warning: If the [Self Service Password Reset \(SSPR\)](#) feature is used in Microsoft Entra ID, an exception to this recommendation is needed as it's known to interfere with SSPR.

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.

This setting can prevent standard users (without Administrator access) from launching Office 365 (O365) applications, displaying the error: "*Windows cannot access the specified device, path, or file. You may not have the appropriate permissions to access the item.*"

Audit:

1. Navigate to the following registry location and note the *WinningProvider* GUID. This value confirms under which User GUID the policy is set.

```
HKLM\SOFTWARE\Microsoft\PolicyManager\current\device\ApplicationManagement:BlockNonAdminUserInstall_WinningProvider
```

2. Navigate to the following registry location and confirm the value is set to 1.

```
HKLM\SOFTWARE\Microsoft\PolicyManager\Providers\{GUID}\Default\Device\ApplicationManagement:BlockNonAdminUserInstall
```

Remediation:

To establish the recommended configuration, set the following Custom Configuration Policy to 1:

```
Name: <Enter name>
Description: <Enter Description>
OMA-URI:
./Device/Vendor/MSFT/Policy/Config/ApplicationManagement/BlockNonAdminUserInstall
Data type: Integer
Value: 1
```

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. | ● | ● | ● |

86.1.6 (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:

1. Navigate to the following registry location and note the *WinningProvider* GUID. This value confirms under which User GUID the policy is set.

```
HKLM\SOFTWARE\Microsoft\PolicyManager\current\device\System:AllowLocation_WinningProvider
```

2. Navigate to the following registry location and confirm the value is set to 0.

```
HKLM\SOFTWARE\Microsoft\PolicyManager\Providers\{GUID}\Default\Device\System:AllowLocation
```

Remediation:

To establish the recommended configuration, set the following Custom Configuration Policy to 0:

| | |
|--------------|---|
| Name: | <Enter name> |
| Description: | <Enter Description> |
| OMA-URI: | ./Device/Vendor/MSFT/Policy/Config/System/AllowLocation |
| Data type: | Integer |
| Value: | 0 |

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 |
|------------------|---|------|------|------|
| 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. | | ● | ● |

86.1.7 (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 third-party.

Impact:

Users will no longer see personalized recommendations from Microsoft and notifications about their Microsoft account.

Audit:

1. Navigate to the following registry location and note the *WinningProvider* GUID. This value confirms under which User GUID the policy is set.

```
HKLM\SOFTWARE\Microsoft\PolicyManager\current\device\Experience:AllowWindowsConsumerFeatures_WinningProvider
```

2. Navigate to the following registry location and confirm the value is set to 0.

```
HKLM\SOFTWARE\Microsoft\PolicyManager\Providers\{GUID}\Default\Device\Experience:AllowWindowsConsumerFeatures
```

Remediation:

To establish the recommended configuration, set the following Custom Configuration Policy to 0:

```
Name: <Enter name>
Description: <Enter Description>
OMA-URI:
./Device/Vendor/MSFT/Policy/Config/Experience/AllowWindowsConsumerFeatures
Data type: Integer
Value: 0
```

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 |
|------------------|---|------|------|------|
| 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. | | ● | ● |

86.1.8 (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 third-party notifications and updates from the cloud/Internet. In a high security environment, external systems, especially those hosted outside the organization, should be prevented from having an impact on the secure workstations.

Impact:

Applications and system features will not be able receive notifications from the network from WNS or via notification polling APIs.

Audit:

1. Navigate to the following registry location and note the *WinningProvider* GUID. This value confirms under which User GUID the policy is set.

```
HKLM\SOFTWARE\Microsoft\PolicyManager\current\device\Notifications:DisallowCloudNotification_WinningProvider
```

2. Navigate to the following registry location and confirm the value is set to 1.

```
HKLM\SOFTWARE\Microsoft\PolicyManager\Providers\{GUID}\Default\Device\Notifications:DisallowCloudNotification
```

Remediation:

To establish the recommended configuration, set the following Custom Configuration Policy to 1:

```
Name: <Enter name>
Description: <Enter Description>
OMA-URI:
./Device/Vendor/MSFT/Policy/Config/Notifications/DisallowCloudNotification
Data type: Integer
Value: 1
```

Default Value:

Disabled.

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|------|
| v8 | 0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped | | | |
| 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. | | ● | ● |

