CIS Benchmarks

Security Configuration Assessment Report for MOTUNUI

CIS-CAT Host IP Address: 10.0.2.15

CIS Microsoft Windows 10 Enterprise Release 1803 Benchmark v1.5.0

Level 1 (L1) - Corporate/Enterprise Environment (general use)
Monday, August 12 2019 20:19:11
Assessment Duration: 4 minutes, 6 seconds

Report generated by the Center for Internet Security's Configuration Assessment Tool (CIS-CAT) v3.0.56.
For further information, please visit The Center for Internet Security or send an e-mail to feedback@cisecurity.org.

Summary

Description	Tests				Scoring		
	Pass	Fail	Error	Unkn.	Score	Max	Percent
1 Account Policies	**2**	**5**	**0**	**2**	**2.0**	**9.0**	**22%**
1.1 Password Policy	0	4	0	2	0.0	6.0	0%
1.2 Account Lockout Policy	2	1	0	0	2.0	3.0	67%
2 Local Policies	**59**	**40**	**0**	**1**	**59.0**	**100.0**	**59%**
2.1 Audit Policy	0	0	0	0	0.0	0.0	0%
2.2 User Rights Assignment	26	11	0	0	26.0	37.0	70%
2.3 Security Options	33	29	0	1	33.0	63.0	52%
2.3.1 Accounts	2	4	0	0	2.0	6.0	33%
2.3.2 Audit	1	1	0	0	1.0	2.0	50%
2.3.3 DCOM	0	0	0	0	0.0	0.0	0%
2.3.4 Devices	0	1	0	0	0.0	1.0	0%
2.3.5 Domain controller	0	0	0	0	0.0	0.0	0%
2.3.6 Domain member	6	0	0	0	6.0	6.0	100%
2.3.7 Interactive logon	1	6	0	0	1.0	7.0	14%
2.3.8 Microsoft network client	2	1	0	0	2.0	3.0	67%
2.3.9 Microsoft network server	2	3	0	0	2.0	5.0	40%
2.3.10 Network access	8	3	0	1	8.0	12.0	67%
2.3.11 Network security	3	7	0	0	3.0	10.0	30%
2.3.12 Recovery console	0	0	0	0	0.0	0.0	0%
2.3.13 Shutdown	0	0	0	0	0.0	0.0	0%
2.3.14 System cryptography	0	0	0	0	0.0	0.0	0%
2.3.15 System objects	2	0	0	0	2.0	2.0	100%
2.3.16 System settings	0	0	0	0	0.0	0.0	0%
2.3.17 User Account Control	6	3	0	0	6.0	9.0	67%
3 Event Log	**0**	**0**	**0**	**0**	**0.0**	**0.0**	**0%**
4 Restricted Groups	**0**	**0**	**0**	**0**	**0.0**	**0.0**	**0%**
5 System Services	**8**	**13**	**0**	**0**	**8.0**	**21.0**	**38%**
6 Registry	**0**	**0**	**0**	**0**	**0.0**	**0