Appendix: Summary Table

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|---|--------------------------|-------------------------------------|
| | | Yes | No |
| 1 | Above Lock | | |
| 1.1 | (L1) Ensure 'Allow Cortana Above Lock' is set to 'Block' (Automated) | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 2 | Accounts | | |
| 3 | Administrative Templates | | |
| 3.1 | Control Panel | | |
| 3.1.1 | Add or Remove Programs | | |
| 3.1.2 | Display | | |
| 3.1.3 | Personalization | | |
| 3.1.3.1 | (L1) Ensure 'Enable screen saver (User)' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 3.1.3.2 | (L1) Ensure 'Prevent enabling lock screen camera' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 3.1.3.3 | (L1) Ensure 'Prevent enabling lock screen slide show' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 3.1.4 | Printers | | |
| 3.1.5 | Programs | | |
| 3.1.6 | Regional and Language Options | | |
| 3.1.6.1 | Handwriting personalization | | |
| 3.1.7 | User Account | | |
| 3.2 | Desktop | | |
| 3.3 | LAPS (legacy) | | |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|---|--------------------------|--------------------------|
| | | Yes | No |
| 3.4 | MS Security Guide | | |
| 3.4.1 | (L1) Ensure 'Apply UAC restrictions to local accounts on network logons' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.2 | (L1) Ensure 'Configure SMB v1 client driver' is set to 'Enabled: Disable driver (recommended)' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.3 | (L1) Ensure 'Configure SMB v1 server' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.4 | (L1) Ensure 'Enable Structured Exception Handling Overwrite Protection (SEHOP)' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4.5 | (L1) Ensure 'WDigest Authentication' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.5 | MSS (Legacy) | | |
| 3.5.1 | (L1) Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.5.2 | (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"/> |
| 3.5.3 | (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"/> |
| 3.5.4 | (L2) Ensure 'MSS: (DisableSavePassword) Prevent the dial-up password from being saved (recommended)' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.5.5 | (L1) Ensure 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|--|--------------------------|--------------------------|
| | | Yes | No |
| 3.5.6 | (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"/> |
| 3.5.7 | (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"/> |
| 3.5.8 | (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"/> |
| 3.5.9 | (L1) Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.5.10 | (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"/> |
| 3.5.11 | (L2) Ensure 'MSS: (TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted' is set to 'Enabled: 3' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.5.12 | (L2) Ensure 'MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted' is set to 'Enabled: 3' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.5.13 | (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"/> |
| 3.6 | Network | | |
| 3.6.1 | Background Intelligent Transfer Service (BITS) | | |
| 3.6.2 | BranchCache | | |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|--|--------------------------|-------------------------------------|
| | | Yes | No |
| 3.6.3 | DirectAccess Client Experience Settings | | |
| 3.6.4 | DNS Client | | |
| 3.6.4.1 | (L1) Ensure 'Turn off multicast name resolution' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 3.6.5 | Hotspot Authentication | | |
| 3.6.6 | Lanman Server | | |
| 3.6.7 | Lanman Workstation | | |
| 3.6.8 | Link-Layer Topology Discovery | | |
| 3.6.8.1 | (L2) Ensure 'Turn on Mapper I/O (LLTDIO) driver' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 3.6.8.2 | (L2) Ensure 'Turn on Responder (RSPNDR) driver' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 3.6.9 | Network Connections | | |
| 3.6.9.1 | (L1) Ensure 'Prohibit installation and configuration of Network Bridge on your DNS domain network' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 3.6.9.2 | (L1) Ensure 'Prohibit use of Internet Connection Sharing on your DNS domain network' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 3.6.9.3 | (L1) Ensure 'Require domain users to elevate when setting a network's location' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 3.6.10 | Network Connectivity Status Indicator | | |
| 3.6.11 | Network Provider | | |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|---|--------------------------|--------------------------|
| | | Yes | No |
| 3.6.11.1 | (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"/> |
| 3.6.12 | Offline Files | | |
| 3.6.13 | QoS Packet Scheduler | | |
| 3.6.14 | SNMP | | |
| 3.6.15 | SSL Configuration Settings | | |
| 3.6.16 | TCPIP Settings | | |
| 3.6.17 | Windows Connect Now | | |
| 3.6.17.1 | (L2) Ensure 'Configuration of wireless settings using Windows Connect Now' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.6.17.2 | (L2) Ensure 'Prohibit access of the Windows Connect Now wizards' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.6.18 | Windows Connection Manager | | |
| 3.6.18.1 | (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"/> |
| 3.6.18.2 | (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"/> |
| 3.6.19 | Wireless Display | | |
| 3.6.19.1 | (L1) Ensure 'Require PIN pairing' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.7 | Printers | | |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|---|--------------------------|--------------------------|
| | | Yes | No |
| 3.7.1 | (L1) Ensure 'Allow Print Spooler to accept client connections' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.7.2 | (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"/> |
| 3.7.3 | (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"/> |
| 3.8 | Shared Folders | | |
| 3.9 | Start Menu and Taskbar | | |
| 3.9.1 | Notifications | | |
| 3.9.1.1 | (L1) Ensure 'Turn off toast notifications on the lock screen (User)' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.10 | System | | |
| 3.10.1 | Access-Denied Assistance | | |
| 3.10.2 | App-V | | |
| 3.10.3 | Application Compatibility Settings | | |
| 3.10.4 | Audit Process Creation | | |
| 3.10.4.1 | (L1) Ensure 'Include command line in process creation events' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.10.5 | Credentials Delegation | | |
| 3.10.5.1 | (L1) Ensure 'Encryption Oracle Remediation' is set to 'Enabled: Force Updated Clients' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.10.5.2 | (L1) Ensure 'Remote host allows delegation of non-exportable credentials' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.10.6 | Ctrl+Alt+Del Options | | |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|--|--------------------------|--------------------------|
| | | Yes | No |
| 3.10.7 | Device Guard | | |
| 3.10.8 | Device Health Attestation Service | | |
| 3.10.9 | Device Installation | | |
| 3.10.9.1 | Device Installation Restrictions | | |
| 3.10.9.1.1 | (BL) Ensure 'Prevent installation of devices that match any of these device IDs' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.10.9.1.2 | (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"/> |
| 3.10.9.1.3 | (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"/> |
| 3.10.9.1.4 | (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"/> |
| 3.10.9.1.5 | (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"/> |
| 3.10.9.1.6 | (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"/> |
| 3.10.9.2 | (L1) Ensure 'Prevent device metadata retrieval from the Internet' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.10.10 | Disk NV Cache | | |
| 3.10.11 | Disk Quotas | | |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|---|--------------------------|-------------------------------------|
| | | Yes | No |
| 3.10.12 | Driver Installation | | |
| 3.10.13 | Early Launch Antimalware | | |
| 3.10.13.1 | (L1) Ensure 'Boot-Start Driver Initialization Policy' is set to 'Enabled: Good, unknown and bad but critical' (Automated) | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 3.10.14 | Enhanced Storage Access | | |
| 3.10.15 | File Classification Infrastructure | | |
| 3.10.16 | File Share Shadow Copy Provider | | |
| 3.10.17 | Filesystem | | |
| 3.10.18 | Folder Redirection | | |
| 3.10.19 | Group Policy | | |
| 3.10.19.1 | (L1) Ensure 'Configure registry policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE' (Automated) | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 3.10.19.2 | (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 checked="" type="checkbox"/> |
| 3.10.19.3 | (L1) Ensure 'Configure security policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE' (Automated) | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 3.10.19.4 | (L1) Ensure 'Configure security policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE' (Automated) | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 3.10.19.5 | (L1) Ensure 'Continue experiences on this device' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 3.10.19.6 | (L1) Ensure 'Turn off background refresh of Group Policy' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input checked="" type="checkbox"/> |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|---|--------------------------|--------------------------|
| | | Yes | No |
| 3.10.20 | Internet Communication Management | | |
| 3.10.20.1 | Internet Communication settings | | |
| 3.10.20.1.1 | (L2) Ensure 'Turn off access to the Store' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.10.20.1.2 | (L1) Ensure 'Turn off downloading of print drivers over HTTP' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.10.20.1.3 | (L2) Ensure 'Turn off Help Experience Improvement Program (User)' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.10.20.1.4 | (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"/> |
| 3.10.20.1.5 | (L1) Ensure 'Turn off Internet download for Web publishing and online ordering wizards' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.10.20.1.6 | (L2) Ensure 'Turn off printing over HTTP' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.10.20.1.7 | (L2) Ensure 'Turn off Registration if URL connection is referring to Microsoft.com' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.10.20.1.8 | (L2) Ensure 'Turn off Search Companion content file updates' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.10.20.1.9 | (L2) Ensure 'Turn off the "Order Prints" picture task' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.10.20.1.10 | (L2) Ensure 'Turn off the "Publish to Web" task for files and folders' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.10.20.1.11 | (L2) Ensure 'Turn off the Windows Messenger Customer Experience Improvement Program' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|--|--------------------------|--------------------------|
| | | Yes | No |
| 3.10.20.1.12 | (L2) Ensure 'Turn off Windows Customer Experience Improvement Program' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.10.20.1.13 | (L2) Ensure 'Turn off Windows Error Reporting' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.10.21 | iSCSI | | |
| 3.10.22 | KDC | | |
| 3.10.23 | Kerberos | | |
| 3.10.23.1 | (L2) Ensure 'Support device authentication using certificate' is set to 'Enabled: Automatic' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.10.24 | Locale Services | | |
| 3.10.24.1 | (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"/> |
| 3.10.25 | Logon | | |
| 3.10.25.1 | (L1) Ensure 'Block user from showing account details on sign-in' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.10.25.2 | (L1) Ensure 'Do not display network selection UI' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.10.25.3 | (L1) Ensure 'Do not enumerate connected users on domain-joined computers' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.10.25.4 | (L1) Ensure 'Enumerate local users on domain-joined computers' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.10.25.5 | (L1) Ensure 'Turn off app notifications on the lock screen' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.10.25.6 | (L1) Ensure 'Turn off picture password sign-in' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|---|--------------------------|--------------------------|
| | | Yes | No |
| 3.10.25.7 | (L1) Ensure 'Turn on convenience PIN sign-in' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.10.26 | Mitigation Options | | |
| 3.10.27 | Net Logon | | |
| 3.10.28 | Power Management | | |
| 3.10.28.1 | Button Settings | | |
| 3.10.28.2 | Hard Disk Settings | | |
| 3.10.28.3 | Notification Settings | | |
| 3.10.28.4 | Power Throttling Settings | | |
| 3.10.28.5 | Sleep Settings | | |
| 3.10.28.5.1 | (L1) Ensure 'Allow network connectivity during connected-standby (on battery)' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.10.28.5.2 | (L1) Ensure 'Allow network connectivity during connected-standby (plugged in)' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.10.28.5.3 | (BL) Ensure 'Allow standby states (S1-S3) when sleeping (on battery)' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.10.28.5.4 | (BL) Ensure 'Allow standby states (S1-S3) when sleeping (plugged in)' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.10.28.5.5 | (L1) Ensure 'Require a password when a computer wakes (on battery)' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.10.28.5.6 | (L1) Ensure 'Require a password when a computer wakes (plugged in)' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.10.29 | Remote Assistance | | |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|---|--------------------------|--------------------------|
| | | Yes | No |
| 3.10.29.1 | (L1) Ensure 'Configure Offer Remote Assistance' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.10.29.2 | (L1) Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.10.30 | Remote Procedure Call | | |
| 3.10.30.1 | (L1) Ensure 'Enable RPC Endpoint Mapper Client Authentication' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.10.30.2 | (L1) Ensure 'Restrict Unauthenticated RPC clients' is set to 'Enabled: Authenticated' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.10.31 | Remote Storage Access | | |
| 3.10.32 | Scripts | | |
| 3.10.33 | Security Settings | | |
| 3.10.34 | Server Manager | | |
| 3.10.35 | Shutdown | | |
| 3.10.36 | Shutdown Options | | |
| 3.10.37 | System Restore | | |
| 3.10.38 | Troubleshooting and Diagnostics | | |
| 3.10.38.1 | Application Compatibility Diagnostic | | |
| 3.10.38.2 | Corrupted File Recovery | | |
| 3.10.38.3 | Disk Diagnostic | | |
| 3.10.38.4 | Fault Tolerant Heap | | |
| 3.10.38.5 | Microsoft Support Diagnostic Tool | | |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|--|--------------------------|--------------------------|
| | | Yes | No |
| 3.10.38.5.1 | (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"/> |
| 3.10.39 | Trusted Platform Module Services | | |
| 3.10.40 | User Profiles | | |
| 3.10.41 | Windows File Protection | | |
| 3.10.42 | Windows Time Service | | |
| 3.10.42.1 | Time Providers | | |
| 3.10.42.1.1 | (L1) Ensure 'Enable Windows NTP Client' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.10.42.1.2 | (L1) Ensure 'Enable Windows NTP Server' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11 | Windows Components | | |
| 3.11.1 | ActiveX Installer Service | | |
| 3.11.2 | App Package Deployment | | |
| 3.11.3 | App runtime | | |
| 3.11.3.1 | (L1) Ensure 'Allow Microsoft accounts to be optional' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11.3.2 | (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"/> |
| 3.11.4 | Application Compatibility | | |
| 3.11.5 | Attachment Manager | | |
| 3.11.5.1 | (L1) Ensure 'Do not preserve zone information in file attachments (User)' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|--|--------------------------|--------------------------|
| | | Yes | No |
| 3.11.5.2 | (L1) Ensure 'Notify antivirus programs when opening attachments (User)' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11.6 | AutoPlay Policies | | |
| 3.11.6.1 | (L1) Ensure 'Disallow Autoplay for non-volume devices' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11.6.2 | (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"/> |
| 3.11.6.3 | (L1) Ensure 'Turn off Autoplay' is set to 'Enabled: All drives' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11.7 | BitLocker Drive Encryption | | |
| 3.11.7.1 | Fixed Data Drives | | |
| 3.11.7.1.1 | (BL) Ensure 'Choose how BitLocker-protected fixed drives can be recovered' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11.7.1.2 | (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"/> |
| 3.11.7.1.3 | (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"/> |
| 3.11.7.1.4 | (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"/> |
| 3.11.7.1.5 | (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"/> |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|---|--------------------------|--------------------------|
| | | Yes | No |
| 3.11.7.1.6 | (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"/> |
| 3.11.7.1.7 | (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"/> |
| 3.11.7.1.8 | (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"/> |
| 3.11.7.2 | Operating System Drives | | |
| 3.11.7.2.1 | (BL) Ensure 'Allow enhanced PINs for startup' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11.7.2.2 | (BL) Ensure 'Choose how BitLocker-protected operating system drives can be recovered' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11.7.2.3 | (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"/> |
| 3.11.7.2.4 | (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"/> |
| 3.11.7.2.5 | (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"/> |
| 3.11.7.2.6 | (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"/> |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|--|--------------------------|--------------------------|
| | | Yes | No |
| 3.11.7.2.7 | (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"/> |
| 3.11.7.2.8 | (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"/> |
| 3.11.7.2.9 | (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"/> |
| 3.11.7.2.10 | (BL) Ensure 'Require additional authentication at startup' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11.7.2.11 | (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"/> |
| 3.11.7.2.12 | (BL) Ensure 'Require additional authentication at startup: Configure TPM startup key and PIN:' is set to 'Enabled: Do not allow startup key and PIN with TPM' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11.7.2.13 | (BL) Ensure 'Require additional authentication at startup: Configure TPM startup key:' is set to 'Enabled: Do not allow startup key with TPM' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11.7.2.14 | (BL) Ensure 'Require additional authentication at startup: Configure TPM startup PIN:' is set to 'Enabled: Require startup PIN with TPM' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11.7.2.15 | (BL) Ensure 'Require additional authentication at startup: Configure TPM startup:' is set to 'Enabled: Do not allow TPM' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11.7.3 | Removable Data Drives | | |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|--|--------------------------|--------------------------|
| | | Yes | No |
| 3.11.7.3.1 | (BL) Ensure 'Deny write access to removable drives not protected by BitLocker' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11.7.3.2 | (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"/> |
| 3.11.8 | Credential User Interface | | |
| 3.11.8.1 | (L1) Ensure 'Do not display the password reveal button' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11.8.2 | (L1) Ensure 'Enumerate administrator accounts on elevation' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11.8.3 | (L1) Ensure 'Prevent the use of security questions for local accounts' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11.9 | Data Collection and Preview Builds | | |
| 3.11.10 | Delivery Optimization | | |
| 3.11.11 | Desktop Window Manager | | |
| 3.11.12 | Device and Driver Compatibility | | |
| 3.11.13 | Digital Locker | | |
| 3.11.14 | Event Forwarding | | |
| 3.11.15 | Event Log Service | | |
| 3.11.15.1 | Application | | |
| 3.11.15.1.1 | (L1) Ensure 'Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11.15.1.2 | (L1) Ensure 'Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|--|--------------------------|--------------------------|
| | | Yes | No |
| 3.11.15.2 | Security | | |
| 3.11.15.2.1 | (L1) Ensure 'Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11.15.2.2 | (L1) Ensure 'Specify the maximum log file size (KB)' is set to 'Enabled: 196,608 or greater' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11.15.3 | Setup | | |
| 3.11.15.3.1 | (L1) Ensure 'Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11.15.3.2 | (L1) Ensure 'Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11.15.4 | System | | |
| 3.11.15.4.1 | (L1) Ensure 'Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11.15.4.2 | (L1) Ensure 'Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11.16 | Event Logging | | |
| 3.11.17 | Event Viewer | | |
| 3.11.18 | File Explorer | | |
| 3.11.18.1 | (L1) Ensure 'Configure Windows Defender SmartScreen' is set to 'Enabled: Warn and prevent bypass' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11.18.2 | (L1) Ensure 'Turn off Data Execution Prevention for Explorer' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11.18.3 | (L1) Ensure 'Turn off heap termination on corruption' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|--|--------------------------|--------------------------|
| | | Yes | No |
| 3.11.18.4 | (L1) Ensure 'Turn off shell protocol protected mode' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11.19 | File Revocation | | |
| 3.11.20 | Home Group | | |
| 3.11.20.1 | (L1) Ensure 'Prevent the computer from joining a homegroup' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11.21 | IME | | |
| 3.11.22 | Instant Search | | |
| 3.11.23 | Internet Explorer | | |
| 3.11.23.1 | (L1) Ensure 'Disable Internet Explorer 11 as a standalone browser' is set to 'Enabled: Always' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11.24 | Internet Information Services | | |
| 3.11.25 | Location and Sensors | | |
| 3.11.25.1 | Windows Location Provider | | |
| 3.11.26 | Maintenance Scheduler | | |
| 3.11.27 | Microsoft Account | | |
| 3.11.27.1 | (L1) Ensure 'Block all consumer Microsoft account user authentication' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11.28 | Microsoft Defender Antivirus | | |
| 3.11.28.1 | Client Interface | | |
| 3.11.28.2 | Exclusions | | |
| 3.11.28.3 | MAPS | | |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|---|--------------------------|--------------------------|
| | | Yes | No |
| 3.11.28.3.1 | (L1) Ensure 'Configure local setting override for reporting to Microsoft MAPS' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11.28.3.2 | (L2) Ensure 'Join Microsoft MAPS' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11.28.4 | Microsoft Defender Exploit Guard | | |
| 3.11.28.5 | MpEngine | | |
| 3.11.28.6 | Network Inspection System | | |
| 3.11.28.7 | Quarantine | | |
| 3.11.28.8 | Real-time Protection | | |
| 3.11.28.9 | Remediation | | |
| 3.11.28.10 | Reporting | | |
| 3.11.28.10.1 | (L2) Ensure 'Configure Watson events' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11.28.11 | (L1) Ensure 'Turn off Microsoft Defender Antivirus' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11.29 | Microsoft Management Console | | |
| 3.11.30 | Microsoft User Experience Virtualization | | |
| 3.11.31 | Network Sharing | | |
| 3.11.31.1 | (L1) Ensure 'Prevent users from sharing files within their profile. (User)' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11.32 | Online Assistance | | |
| 3.11.33 | Portable Operating System | | |
| 3.11.34 | Presentation Settings | | |
| 3.11.35 | Push To Install | | |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|---|--------------------------|--------------------------|
| | | Yes | No |
| 3.11.35.1 | (L2) Ensure 'Turn off Push To Install service' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11.36 | Remote Desktop Services | | |
| 3.11.36.1 | RD Gateway | | |
| 3.11.36.2 | RD Licensing | | |
| 3.11.36.3 | Remote Desktop Connection Client | | |
| 3.11.36.3.1 | RemoteFX USB Device Redirection | | |
| 3.11.36.3.2 | (L1) Ensure 'Do not allow passwords to be saved' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11.36.4 | Remote Desktop Session Host | | |
| 3.11.36.4.1 | Azure Virtual Desktop | | |
| 3.11.36.4.2 | Connections | | |
| 3.11.36.4.2.1 | (L2) Ensure 'Allow users to connect remotely by using Remote Desktop Services' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11.36.4.3 | Device and Resource Redirection | | |
| 3.11.36.4.3.1 | (L2) Ensure 'Do not allow COM port redirection' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11.36.4.3.2 | (L1) Ensure 'Do not allow drive redirection' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11.36.4.3.3 | (L2) Ensure 'Do not allow LPT port redirection' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11.36.4.3.4 | (L2) Ensure 'Do not allow supported Plug and Play device redirection' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11.36.4.4 | Licensing | | |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|--|--------------------------|--------------------------|
| | | Yes | No |
| 3.11.36.4.5 | Printer Redirection | | |
| 3.11.36.4.6 | Profiles | | |
| 3.11.36.4.7 | RD Connection Broker | | |
| 3.11.36.4.8 | Remote Session Environment | | |
| 3.11.36.4.9 | Security | | |
| 3.11.36.4.9.1 | (L1) Ensure 'Always prompt for password upon connection' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11.36.4.9.2 | (L1) Ensure 'Require secure RPC communication' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11.36.4.9.3 | (L1) Ensure 'Require use of specific security layer for remote (RDP) connections' is set to 'Enabled: SSL' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11.36.4.9.4 | (L1) Ensure 'Require user authentication for remote connections by using Network Level Authentication' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11.36.4.9.5 | (L1) Ensure 'Set client connection encryption level' is set to 'Enabled: High Level' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11.36.4.10 | Session Time Limits | | |
| 3.11.36.4.10.1 | (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"/> |
| 3.11.36.4.10.2 | (L2) Ensure 'Set time limit for disconnected sessions' is set to 'Enabled: 1 minute' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11.36.4.11 | Temporary folders | | |
| 3.11.36.4.11.1 | (L1) Ensure 'Do not delete temp folders upon exit' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11.37 | RSS Feeds | | |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|--|--------------------------|--------------------------|
| | | Yes | No |
| 3.11.37.1 | (L1) Ensure 'Prevent downloading of enclosures' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11.38 | Security Center | | |
| 3.11.39 | Shutdown Options | | |
| 3.11.40 | Smart Card | | |
| 3.11.41 | Sound Recorder | | |
| 3.11.42 | Store | | |
| 3.11.42.1 | (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"/> |
| 3.11.42.2 | (L2) Ensure 'Turn off the Store application' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11.43 | Sync your settings | | |
| 3.11.44 | Tablet PC | | |
| 3.11.45 | Tenant Restrictions | | |
| 3.11.46 | Windows Calendar | | |
| 3.11.47 | Windows Color System | | |
| 3.11.48 | Windows Error Reporting | | |
| 3.11.49 | Windows Installer | | |
| 3.11.49.1 | (L2) Ensure 'Prevent Internet Explorer security prompt for Windows Installer scripts' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11.50 | Windows Logon Options | | |
| 3.11.50.1 | (L1) Ensure 'Sign-in and lock last interactive user automatically after a restart' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|---|--------------------------|--------------------------|
| | | Yes | No |
| 3.11.51 | Windows Media Digital Rights Management | | |
| 3.11.52 | Windows Media Player | | |
| 3.11.52.1 | Playback | | |
| 3.11.52.1.1 | (L2) Ensure 'Prevent Codec Download (User)' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11.53 | Windows Mobility Center | | |
| 3.11.54 | Windows PowerShell | | |
| 3.11.54.1 | (L1) Ensure 'Turn on PowerShell Script Block Logging' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11.54.2 | (L1) Ensure 'Turn on PowerShell Transcription' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11.55 | Windows Remote Management (WinRM) | | |
| 3.11.55.1 | WinRM Client | | |
| 3.11.55.1.1 | (L1) Ensure 'Allow Basic authentication' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11.55.1.2 | (L1) Ensure 'Allow unencrypted traffic' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11.55.1.3 | (L1) Ensure 'Disallow Digest authentication' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11.55.2 | WinRM Service | | |
| 3.11.55.2.1 | (L1) Ensure 'Allow Basic authentication' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11.55.2.2 | (L2) Ensure 'Allow remote server management through WinRM' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11.55.2.3 | (L1) Ensure 'Allow unencrypted traffic' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|---|--------------------------|--------------------------|
| | | Yes | No |
| 3.11.55.2.4 | (L1) Ensure 'Disallow WinRM from storing RunAs credentials' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11.56 | Windows Remote Shell | | |
| 3.11.56.1 | (L2) Ensure 'Allow Remote Shell Access' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 4 | Application Defaults | | |
| 5 | Auditing | | |
| 5.1 | (L1) Ensure 'Account Logon Audit Credential Validation' is set to 'Success and Failure' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2 | (L1) Ensure 'Account Logon Logoff Audit Account Lockout' is set to include 'Failure' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3 | (L1) Ensure 'Account Logon Logoff Audit Group Membership' is set to include 'Success' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4 | (L1) Ensure 'Account Logon Logoff Audit Logoff' is set to include 'Success' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.5 | (L1) Ensure 'Account Logon Logoff Audit Logon' is set to 'Success and Failure' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.6 | (L1) Ensure 'Account Management Audit Application Group Management' is set to 'Success and Failure' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.7 | (L1) Ensure 'Audit Authentication Policy Change' is set to include 'Success' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.8 | (L1) Ensure 'Audit Authorization Policy Change' is set to include 'Success' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.9 | (L1) Ensure 'Audit Changes to Audit Policy' is set to include 'Success' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.10 | (L1) Ensure 'Audit File Share Access' is set to 'Success and Failure' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|---|--------------------------|--------------------------|
| | | Yes | No |
| 5.11 | (L1) Ensure 'Audit Other Logon Logoff Events' is set to 'Success and Failure' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.12 | (L1) Ensure 'Audit Security Group Management' is set to include 'Success' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.13 | (L1) Ensure 'Audit Security System Extension' is set to include 'Success' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.14 | (L1) Ensure 'Audit Special Logon' is set to include 'Success' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.15 | (L1) Ensure 'Audit User Account Management' is set to 'Success and Failure' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.16 | (L1) Ensure 'Detailed Tracking Audit PNP Activity' is set to include 'Success' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.17 | (L1) Ensure 'Detailed Tracking Audit Process Creation' is set to include 'Success' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.18 | (L1) Ensure 'Object Access Audit Detailed File Share' is set to include 'Failure' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.19 | (L1) Ensure 'Object Access Audit Other Object Access Events' is set to 'Success and Failure' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.20 | (L1) Ensure 'Object Access Audit Removable Storage' is set to 'Success and Failure' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.21 | (L1) Ensure 'Policy Change Audit MPSSVC Rule Level Policy Change' is set to 'Success and Failure' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.22 | (L1) Ensure 'Policy Change Audit Other Policy Change Events' is set to include 'Failure' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.23 | (L1) Ensure 'Privilege Use Audit Sensitive Privilege Use' is set to 'Success and Failure' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.24 | (L1) Ensure 'System Audit I Psec Driver' is set to 'Success and Failure' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|--|--------------------------|--------------------------|
| | | Yes | No |
| 5.25 | (L1) Ensure 'System Audit Other System Events' is set to 'Success and Failure' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.26 | (L1) Ensure 'System Audit Security State Change' is set to include 'Success' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.27 | (L1) Ensure 'System Audit System Integrity' is set to 'Success and Failure' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 6 | Authentication | | |
| 7 | BitLocker | | |
| 8 | BITS | | |
| 9 | Bluetooth | | |
| 10 | Browser | | |
| 11 | Camera | | |
| 11.1 | (L2) Ensure 'Allow Camera' is set to 'Not allowed' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 12 | Cellular | | |
| 13 | Cloud Desktop | | |
| 14 | Config Refresh | | |
| 15 | Connectivity | | |
| 16 | Control Policy Conflict | | |
| 17 | Converters | | |
| 18 | Credential Providers | | |
| 19 | Cryptography | | |
| 20 | Data Protection | | |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|---|--------------------------|--------------------------|
| | | Yes | No |
| 21 | Defender | | |
| 21.1 | (L1) Ensure 'Allow Behavior Monitoring' is set to 'Allowed' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 21.2 | (L1) Ensure 'Allow Email Scanning' is set to 'Allowed' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 21.3 | (L1) Ensure 'Allow Full Scan Removable Drive Scanning' is set to 'Allowed' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 21.4 | (L1) Ensure 'Allow Realtime Monitoring' is set to 'Allowed' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 21.5 | (L1) Ensure 'Allow scanning of all downloaded files and attachments' is set to 'Allowed' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 21.6 | (L1) Ensure 'Allow Script Scanning' is set to 'Allowed' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 21.7 | (L1) Ensure 'Attack Surface Reduction rules' are configured (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 21.8 | (L2) Ensure 'Enable File Hash Computation' is set to 'Enable' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 21.9 | (L1) Ensure 'Enable Network Protection' is set to 'Enabled (block mode)' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 21.10 | (L1) Ensure 'PUA Protection' is set to 'PUA Protection on' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 22 | Delivery Optimization | | |
| 22.1 | (L1) Ensure 'DO Download Mode' is NOT set to 'HTTP blended with Internet Peering' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 23 | Device Guard | | |
| 23.1 | (NG) Ensure 'Enable Virtualization Based Security' is set to 'Enable virtualization based security' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|--|--------------------------|--------------------------|
| | | Yes | No |
| 23.2 | (NG) Ensure 'Require Platform Security Features' is set to 'Turns on VBS with Secure Boot' or higher (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 23.3 | (NG) Ensure 'Credential Guard' is set to 'Enabled with UEFI lock' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 23.4 | (NG) Ensure 'Configure System Guard Launch' is set to 'Unmanaged Enables Secure Launch if supported by hardware' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 24 | Device Lock | | |
| 24.1 | (L1) Ensure 'Alphanumeric Device Password Required' is set to 'Password, Numeric PIN, or Alphanumeric PIN required' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 24.2 | (L1) Ensure 'Device Password Expiration' is set to '365 or fewer days, but not 0' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 24.3 | (L1) Ensure 'Device Password History' is set to '24 or more password(s)' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 24.4 | (L1) Ensure 'Min Device Password Complex Characters' is set to 'Digits lowercase letters and uppercase letters are required' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 24.5 | (L1) Ensure 'Min Device Password Length' is set to '14 or more character(s)' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 24.6 | (L1) Ensure 'Minimum Password Age' is set to '1 or more day(s)' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 25 | Dma Guard | | |
| 26 | Eap | | |
| 27 | Education | | |
| 28 | Enterprise Cloud Print | | |
| 29 | eSIM | | |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|---|--------------------------|-------------------------------------|
| | | Yes | No |
| 30 | Experience | | |
| 30.1 | (L1) Ensure 'Allow Cortana' is set to 'Block' (Automated) | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 30.2 | (L2) Ensure 'Allow Windows Spotlight (User)' is set to 'Block' (Automated) | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 30.3 | (L1) Ensure 'Do not show feedback notifications' is set to 'Feedback notifications are disabled' (Automated) | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 31 | Exploit Guard | | |
| 32 | Federated Authentication | | |
| 33 | Feeds | | |
| 33.1 | (L2) Ensure 'Enable news and interests' is set to 'Not Allowed' (Automated) | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 34 | File Explorer | | |
| 35 | Firewall | | |
| 35.1 | (L1) Ensure 'Enable Domain Network Firewall' is set to 'True' (Automated) | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 35.2 | (L1) Ensure 'Enable Domain Network Firewall: Default Inbound Action for Domain Profile' is set to 'Block' (Automated) | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 35.3 | (L1) Ensure 'Enable Domain Network Firewall: Disable Inbound Notifications' is set to 'True' (Automated) | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 35.4 | (L1) Ensure 'Enable Private Network Firewall' is set to 'True' (Automated) | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 35.5 | (L1) Ensure 'Enable Private Network Firewall: Default Inbound Action for Private Profile' is set to 'Block' (Automated) | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 35.6 | (L1) Ensure 'Enable Private Network Firewall: Disable Inbound Notifications' is set to 'True' (Automated) | <input type="checkbox"/> | <input checked="" type="checkbox"/> |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|---|--------------------------|--------------------------|
| | | Yes | No |
| 35.7 | (L1) Ensure 'Enable Public Network Firewall' is set to 'True' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 35.8 | (L1) Ensure 'Enable Public Network Firewall: Allow Local Ipsec Policy Merge' is set to 'False' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 35.9 | (L1) Ensure 'Enable Public Network Firewall: Allow Local Policy Merge' is set to 'False' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 35.10 | (L1) Ensure 'Enable Public Network Firewall: Default Inbound Action for Public Profile' is set to 'Block' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 35.11 | (L1) Ensure 'Enable Public Network Firewall: Disable Inbound Notifications' is set to 'True' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 36 | FSLogix | | |
| 37 | Games | | |
| 38 | Handwriting | | |
| 39 | Human Presence | | |
| 40 | Kerberos | | |
| 41 | Kiosk Browser | | |
| 42 | Lanman Workstation | | |
| 42.1 | (L1) Ensure 'Enable insecure guest logons' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 43 | Licensing | | |
| 43.1 | (L2) Ensure 'Disallow KMS Client Online AVS Validation' is set to 'Allow' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 44 | List Sync | | |
| 45 | Local Policies Security Options | | |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|--|--------------------------|--------------------------|
| | | Yes | No |
| 45.1 | (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"/> |
| 45.2 | (L1) Ensure 'Accounts: Enable Guest account status' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 45.3 | (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"/> |
| 45.4 | (L1) Configure 'Accounts: Rename administrator account' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 45.5 | (L1) Configure 'Accounts: Rename guest account' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 45.6 | (L2) Ensure 'Devices: Prevent users from installing printer drivers when connecting to shared printers' is set to 'Enable' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 45.7 | (L1) Ensure 'Interactive logon: Do not display last signed-in' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 45.8 | (L1) Ensure 'Interactive logon: Do not require CTRL+ALT+DEL' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 45.9 | (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"/> |
| 45.10 | (L1) Configure 'Interactive logon: Message text for users attempting to log on' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 45.11 | (L1) Configure 'Interactive logon: Message title for users attempting to log on' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 45.12 | (L1) Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or higher (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 45.13 | (L1) Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|---|--------------------------|--------------------------|
| | | Yes | No |
| 45.14 | (L1) Ensure 'Microsoft network client: Digitally sign communications (if server agrees)' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 45.15 | (L1) Ensure 'Microsoft network client: Send unencrypted password to third-party SMB servers' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 45.16 | (L1) Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 45.17 | (L1) Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 45.18 | (L1) Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 45.19 | (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"/> |
| 45.20 | (L1) Ensure 'Network access: Restrict anonymous access to Named Pipes and Shares' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 45.21 | (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"/> |
| 45.22 | (L1) Ensure 'Network security: Allow Local System to use computer identity for NTLM' is set to 'Allow' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 45.23 | (L1) Ensure 'Network Security: Allow PKU2U authentication requests' is set to 'Block' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 45.24 | (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"/> |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|--|--------------------------|--------------------------|
| | | Yes | No |
| 45.25 | (L1) Ensure 'Network security: LAN Manager authentication level' is set to 'Send LM and NTLMv2 responses only. Refuse LM and NTLM' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 45.26 | (L1) Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' is set to 'Require NTLM and 128-bit encryption' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 45.27 | (L1) Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require NTLM and 128-bit encryption' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 45.28 | (L1) Ensure 'Network security: Restrict NTLM: Audit Incoming NTLM Traffic' is set to 'Enable auditing for all accounts' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 45.29 | (L1) Ensure 'User Account Control: Behavior of the elevation prompt for administrators' is set to 'Prompt for consent on the secure desktop' or higher (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 45.30 | (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"/> |
| 45.31 | (L1) Ensure 'User Account Control: Detect application installations and prompt for elevation' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 45.32 | (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"/> |
| 45.33 | (L1) Ensure 'User Account Control: Use Admin Approval Mode' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 45.34 | (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"/> |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|---|--------------------------|--------------------------|
| | | Yes | No |
| 45.35 | (L1) Ensure 'User Account Control: Run all administrators in Admin Approval Mode' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 45.36 | (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"/> |
| 46 | Lock Down | | |
| 47 | Memory Dump | | |
| 48 | Microsoft App Store | | |
| 48.1 | (L1) Ensure 'Allow apps from the Microsoft app store to auto update' is set to 'Allowed' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 48.2 | (L1) Ensure 'Allow Game DVR' is set to 'Block' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 48.3 | (L2) Ensure 'Disable Store Originated Apps' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 48.4 | (L1) Ensure 'MSI Allow user control over installs' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 48.5 | (L1) Ensure 'MSI Always install with elevated privileges' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 48.6 | (L1) Ensure 'MSI Always install with elevated privileges (User)' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 48.7 | (L1) Ensure 'Require Private Store Only' is set to 'Only Private store is enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 49 | Microsoft Defender for Endpoint | | |
| 50 | Mixed Reality | | |
| 51 | Network Isolation | | |
| 52 | Network List Manager | | |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|---|--------------------------|--------------------------|
| | | Yes | No |
| 53 | News and interests | | |
| 54 | Notifications | | |
| 55 | PDE | | |
| 56 | Power | | |
| 57 | Printer Provisioning | | |
| 58 | Privacy | | |
| 58.1 | (L2) Ensure 'Allow Cross Device Clipboard' is set to 'Block' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 58.2 | (L1) Ensure 'Allow Input Personalization' is set to 'Block' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 58.3 | (L2) Ensure 'Disable Advertising ID' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 58.4 | (L1) Ensure 'Let Apps Activate With Voice Above Lock' is set to 'Enabled: Force Deny' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 58.5 | (L2) Ensure 'Upload User Activities' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 59 | Remote Desktop | | |
| 60 | Search | | |
| 60.1 | (L2) Ensure 'Allow Cloud Search' is set to 'Not allowed' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 60.2 | (L1) Ensure 'Allow Indexing Encrypted Stores Or Items' is set to 'Block' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 60.3 | (L1) Ensure 'Allow Search To Use Location' is set to 'Block' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 61 | Security | | |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|--|--------------------------|--------------------------|
| | | Yes | No |
| 62 | Settings | | |
| 62.1 | (L2) Ensure 'Allow Online Tips' is set to 'Block' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 63 | Shared PC | | |
| 64 | Smart Screen | | |
| 65 | Speech | | |
| 66 | Storage | | |
| 67 | System | | |
| 67.1 | (L1) Ensure 'Allow Telemetry' is set to 'Basic' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 67.2 | (L2) Ensure 'Allow Font Providers' is set to 'Not allowed' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 67.3 | (L2) Ensure 'Disable One Drive File Sync' is set to 'Sync Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 68 | Task Manager | | |
| 69 | System Services | | |
| 69.1 | (L2) Ensure 'Bluetooth Audio Gateway Service (BTAGService)' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 69.2 | (L2) Ensure 'Bluetooth Support Service (bthserv)' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 69.3 | (L1) Ensure 'Computer Browser (Browser)' is set to 'Disabled' or 'Not Installed' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 69.4 | (L2) Ensure 'Downloaded Maps Manager (MapsBroker)' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 69.5 | (L2) Ensure 'Geolocation Service (lfsvc)' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|--|--------------------------|--------------------------|
| | | Yes | No |
| 69.6 | (L1) Ensure 'IIS Admin Service (IISADMIN)' is set to 'Disabled' or 'Not Installed' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 69.7 | (L1) Ensure 'Infrared monitor service (irmon)' is set to 'Disabled' or 'Not Installed' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 69.8 | (L1) Ensure 'Internet Connection Sharing (ICS) (SharedAccess)' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 69.9 | (L2) Ensure 'Link-Layer Topology Discovery Mapper (lltdsvc)' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 69.10 | (L1) Ensure 'LxssManager (LxssManager)' is set to 'Disabled' or 'Not Installed' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 69.11 | (L1) Ensure 'Microsoft FTP Service (FTPSVC)' is set to 'Disabled' or 'Not Installed' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 69.12 | (L2) Ensure 'Microsoft iSCSI Initiator Service (MSiSCSI)' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 69.13 | (L1) Ensure 'OpenSSH SSH Server (sshd)' is set to 'Disabled' or 'Not Installed' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 69.14 | (L2) Ensure 'Peer Name Resolution Protocol (PNRPPsvc)' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 69.15 | (L2) Ensure 'Peer Networking Grouping (p2psvc)' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 69.16 | (L2) Ensure 'Peer Networking Identity Manager (p2pimsvc)' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 69.17 | (L2) Ensure 'PNRP Machine Name Publication Service (PNRPAutoReg)' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 69.18 | (L2) Ensure 'Print Spooler (Spooler)' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 69.19 | (L2) Ensure 'Problem Reports and Solutions Control Panel Support (wercplsupport)' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|--|--------------------------|--------------------------|
| | | Yes | No |
| 69.20 | (L2) Ensure 'Remote Access Auto Connection Manager (RasAuto)' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 69.21 | (L2) Ensure 'Remote Desktop Configuration (SessionEnv)' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 69.22 | (L2) Ensure 'Remote Desktop Services (TermService)' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 69.23 | (L2) Ensure 'Remote Desktop Services UserMode Port Redirector (UmRdpService)' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 69.24 | (L1) Ensure 'Remote Procedure Call (RPC) Locator (RpcLocator)' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 69.25 | (L2) Ensure 'Remote Registry (RemoteRegistry)' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 69.26 | (L1) Ensure 'Routing and Remote Access (RemoteAccess)' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 69.27 | (L2) Ensure 'Server (LanmanServer)' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 69.28 | (L1) Ensure 'Simple TCP/IP Services (simptcp)' is set to 'Disabled' or 'Not Installed' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 69.29 | (L2) Ensure 'SNMP Service (SNMP)' is set to 'Disabled' or 'Not Installed' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 69.30 | (L1) Ensure 'Special Administration Console Helper (sacsrv)' is set to 'Disabled' or 'Not Installed' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 69.31 | (L1) Ensure 'SSDP Discovery (SSDPSRV)' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 69.32 | (L1) Ensure 'UPnP Device Host (upnphost)' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 69.33 | (L1) Ensure 'Web Management Service (WMSvc)' is set to 'Disabled' or 'Not Installed' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|--|--------------------------|--------------------------|
| | | Yes | No |
| 69.34 | (L2) Ensure 'Windows Error Reporting Service (WerSvc)' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 69.35 | (L2) Ensure 'Windows Event Collector (Webservice)' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 69.36 | (L1) Ensure 'Windows Media Player Network Sharing Service (WMPNetworkSvc)' is set to 'Disabled' or 'Not Installed' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 69.37 | (L1) Ensure 'Windows Mobile Hotspot Service (icssvc)' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 69.38 | (L2) Ensure 'Windows Push Notifications System Service (WpnService)' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 69.39 | (L2) Ensure 'Windows PushToInstall Service (PushToInstall)' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 69.40 | (L2) Ensure 'Windows Remote Management (WS-Management) (WinRM)' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 69.41 | (L1) Ensure 'World Wide Web Publishing Service (W3SVC)' is set to 'Disabled' or 'Not Installed' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 69.42 | (L1) Ensure 'Xbox Accessory Management Service (XboxGipSvc)' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 69.43 | (L1) Ensure 'Xbox Live Auth Manager (XblAuthManager)' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 69.44 | (L1) Ensure 'Xbox Live Game Save (XblGameSave)' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 69.45 | (L1) Ensure 'Xbox Live Networking Service (XboxNetApiSvc)' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 70 | Task Scheduler | | |
| 71 | Text Input | | |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|---|--------------------------|--------------------------|
| | | Yes | No |
| 72 | Time Language Settings | | |
| 73 | Troubleshooting | | |
| 74 | User Rights | | |
| 74.1 | (L1) Ensure 'Access Credential Manager As Trusted Caller' is set to 'No One' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 74.2 | (L1) Ensure 'Access From Network' is set to 'Administrators, Remote Desktop Users' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 74.3 | (L1) Ensure 'Act As Part Of The Operating System' is set to 'No One' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 74.4 | (L1) Ensure 'Allow Local Log On' is set to 'Administrators, Users' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 74.5 | (L1) Ensure 'Backup Files And Directories' is set to 'Administrators' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 74.6 | (L1) Ensure 'Change System Time' is set to 'Administrators, LOCAL SERVICE' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 74.7 | (L1) Ensure 'Create Global Objects' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 74.8 | (L1) Ensure 'Create Page File' is set to 'Administrators' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 74.9 | (L1) Ensure 'Create Permanent Shared Objects' is set to 'No One' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 74.10 | (L1) Configure 'Create Symbolic Links' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 74.11 | (L1) Ensure 'Create Token' is set to 'No One' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 74.12 | (L1) Ensure 'Debug Programs' is set to 'Administrators' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|--|--------------------------|--------------------------|
| | | Yes | No |
| 74.13 | (L1) Ensure 'Deny Access From Network' to include 'Guests, Local account' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 74.14 | (L1) Ensure 'Deny Local Log On' to include 'Guests' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 74.15 | (L1) Ensure 'Deny Remote Desktop Services Log On' to include 'Guests, Local account' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 74.16 | (L1) Ensure 'Enable Delegation' is set to 'No One' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 74.17 | (L1) Ensure 'Generate Security Audits' is set to 'LOCAL SERVICE, NETWORK SERVICE' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 74.18 | (L1) Ensure 'Impersonate Client' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 74.19 | (L1) Ensure 'Increase Scheduling Priority' is set to 'Administrators, Window Manager\Window Manager Group' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 74.20 | (L1) Ensure 'Load Unload Device Drivers' is set to 'Administrators' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 74.21 | (L1) Ensure 'Lock Memory' is set to 'No One' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 74.22 | (L1) Ensure 'Manage auditing and security log' is set to 'Administrators' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 74.23 | (L1) Ensure 'Manage Volume' is set to 'Administrators' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 74.24 | (L1) Ensure 'Modify Firmware Environment' is set to 'Administrators' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 74.25 | (L1) Ensure 'Modify Object Label' is set to 'No One' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|---|--------------------------|--------------------------|
| | | Yes | No |
| 74.26 | (L1) Ensure 'Profile Single Process' is set to 'Administrators' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 74.27 | (L1) Ensure 'Remote Shutdown' is set to 'Administrators' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 74.28 | (L1) Ensure 'Restore Files And Directories' is set to 'Administrators' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 74.29 | (L1) Ensure 'Take Ownership' is set to 'Administrators' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 75 | Virtualization Based Technology | | |
| 76 | Wi-Fi Settings | | |
| 77 | Widgets | | |
| 78 | Windows Defender Security Center | | |
| 78.1 | (L1) Ensure 'Disallow Exploit Protection Override' is set to '(Enable)' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 79 | Windows Hello For Business | | |
| 79.1 | (L1) Ensure 'Facial Features Use Enhanced Anti Spoofing' is set to 'true' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 79.2 | (L1) Ensure 'Minimum PIN Length' is set to '6 more character(s)' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 79.3 | (L1) Ensure 'Require Security Device' is set to 'true' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 80 | Windows Ink Workspace | | |
| 80.1 | (L2) Ensure 'Allow suggested apps in Windows Ink Workspace' is set to 'Block' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 80.2 | (L1) Ensure 'Allow Windows Ink Workspace' is set to 'Enabled: but the user can't access it above the lock screen' OR 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|--|--------------------------|--------------------------|
| | | Yes | No |
| 81 | Windows Logon | | |
| 82 | Windows Subsystem For Linux | | |
| 83 | Windows Update For Business | | |
| 83.1 | (L1) Ensure 'Allow Auto Update' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 83.2 | (L1) Ensure 'Defer Feature Updates Period in Days' is set to 'Enabled: 180 or more days' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 83.3 | (L1) Ensure 'Defer Quality Updates Period (Days)' is set to 'Enabled: 0 days' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 83.4 | (L1) Ensure 'Manage preview builds' is set to 'Disable Preview builds' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 83.5 | (L1) Ensure 'Scheduled Install Day' is set to 'Every day' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 83.6 | (L1) Ensure 'Block "Pause Updates" ability' is set to 'Block' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 84 | Wireless Display | | |
| 85 | Windows LAPS | | |
| 85.1 | (L1) Ensure 'Backup Directory' is set to 'Backup the password to Azure AD only' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 85.2 | (L1) Ensure 'Password Age Days' is set to 'Configured: 30 or fewer' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 85.3 | (L1) Ensure 'Password Complexity' is set to 'Large letters + small letters + numbers + special characters' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 85.4 | (L1) Ensure 'Password Length' is set to 'Configured: 15 or more' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|--|--------------------------|--------------------------|
| | | Yes | No |
| 85.5 | (L1) Ensure 'Post-authentication actions' is set to 'Reset the password and logoff the managed account' or higher (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 85.6 | (L1) Ensure 'Post Authentication Reset Delay' is set to 'Configured: 8 or fewer hours, but not 0' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 86 | Miscellaneous Recommendations | | |
| 86.1 | Custom Profile | | |
| 86.1.1 | (L2) Ensure 'Allow a Windows app to share application data between users' is set to 'Disabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 86.1.2 | (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"/> |
| 86.1.3 | (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"/> |
| 86.1.4 | (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"/> |
| 86.1.5 | (L1) Ensure 'Prevent non-admin users from installing packaged Windows apps' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 86.1.6 | (L2) Ensure 'Turn off location' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 86.1.7 | (L1) Ensure 'Turn off Microsoft consumer experiences' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 86.1.8 | (L2) Ensure 'Turn off notifications network usage' is set to 'Enabled' (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |

| | | |
|------------------|--------------|--|
| 1/12/2021 | 1.0.0 | Initial Public Release |
| 11/15/2022 | 1.1.0 | UPDATE - 18.9.39 (L2) Ensure 'Turn off location' is set to 'Enabled' Ticket # 15203 |
| 11/15/2022 | 1.1.0 | UPDATE - 18.9.45 (L1) Ensure 'Turn on behavior monitoring' is set to 'Enabled' Ticket # 15205 |
| 11/15/2022 | 1.1.0 | UPDATE - 18.9.45 (L1) Ensure 'Scan removable drives' is set to 'Enabled' Ticket # 15206 |
| 11/15/2022 | 1.1.0 | UPDATE - 18.9.45 (L1) Ensure 'Turn on e-mail scanning' is set to 'Enabled' (L1) Ensure 'Turn on e-mail scanning' is set to 'Enabled' Ticket # 15207 |
| 11/15/2022 | 1.1.0 | UPDATE - 1.1 (L1) Ensure 'Maximum password age' is set to '60 or fewer days, but not 0' TO 365 Ticket # 15687 |
| 11/15/2022 | 1.1.0 | REMOVE - (L1) Ensure 'Network access: Shares that can be accessed anonymously' is set to 'None' Ticket # 16519 |
| 11/15/2022 | 1.1.0 | UPDATE - 18.9.108 (L1) Ensure 'Select when Quality Updates are received' is set to 'Enabled: 0 days' TO registry value '0' Ticket # 16721 |
| 11/15/2022 | 1.1.0 | UPDATE - 18.9.108 (L1) Ensure 'Manage preview builds' is set to 'Enabled: Disable preview builds' to Registry value '0' Ticket # 16723 |
| 11/15/2022 | 1.1.0 | UPDATE - 18.9.108.2.1 (L1) Ensure 'Configure Automatic Updates' is set to 'Enabled' to Any except option 5 Ticket # 16725 |

| | | |
|------------|-------|---|
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or higher Ticket # 16741 |
| 11/15/2022 | 1.1.0 | REMOVE - Ensure 'Network access: Shares that can be accessed anonymously' is set to 'None' Ticket # 16742 |
| 11/15/2022 | 1.1.0 | ADD - Ensure LAPS AdmPwd GPO Extension / CSE is installed Ticket # 16743 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Do not allow password expiration time longer than required by policy' is set to 'Enabled' Ticket # 16744 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Enable Local Admin Password Management' is set to 'Enabled' Ticket # 16745 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Password Settings: Password Complexity' is set to 'Enabled: Large letters + small letters + numbers + special characters' Ticket # 16746 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Password Settings: Password Length' is set to 'Enabled: 15 or more' Ticket # 16748 |
| 11/15/2022 | 1.1.0 | REMOVE - (L1) Ensure 'Network access: Shares that can be accessed anonymously' is set to 'None' Ticket # 16519 |
| 11/15/2022 | 1.1.0 | UPDATE - 18.9.108 (L1) Ensure 'Select when Quality Updates are received' is set to 'Enabled: 0 days' TO registry value '0' Ticket # 16721 |

| | | |
|------------|-------|---|
| 11/15/2022 | 1.1.0 | UPDATE - 18.9.108 (L1) Ensure 'Manage preview builds' is set to 'Enabled: Disable preview builds' to Registry value '0' Ticket # 16723 |
| 11/15/2022 | 1.1.0 | UPDATE - 18.9.108.2.1 (L1) Ensure 'Configure Automatic Updates' is set to 'Enabled' to Any except option 5 Ticket # 16725 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or higher Ticket # 16741 |
| 11/15/2022 | 1.1.0 | REMOVE - Ensure 'Network access: Shares that can be accessed anonymously' is set to 'None' Ticket # 16742 |
| 11/15/2022 | 1.1.0 | ADD - Ensure LAPS AdmPwd GPO Extension / CSE is installed Ticket # 16743 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Do not allow password expiration time longer than required by policy' is set to 'Enabled' Ticket # 16744 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Enable Local Admin Password Management' is set to 'Enabled' Ticket # 16745 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Password Settings: Password Complexity' is set to 'Enabled: Large letters + small letters + numbers + special characters' Ticket # 16746 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Password Settings: Password Length' is set to 'Enabled: 15 or more' Ticket # 16748 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Password Settings: Password Age (Days)' is set to 'Enabled: 30 or fewer' Ticket # 16749 |

| | | |
|------------|-------|---|
| 11/15/2022 | 1.1.0 | ADD - Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled' Ticket # 16750 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'MSS: (DisableSavePassword) Prevent the dial-up password from being saved' is set to 'Enabled' Ticket # 16751 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds' is set to 'Enabled: 300,000 or 5 minutes (recommended)' Ticket # 16752 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' is set to 'Enabled' Ticket # 16753 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)' is set to 'Disabled' Ticket # 16754 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)' is set to 'Enabled: 5 or fewer seconds' Ticket # 16755 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted' is set to 'Enabled: 3' Ticket # 16756 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'MSS: (TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted' is set to 'Enabled: 3' Ticket # 16757 |
| 11/15/2022 | 1.1.0 | ADD - 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' Ticket # 16758 |

| | | |
|------------|-------|--|
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Turn off multicast name resolution' is set to 'Enabled' Ticket # 16759 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Turn on Mapper I/O (LLTDIO) driver' is set to 'Disabled' Ticket # 16760 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Turn on Responder (RSPNDR) driver' is set to 'Disabled' Ticket # 16761 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Require domain users to elevate when setting a network's location' is set to 'Enabled' Ticket # 16762 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Configuration of wireless settings using Windows Connect Now' is set to 'Disabled' Ticket # 16763 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Prohibit access of the Windows Connect Now wizards' is set to 'Enabled' Ticket # 16764 |
| 11/15/2022 | 1.1.0 | ADD - 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' Ticket # 16765 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Allow Print Spooler to accept client connections' is set to 'Disabled' Ticket # 16766 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Point and Print Restrictions: When installing drivers for a new connection' is set to 'Enabled: Show warning and elevation prompt' Ticket # 16767 |

| | | |
|------------|-------|--|
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Point and Print Restrictions: When updating drivers for an existing connection' is set to 'Enabled: Show warning and elevation prompt' Ticket # 16768 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Include command line in process creation events' is set to 'Enabled' Ticket # 16769 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Encryption Oracle Remediation' is set to 'Enabled: Force Updated Clients' Ticket # 16770 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Prevent device metadata retrieval from the Internet' is set to 'Enabled' Ticket # 16771 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Configure registry policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE' Ticket # 16773 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Configure registry policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE' Ticket # 16774 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Continue experiences on this device' is set to 'Disabled' Ticket # 16775 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Turn off background refresh of Group Policy' is set to 'Disabled' Ticket # 16776 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Turn off access to the Store' is set to 'Enabled' Ticket # 16777 |

| | | |
|------------|-------|--|
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com' is set to 'Enabled' Ticket # 16778 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Turn off Registration if URL connection is referring to Microsoft.com' is set to 'Enabled' Ticket # 16779 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Turn off Search Companion content file updates' is set to 'Enabled' Ticket # 16780 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Turn off the "Order Prints" picture task' is set to 'Enabled' Ticket # 16781 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Turn off the "Publish to Web" task for files and folders' is set to 'Enabled' Ticket # 16782 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Turn off the Windows Messenger Customer Experience Improvement Program' is set to 'Enabled' Ticket # 16783 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Turn off Windows Customer Experience Improvement Program' is set to 'Enabled' Ticket # 16784 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Support device authentication using certificate' is set to 'Enabled: Automatic' Ticket # 16785 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Disallow copying of user input methods to the system account for sign-in' is set to 'Enabled' Ticket # 16786 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Block user from showing account details on sign-in' is set to 'Enabled' Ticket # 16787 |

| | | |
|------------|-------|---|
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Enumerate local users on domain-joined computers' is set to 'Disabled' Ticket # 16788 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Allow network connectivity during connected-standby (on battery)' is set to 'Disabled' Ticket # 16789 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Allow network connectivity during connected-standby (plugged in)' is set to 'Disabled' Ticket # 16790 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Microsoft Support Diagnostic Tool: Turn on MSDT interactive communication with support provider' is set to 'Disabled' Ticket # 16791 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Enable Windows NTP Client' is set to 'Enabled' Ticket # 16792 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Enable Windows NTP Server' is set to 'Disabled' Ticket # 16793 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Prevent non-admin users from installing packaged Windows apps' is set to 'Enabled' Ticket # 16794 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Block launching Universal Windows apps with Windows Runtime API access from hosted content.' is set to 'Enabled' Ticket # 16795 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Prevent the use of security questions for local accounts' is set to 'Enabled' Ticket # 16796 |

| | | |
|------------|-------|---|
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Configure Authenticated Proxy usage for the Connected User Experience and Telemetry service' is set to 'Enabled: Disable Authenticated Proxy usage' Ticket # 16797 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Security: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' Ticket # 16798 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Setup: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' Ticket # 16799 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Setup: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' Ticket # 16800 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'System: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' Ticket # 16801 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Turn off shell protocol protected mode' is set to 'Disabled' Ticket # 16802 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Block all consumer Microsoft account user authentication' is set to 'Enabled' Ticket # 16803 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Configure local setting override for reporting to Microsoft MAPS' is set to 'Disabled' Ticket # 16804 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Join Microsoft MAPS' is set to 'Disabled' Ticket # 16805 |

| | | |
|------------|-------|---|
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Enable file hash computation feature' is set to 'Enabled' Ticket # 16806 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Scan all downloaded files and attachments' is set to 'Enabled' Ticket # 16807 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Turn off real-time protection' is set to 'Disabled' Ticket # 16808 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Configure Watson events' is set to 'Disabled' Ticket # 16809 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Turn off Push To Install service' is set to 'Enabled' Ticket # 16811 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Do not allow COM port redirection' is set to 'Enabled' Ticket # 16812 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Do not allow LPT port redirection' is set to 'Enabled' Ticket # 16813 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Do not allow supported Plug and Play device redirection' is set to 'Enabled' Ticket # 16814 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Require use of specific security layer for remote (RDP) connections' is set to 'Enabled: SSL' Ticket # 16815 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Require user authentication for remote connections by using Network Level Authentication' is set to 'Enabled' Ticket # 16816 |

| | | |
|------------|-------|---|
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Set time limit for active but idle Remote Desktop Services sessions' is set to 'Enabled: 15 minutes or less, but not Never (0)' Ticket # 16817 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Set time limit for disconnected sessions' is set to 'Enabled: 1 minute' Ticket # 16818 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Do not delete temp folders upon exit' is set to 'Disabled' Ticket # 16819 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Turn off the offer to update to the latest version of Windows' is set to 'Enabled' Ticket # 16820 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Turn off the Store application' is set to 'Enabled' Ticket # 16821 |
| 11/15/2022 | 1.1.0 | CHANGE - Ensure 'Turn on PowerShell Script Block Logging' is set to 'Disabled' TO Enabled Ticket # 16822 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Turn on PowerShell Transcription' is set to 'Disabled' Ticket # 16823 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Enable screen saver' is set to 'Enabled' Ticket # 16824 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Password protect the screen saver' is set to 'Enabled' Ticket # 16825 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Screen saver timeout' is set to 'Enabled: 900 seconds or fewer, but not 0' Ticket # 16826 |

| | | |
|------------|-------|---|
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Turn off Help Experience Improvement Program' is set to 'Enabled' Ticket # 16827 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Do not use diagnostic data for tailored experiences' is set to 'Enabled' Ticket # 16828 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Turn off all Windows spotlight features' is set to 'Enabled' Ticket # 16829 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Prevent users from sharing files within their profile.' is set to 'Enabled' Ticket # 16830 |
| 11/15/2022 | 1.1.0 | RENAME & UPDATE - 18.9.17 (L1) Ensure 'Allow Telemetry' TO (L1) Ensure 'Allow Diagnostic Data' Ticket # 16831 |
| 10/20/2023 | 2.0.0 | REMOVE - 2.3.4.1 (L1) Ensure 'Devices: Allowed to format and eject removable media' is set to 'Administrators and Interactive Users' Ticket # 15199 |
| 10/20/2023 | 2.0.0 | ADD - 18.9.39 (L1) 'Disable Internet Explorer 11 as a standalone browser' is set to 'Enabled: Always' 16403 |
| 10/20/2023 | 2.0.0 | CHANGE - 1.1 (L1) Ensure 'Password must meet complexity requirements' is set to 'Numbers, lowercase, uppercase and special characters required' TO 'Numbers and lowercase' Ticket# 16994 |
| 10/20/2023 | 2.0.0 | UPDATE - Section changes from Windows 11 Release 22H2 Administrative Templates Ticket# 17124 |

| | | |
|------------|-------|--|
| 10/20/2023 | 2.0.0 | UPDATE – 18.10.87 (L1) 'Turn on PowerShell Transcription' is set to 'Disabled' TO 'Enabled' Ticket# 17516 |
| 10/20/2023 | 2.0.0 | REMOVE - 2.3.1 (L1) Ensure 'Accounts: Administrator account status' is set to 'Disabled' Ticket# 17565 |
| 10/20/2023 | 2.0.0 | UPDATE - 18.10.43.6.1 (L1) Ensure 'Configure Attack Surface Reduction rules' with additional ASR rule for "Block abuse of exploited vulnerable signed drivers" Ticket # 17588 |
| 10/20/2023 | 2.0.0 | ADD - 2.2 (L1) Ensure 'Deny log on as a service' to include 'Guests' Ticket # 19376 |
| 10/20/2023 | 2.0.0 | ADD - 9.3 (L1) Ensure 'Windows Firewall: Public: Settings: Apply local connection security rules' is set to 'No' Ticket # 19377 |
| 10/20/2023 | 2.0.0 | ADD - 18.10.33 (L1) Ensure 'Prevent the computer from joining a homegroup' is set to 'Enabled' Ticket # 19379 |
| 10/20/2023 | 2.0.0 | ADD - 18.10.67 (L1) Ensure 'Turn off Automatic Download and Install of updates' is set to 'Disabled' Ticket # 19380 |
| 10/20/2023 | 2.0.0 | REMOVE - 19.7.7 (L1) Ensure 'Configure Windows spotlight on lock screen' is set to 'Disabled' Ticket #20127 |
| 10/20/2023 | 2.0.0 | REMOVE - 19.7.7 (L1) Ensure 'Do not suggest third-party content in Windows spotlight' is set to 'Enabled' Ticket #20128 |
| 10/20/2023 | 2.0.0 | REMOVE - 19.7.7 (L2) Ensure 'Do not use diagnostic data for tailored experiences' is set to 'Enabled' Ticket #20129 |

| | | |
|------------|-------|---|
| 10/20/2023 | 2.0.0 | REMOVE - 19.7.7. (L2) Ensure 'Turn off all Windows spotlight features' is set to 'Enabled' Ticket #20130 |
| 10/20/2023 | 2.0.0 | REMOVE 19.1.3 (L1) Ensure 'Enable screen saver' is set to 'Enabled' Ticket #20131 |
| 10/20/2023 | 2.0.0 | REMOVE 19.1.3 (L1) Ensure 'Password protect the screen saver' is set to 'Enabled' Ticket #20132 |
| 10/20/2023 | 2.0.0 | REMOVE 19.1.3 (L1) Ensure 'Screen saver timeout' is set to 'Enabled: 900 seconds or fewer, but not 0' Ticket #20133 |
| 10/20/2023 | 2.0.0 | REMOVE - 18.10 (L1) Ensure 'Download Mode' is NOT set to 'Enabled: Internet' Ticket #20134 |
| 02/23/2024 | 3.0.0 | ADD - (L1) Ensure 'Require Security Device' is set to 'true' Ticket #20804 |
| 02/23/2024 | 3.0.0 | ADD - (L1) Ensure 'Minimum PIN Length' is set to '6 more character(s)' Ticket #20803 |
| 02/23/2024 | 3.0.0 | ADD - (L1) Ensure 'Alphanumeric Device Password Required' is set to 'Password, Numeric PIN, or Alphanumeric PIN required' Ticket #20802 |
| 02/23/2024 | 3.0.0 | ADD - LAPS (L1) Ensure 'Post Authentication Reset Delay' is set to 'Configured: 8 or fewer hours, but not 0' Ticket #20728 |
| 02/23/2024 | 3.0.0 | ADD - LAPS (L1) Ensure 'Post-authentication actions' is set to 'Reset the password and logoff the managed account' or higher Ticket #20727 |

| | | |
|------------|-------|---|
| 02/23/2024 | 3.0.0 | ADD - LAPS (L1) Ensure 'Password Length' is set to 'Configured: 15 or more' Ticket #20726 |
| 02/23/2024 | 3.0.0 | ADD - LAPS (L1) Ensure 'Password Complexity' is set to 'Large letters + small letters + numbers + special characters' Ticket #20725 |
| 02/23/2024 | 3.0.0 | ADD - LAPS (L1) Ensure 'Password Age Days' is set to 'Configured: 30 or fewer' Ticket #20724 |
| 02/23/2024 | 3.0.0 | ADD - LAPS (L1) Ensure 'Backup Directory' is set to 'Backup the password to Azure AD only' Ticket #20723 |
| 02/23/2024 | 3.0.0 | REMOVE - Ensure 'Password Settings: Password Age (Days)' is set to 'Enabled: 30 or fewer' Ticket #20707 |
| 02/23/2024 | 3.0.0 | REMOVE - Ensure 'Password Settings: Password Length' is set to 'Enabled: 15 or more' Ticket #20706 |
| 02/23/2024 | 3.0.0 | REMOVE - Ensure 'Password Settings: Password Complexity' is set to 'Enabled: Large letters + small letters + numbers + special characters' Ticket #20705 |
| 02/23/2024 | 3.0.0 | REMOVE - Ensure 'Enable Local Admin Password Management' is set to 'Enabled' Ticket #20704 |
| 02/23/2024 | 3.0.0 | REMOVE - Ensure 'Do not allow password expiration time longer than required by policy' is set to 'Enabled' Ticket #20703 |
| 02/23/2024 | 3.0.0 | REMOVE - Ensure LAPS AdmPwd GPO Extension / CSE is installed Ticket #20702 |

| | | |
|------------|-------|---|
| 02/23/2024 | 3.0.0 | UPDATE - (L1) Ensure 'Disable One Drive File Sync' is set to 'Sync Disabled' TO L2 Ticket #20678 |
| 02/23/2024 | 3.0.0 | REMOVE - Ensure 'Configure Attack Surface Reduction rules' is set to 'Enabled' Ticket #20575 |
| 02/23/2024 | 3.0.0 | REMOVE - Ensure 'Windows Firewall: Public: Outbound connections' is set to 'Allow (default)' Ticket #20537 |
| 02/23/2024 | 3.0.0 | REMOVE - Ensure 'Windows Firewall: Private: Outbound connections' is set to 'Allow (default)' Ticket #20536 |
| 02/23/2024 | 3.0.0 | REMOVE - Ensure 'Windows Firewall: Domain: Outbound connections' is set to 'Allow (default)' Ticket #20535 |
| 02/23/2024 | 3.0.0 | REMOVE - Ensure 'Allow Message Service Cloud Sync' is set to 'Disabled' Ticket #20518 |
| 02/23/2024 | 3.0.0 | REMOVE - (L1) Ensure 'Toggle user control over Insider builds' is set to 'Disabled' Ticket #20283 |
| 02/23/2024 | 3.0.0 | REMOVE - Ensure 'Deny log on as a service' to include 'Guests' (Automated) Ticket #20218 |
| 02/23/2024 | 3.0.0 | ADD - (L1) Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require NTLM and 128-bit encryption' Ticket #20826 |
| 02/23/2024 | 3.0.0 | ADD - (L1) Ensure 'Network security: Restrict NTLM: Audit Incoming NTLM Traffic' is set to 'Enable auditing for all accounts' Ticket #20827 |

| | | |
|------------|-------|--|
| 02/23/2024 | 3.0.0 | ADD - System Services L1 and L2 Ticket #20828 |
| 02/23/2024 | 3.0.0 | ADD - (L1) Ensure 'Configure security policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE' Ticket #20854 |
| 02/23/2024 | 3.0.0 | ADD - (L1) Ensure 'Configure security policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE' Ticket #20855 |
| 02/23/2024 | 3.0.0 | ADD - (L1) Ensure 'Facial Features Use Enhanced Anti Spoofing' is set to 'true' Ticket #20856 |
| 02/23/2024 | 3.0.0 | ADD - (BL) Ensure 'Allow enhanced PINs for startup' is set to 'Enabled' Ticket #20857 |
| 02/23/2024 | 3.0.0 | ADD - (L2) Ensure 'Allow Camera' is set to 'Not Allowed' Ticket #20858 |
| 02/23/2024 | 3.0.0 | ADD - (L1) Ensure 'DO Download Mode' is NOT set to 'Enabled: Internet' Ticket #20863 |
| 02/23/2024 | 3.0.0 | ADD - (L1) Ensure 'Allow Script Scanning' is set to 'Allowed' Ticket #20864 |
| 02/23/2024 | 3.0.0 | ADD - (L2) Ensure 'Enable news and interests' is set to 'Not Allowed' Ticket #20865 |
| 02/23/2024 | 3.0.0 | ADD - (L2) Ensure 'Prevent Internet Explorer security prompt for Windows Installer scripts' is set to 'Disabled' Ticket #20871 |

| | | |
|------------|-------|--|
| 02/23/2024 | 3.0.0 | ADD - (L1) Ensure 'Select when Preview Builds and Feature Updates are received' is set to 'Enabled: 180 or more days' Ticket #20872 |
| 02/23/2024 | 3.0.0 | ADD - (L1) Ensure 'Enable screen saver (User)' is set to 'Enabled' Ticket #20873 |
| 02/23/2024 | 3.0.0 | ADD - (L2) Ensure 'Allow Windows Spotlight (User)' is set to 'Block' Ticket #20874 |
| 02/23/2024 | 3.0.0 | ADD - (L2) Ensure 'Prevent Codec Download' is set to 'Enabled' Ticket #20876 |

Appendix: Change History

| Date | Version | Changes for this version |
|------------|---------|--|
| 1/12/2021 | 1.0.0 | Initial Public Release |
| 11/15/2022 | 1.1.0 | UPDATE - 18.9.39 (L2) Ensure 'Turn off location' is set to 'Enabled' Ticket # 15203 |
| 11/15/2022 | 1.1.0 | UPDATE - 18.9.45 (L1) Ensure 'Turn on behavior monitoring' is set to 'Enabled' Ticket # 15205 |
| 11/15/2022 | 1.1.0 | UPDATE - 18.9.45 (L1) Ensure 'Scan removable drives' is set to 'Enabled' Ticket # 15206 |
| 11/15/2022 | 1.1.0 | UPDATE - 18.9.45 (L1) Ensure 'Turn on e-mail scanning' is set to 'Enabled' (L1) Ensure 'Turn on e-mail scanning' is set to 'Enabled' Ticket # 15207 |
| 11/15/2022 | 1.1.0 | UPDATE - 1.1 (L1) Ensure 'Maximum password age' is set to '60 or fewer days, but not 0' TO 365 Ticket # 15687 |
| 11/15/2022 | 1.1.0 | REMOVE - (L1) Ensure 'Network access: Shares that can be accessed anonymously' is set to 'None' Ticket # 16519 |
| 11/15/2022 | 1.1.0 | UPDATE - 18.9.108 (L1) Ensure 'Select when Quality Updates are received' is set to 'Enabled: 0 days' TO registry value '0' Ticket # 16721 |
| 11/15/2022 | 1.1.0 | UPDATE - 18.9.108 (L1) Ensure 'Manage preview builds' is set to 'Enabled: Disable preview builds' to Registry value '0' Ticket # 16723 |

| Date | Version | Changes for this version |
|-------------|----------------|---|
| 11/15/2022 | 1.1.0 | UPDATE - 18.9.108.2.1 (L1) Ensure 'Configure Automatic Updates' is set to 'Enabled' to Any except option 5 Ticket # 16725 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or higher Ticket # 16741 |
| 11/15/2022 | 1.1.0 | REMOVE - Ensure 'Network access: Shares that can be accessed anonymously' is set to 'None' Ticket # 16742 |
| 11/15/2022 | 1.1.0 | ADD - Ensure LAPS AdmPwd GPO Extension / CSE is installed Ticket # 16743 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Do not allow password expiration time longer than required by policy' is set to 'Enabled' Ticket # 16744 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Enable Local Admin Password Management' is set to 'Enabled' Ticket # 16745 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Password Settings: Password Complexity' is set to 'Enabled: Large letters + small letters + numbers + special characters' Ticket # 16746 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Password Settings: Password Length' is set to 'Enabled: 15 or more' Ticket # 16748 |
| 11/15/2022 | 1.1.0 | REMOVE - (L1) Ensure 'Network access: Shares that can be accessed anonymously' is set to 'None' Ticket # 16519 |

| Date | Version | Changes for this version |
|-------------|----------------|---|
| 11/15/2022 | 1.1.0 | UPDATE - 18.9.108 (L1) Ensure 'Select when Quality Updates are received' is set to 'Enabled: 0 days' TO registry value '0' Ticket # 16721 |
| 11/15/2022 | 1.1.0 | UPDATE - 18.9.108 (L1) Ensure 'Manage preview builds' is set to 'Enabled: Disable preview builds' to Registry value '0' Ticket # 16723 |
| 11/15/2022 | 1.1.0 | UPDATE - 18.9.108.2.1 (L1) Ensure 'Configure Automatic Updates' is set to 'Enabled' to Any except option 5 Ticket # 16725 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or higher Ticket # 16741 |
| 11/15/2022 | 1.1.0 | REMOVE - Ensure 'Network access: Shares that can be accessed anonymously' is set to 'None' Ticket # 16742 |
| 11/15/2022 | 1.1.0 | ADD - Ensure LAPS AdmPwd GPO Extension / CSE is installed Ticket # 16743 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Do not allow password expiration time longer than required by policy' is set to 'Enabled' Ticket # 16744 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Enable Local Admin Password Management' is set to 'Enabled' Ticket # 16745 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Password Settings: Password Complexity' is set to 'Enabled: Large letters + small letters + numbers + special characters' Ticket # 16746 |

| Date | Version | Changes for this version |
|-------------|----------------|---|
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Password Settings: Password Length' is set to 'Enabled: 15 or more' Ticket # 16748 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Password Settings: Password Age (Days)' is set to 'Enabled: 30 or fewer' Ticket # 16749 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled' Ticket # 16750 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'MSS: (DisableSavePassword) Prevent the dial-up password from being saved' is set to 'Enabled' Ticket # 16751 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds' is set to 'Enabled: 300,000 or 5 minutes (recommended)' Ticket # 16752 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' is set to 'Enabled' Ticket # 16753 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)' is set to 'Disabled' Ticket # 16754 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)' is set to 'Enabled: 5 or fewer seconds' Ticket # 16755 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted' is set to 'Enabled: 3' Ticket # 16756 |

| Date | Version | Changes for this version |
|-------------|----------------|---|
| 11/15/2022 | 1.1.0 | ADD - Ensure 'MSS: (TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted' is set to 'Enabled: 3' Ticket # 16757 |
| 11/15/2022 | 1.1.0 | ADD - 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' Ticket # 16758 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Turn off multicast name resolution' is set to 'Enabled' Ticket # 16759 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Turn on Mapper I/O (LLTDIO) driver' is set to 'Disabled' Ticket # 16760 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Turn on Responder (RSPNDR) driver' is set to 'Disabled' Ticket # 16761 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Require domain users to elevate when setting a network's location' is set to 'Enabled' Ticket # 16762 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Configuration of wireless settings using Windows Connect Now' is set to 'Disabled' Ticket # 16763 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Prohibit access of the Windows Connect Now wizards' is set to 'Enabled' Ticket # 16764 |
| 11/15/2022 | 1.1.0 | ADD - 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' Ticket # 16765 |

| Date | Version | Changes for this version |
|-------------|----------------|--|
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Allow Print Spooler to accept client connections' is set to 'Disabled' Ticket # 16766 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Point and Print Restrictions: When installing drivers for a new connection' is set to 'Enabled: Show warning and elevation prompt' Ticket # 16767 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Point and Print Restrictions: When updating drivers for an existing connection' is set to 'Enabled: Show warning and elevation prompt' Ticket # 16768 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Include command line in process creation events' is set to 'Enabled' Ticket # 16769 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Encryption Oracle Remediation' is set to 'Enabled: Force Updated Clients' Ticket # 16770 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Prevent device metadata retrieval from the Internet' is set to 'Enabled' Ticket # 16771 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Configure registry policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE' Ticket # 16773 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Configure registry policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE' Ticket # 16774 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Continue experiences on this device' is set to 'Disabled' Ticket # 16775 |

| Date | Version | Changes for this version |
|-------------|----------------|--|
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Turn off background refresh of Group Policy' is set to 'Disabled' Ticket # 16776 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Turn off access to the Store' is set to 'Enabled' Ticket # 16777 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com' is set to 'Enabled' Ticket # 16778 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Turn off Registration if URL connection is referring to Microsoft.com' is set to 'Enabled' Ticket # 16779 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Turn off Search Companion content file updates' is set to 'Enabled' Ticket # 16780 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Turn off the "Order Prints" picture task' is set to 'Enabled' Ticket # 16781 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Turn off the "Publish to Web" task for files and folders' is set to 'Enabled' Ticket # 16782 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Turn off the Windows Messenger Customer Experience Improvement Program' is set to 'Enabled' Ticket # 16783 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Turn off Windows Customer Experience Improvement Program' is set to 'Enabled' Ticket # 16784 |

| Date | Version | Changes for this version |
|-------------|----------------|---|
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Support device authentication using certificate' is set to 'Enabled: Automatic' Ticket # 16785 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Disallow copying of user input methods to the system account for sign-in' is set to 'Enabled' Ticket # 16786 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Block user from showing account details on sign-in' is set to 'Enabled' Ticket # 16787 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Enumerate local users on domain-joined computers' is set to 'Disabled' Ticket # 16788 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Allow network connectivity during connected-standby (on battery)' is set to 'Disabled' Ticket # 16789 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Allow network connectivity during connected-standby (plugged in)' is set to 'Disabled' Ticket # 16790 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Microsoft Support Diagnostic Tool: Turn on MSDT interactive communication with support provider' is set to 'Disabled' Ticket # 16791 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Enable Windows NTP Client' is set to 'Enabled' Ticket # 16792 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Enable Windows NTP Server' is set to 'Disabled' Ticket # 16793 |

| Date | Version | Changes for this version |
|-------------|----------------|---|
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Prevent non-admin users from installing packaged Windows apps' is set to 'Enabled' Ticket # 16794 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Block launching Universal Windows apps with Windows Runtime API access from hosted content.' is set to 'Enabled' Ticket # 16795 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Prevent the use of security questions for local accounts' is set to 'Enabled' Ticket # 16796 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Configure Authenticated Proxy usage for the Connected User Experience and Telemetry service' is set to 'Enabled: Disable Authenticated Proxy usage' Ticket # 16797 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Security: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' Ticket # 16798 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Setup: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' Ticket # 16799 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Setup: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' Ticket # 16800 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'System: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' Ticket # 16801 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Turn off shell protocol protected mode' is set to 'Disabled' Ticket # 16802 |

| Date | Version | Changes for this version |
|-------------|----------------|--|
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Block all consumer Microsoft account user authentication' is set to 'Enabled' Ticket # 16803 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Configure local setting override for reporting to Microsoft MAPS' is set to 'Disabled' Ticket # 16804 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Join Microsoft MAPS' is set to 'Disabled' Ticket # 16805 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Enable file hash computation feature' is set to 'Enabled' Ticket # 16806 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Scan all downloaded files and attachments' is set to 'Enabled' Ticket # 16807 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Turn off real-time protection' is set to 'Disabled' Ticket # 16808 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Configure Watson events' is set to 'Disabled' Ticket # 16809 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Turn off Push To Install service' is set to 'Enabled' Ticket # 16811 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Do not allow COM port redirection' is set to 'Enabled' Ticket # 16812 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Do not allow LPT port redirection' is set to 'Enabled' Ticket # 16813 |

| Date | Version | Changes for this version |
|-------------|----------------|---|
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Do not allow supported Plug and Play device redirection' is set to 'Enabled' Ticket # 16814 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Require use of specific security layer for remote (RDP) connections' is set to 'Enabled: SSL' Ticket # 16815 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Require user authentication for remote connections by using Network Level Authentication' is set to 'Enabled' Ticket # 16816 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Set time limit for active but idle Remote Desktop Services sessions' is set to 'Enabled: 15 minutes or less, but not Never (0)' Ticket # 16817 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Set time limit for disconnected sessions' is set to 'Enabled: 1 minute' Ticket # 16818 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Do not delete temp folders upon exit' is set to 'Disabled' Ticket # 16819 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Turn off the offer to update to the latest version of Windows' is set to 'Enabled' Ticket # 16820 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Turn off the Store application' is set to 'Enabled' Ticket # 16821 |
| 11/15/2022 | 1.1.0 | CHANGE - Ensure 'Turn on PowerShell Script Block Logging' is set to 'Disabled' TO Enabled Ticket # 16822 |

| Date | Version | Changes for this version |
|-------------|----------------|--|
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Turn on PowerShell Transcription' is set to 'Disabled' Ticket # 16823 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Enable screen saver' is set to 'Enabled' Ticket # 16824 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Password protect the screen saver' is set to 'Enabled' Ticket # 16825 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Screen saver timeout' is set to 'Enabled: 900 seconds or fewer, but not 0' Ticket # 16826 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Turn off Help Experience Improvement Program' is set to 'Enabled' Ticket # 16827 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Do not use diagnostic data for tailored experiences' is set to 'Enabled' Ticket # 16828 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Turn off all Windows spotlight features' is set to 'Enabled' Ticket # 16829 |
| 11/15/2022 | 1.1.0 | ADD - Ensure 'Prevent users from sharing files within their profile.' is set to 'Enabled' Ticket # 16830 |
| 11/15/2022 | 1.1.0 | RENAME & UPDATE - 18.9.17 (L1) Ensure 'Allow Telemetry' TO (L1) Ensure 'Allow Diagnostic Data' Ticket # 16831 |
| 10/20/2023 | 2.0.0 | REMOVE - 2.3.4.1 (L1) Ensure 'Devices: Allowed to format and eject removable media' is set to 'Administrators and Interactive Users' Ticket # 15199 |

| Date | Version | Changes for this version |
|-------------|----------------|---|
| 10/20/2023 | 2.0.0 | ADD - 18.9.39 (L1) 'Disable Internet Explorer 11 as a standalone browser' is set to 'Enabled: Always' 16403 |
| 10/20/2023 | 2.0.0 | CHANGE - 1.1 (L1) Ensure 'Password must meet complexity requirements' is set to 'Numbers, lowercase, uppercase and special characters required' TO 'Numbers and lowercase' Ticket# 16994 |
| 10/20/2023 | 2.0.0 | UPDATE - Section changes from Windows 11 Release 22H2 Administrative Templates Ticket# 17124 |
| 10/20/2023 | 2.0.0 | UPDATE – 18.10.87 (L1) 'Turn on PowerShell Transcription' is set to 'Disabled' TO 'Enabled' Ticket# 17516 |
| 10/20/2023 | 2.0.0 | REMOVE - 2.3.1 (L1) Ensure 'Accounts: Administrator account status' is set to 'Disabled' Ticket# 17565 |
| 10/20/2023 | 2.0.0 | UPDATE - 18.10.43.6.1 (L1) Ensure 'Configure Attack Surface Reduction rules' with additional ASR rule for "Block abuse of exploited vulnerable signed drivers" Ticket # 17588 |
| 10/20/2023 | 2.0.0 | ADD - 2.2 (L1) Ensure 'Deny log on as a service' to include 'Guests' Ticket # 19376 |
| 10/20/2023 | 2.0.0 | ADD - 9.3 (L1) Ensure 'Windows Firewall: Public: Settings: Apply local connection security rules' is set to 'No' Ticket # 19377 |
| 10/20/2023 | 2.0.0 | ADD - 18.10.33 (L1) Ensure 'Prevent the computer from joining a homegroup' is set to 'Enabled' Ticket # 19379 |

| Date | Version | Changes for this version |
|-------------|----------------|--|
| 10/20/2023 | 2.0.0 | ADD - 18.10.67 (L1) Ensure 'Turn off Automatic Download and Install of updates' is set to 'Disabled' Ticket # 19380 |
| 10/20/2023 | 2.0.0 | REMOVE - 19.7.7 (L1) Ensure 'Configure Windows spotlight on lock screen' is set to 'Disabled' Ticket #20127 |
| 10/20/2023 | 2.0.0 | REMOVE - 19.7.7 (L1) Ensure 'Do not suggest third-party content in Windows spotlight' is set to 'Enabled' Ticket #20128 |
| 10/20/2023 | 2.0.0 | REMOVE - 19.7.7 (L2) Ensure 'Do not use diagnostic data for tailored experiences' is set to 'Enabled' Ticket #20129 |
| 10/20/2023 | 2.0.0 | REMOVE - 19.7.7. (L2) Ensure 'Turn off all Windows spotlight features' is set to 'Enabled' Ticket #20130 |
| 10/20/2023 | 2.0.0 | REMOVE 19.1.3 (L1) Ensure 'Enable screen saver' is set to 'Enabled' Ticket #20131 |
| 10/20/2023 | 2.0.0 | REMOVE 19.1.3 (L1) Ensure 'Password protect the screen saver' is set to 'Enabled' Ticket #20132 |
| 10/20/2023 | 2.0.0 | REMOVE 19.1.3 (L1) Ensure 'Screen saver timeout' is set to 'Enabled: 900 seconds or fewer, but not 0' Ticket #20133 |
| 10/20/2023 | 2.0.0 | REMOVE - 18.10 (L1) Ensure 'Download Mode' is NOT set to 'Enabled: Internet' Ticket #20134 |
| 02/23/2024 | 3.0.0 | ADD - (L1) Ensure 'Require Security Device' is set to 'true' Ticket #20804 |

| Date | Version | Changes for this version |
|-------------|----------------|---|
| 02/23/2024 | 3.0.0 | ADD - (L1) Ensure 'Minimum PIN Length' is set to '6 more character(s)' Ticket #20803 |
| 02/23/2024 | 3.0.0 | ADD - (L1) Ensure 'Alphanumeric Device Password Required' is set to 'Password, Numeric PIN, or Alphanumeric PIN required' Ticket #20802 |
| 02/23/2024 | 3.0.0 | ADD - LAPS (L1) Ensure 'Post Authentication Reset Delay' is set to 'Configured: 8 or fewer hours, but not 0' Ticket #20728 |
| 02/23/2024 | 3.0.0 | ADD - LAPS (L1) Ensure 'Post-authentication actions' is set to 'Reset the password and logoff the managed account' or higher Ticket #20727 |
| 02/23/2024 | 3.0.0 | ADD - LAPS (L1) Ensure 'Password Length' is set to 'Configured: 15 or more' Ticket #20726 |
| 02/23/2024 | 3.0.0 | ADD - LAPS (L1) Ensure 'Password Complexity' is set to 'Large letters + small letters + numbers + special characters' Ticket #20725 |
| 02/23/2024 | 3.0.0 | ADD - LAPS (L1) Ensure 'Password Age Days' is set to 'Configured: 30 or fewer' Ticket #20724 |
| 02/23/2024 | 3.0.0 | ADD - LAPS (L1) Ensure 'Backup Directory' is set to 'Backup the password to Azure AD only' Ticket #20723 |
| 02/23/2024 | 3.0.0 | REMOVE - Ensure 'Password Settings: Password Age (Days)' is set to 'Enabled: 30 or fewer' Ticket #20707 |

| Date | Version | Changes for this version |
|-------------|----------------|---|
| 02/23/2024 | 3.0.0 | REMOVE - Ensure 'Password Settings: Password Length' is set to 'Enabled: 15 or more' Ticket #20706 |
| 02/23/2024 | 3.0.0 | REMOVE - Ensure 'Password Settings: Password Complexity' is set to 'Enabled: Large letters + small letters + numbers + special characters' Ticket #20705 |
| 02/23/2024 | 3.0.0 | REMOVE - Ensure 'Enable Local Admin Password Management' is set to 'Enabled' Ticket #20704 |
| 02/23/2024 | 3.0.0 | REMOVE - Ensure 'Do not allow password expiration time longer than required by policy' is set to 'Enabled' Ticket #20703 |
| 02/23/2024 | 3.0.0 | REMOVE - Ensure LAPS AdmPwd GPO Extension / CSE is installed Ticket #20702 |
| 02/23/2024 | 3.0.0 | UPDATE - (L1) Ensure 'Disable One Drive File Sync' is set to 'Sync Disabled' TO L2 Ticket #20678 |
| 02/23/2024 | 3.0.0 | REMOVE - Ensure 'Configure Attack Surface Reduction rules' is set to 'Enabled' Ticket #20575 |
| 02/23/2024 | 3.0.0 | REMOVE - Ensure 'Windows Firewall: Public: Outbound connections' is set to 'Allow (default)' Ticket #20537 |
| 02/23/2024 | 3.0.0 | REMOVE - Ensure 'Windows Firewall: Private: Outbound connections' is set to 'Allow (default)' Ticket #20536 |

| Date | Version | Changes for this version |
|-------------|----------------|---|
| 02/23/2024 | 3.0.0 | REMOVE - Ensure 'Windows Firewall: Domain: Outbound connections' is set to 'Allow (default)' Ticket #20535 |
| 02/23/2024 | 3.0.0 | REMOVE - Ensure 'Allow Message Service Cloud Sync' is set to 'Disabled' Ticket #20518 |
| 02/23/2024 | 3.0.0 | REMOVE - (L1) Ensure 'Toggle user control over Insider builds' is set to 'Disabled' Ticket #20283 |
| 02/23/2024 | 3.0.0 | REMOVE - Ensure 'Deny log on as a service' to include 'Guests' (Automated) Ticket #20218 |
| 02/23/2024 | 3.0.0 | ADD - (L1) Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require NTLM and 128-bit encryption' Ticket #20826 |
| 02/23/2024 | 3.0.0 | ADD - (L1) Ensure 'Network security: Restrict NTLM: Audit Incoming NTLM Traffic' is set to 'Enable auditing for all accounts' Ticket #20827 |
| 02/23/2024 | 3.0.0 | ADD - System Services L1 and L2 Ticket #20828 |
| 02/23/2024 | 3.0.0 | ADD - (L1) Ensure 'Configure security policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE' Ticket #20854 |
| 02/23/2024 | 3.0.0 | ADD - (L1) Ensure 'Configure security policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE' Ticket #20855 |

| Date | Version | Changes for this version |
|-------------|----------------|--|
| 02/23/2024 | 3.0.0 | ADD - (L1) Ensure 'Facial Features Use Enhanced Anti Spoofing' is set to 'true' Ticket #20856 |
| 02/23/2024 | 3.0.0 | ADD - (BL) Ensure 'Allow enhanced PINs for startup' is set to 'Enabled' Ticket #20857 |
| 02/23/2024 | 3.0.0 | ADD - (L2) Ensure 'Allow Camera' is set to 'Not Allowed' Ticket #20858 |
| 02/23/2024 | 3.0.0 | ADD - (L1) Ensure 'DO Download Mode' is NOT set to 'Enabled: Internet' Ticket #20863 |
| 02/23/2024 | 3.0.0 | ADD - (L1) Ensure 'Allow Script Scanning' is set to 'Allowed' Ticket #20864 |
| 02/23/2024 | 3.0.0 | ADD - (L2) Ensure 'Enable news and interests' is set to 'Not Allowed' Ticket #20865 |
| 02/23/2024 | 3.0.0 | ADD - (L2) Ensure 'Prevent Internet Explorer security prompt for Windows Installer scripts' is set to 'Disabled' Ticket #20871 |
| 02/23/2024 | 3.0.0 | ADD - (L1) Ensure 'Select when Preview Builds and Feature Updates are received' is set to 'Enabled: 180 or more days' Ticket #20872 |
| 02/23/2024 | 3.0.0 | ADD - (L1) Ensure 'Enable screen saver (User)' is set to 'Enabled' Ticket #20873 |
| 02/23/2024 | 3.0.0 | ADD - (L2) Ensure 'Allow Windows Spotlight (User)' is set to 'Block' Ticket #20874 |

| Date | Version | Changes for this version |
|------------|---------|---|
| 02/23/2024 | 3.0.0 | ADD - (L2) Ensure 'Prevent Codec Download' is set to 'Enabled' Ticket #20876 |
| 03/01/2024 | 3.0.1 | UPDATE - Bug Fix v3.0.1 Remediation Sections |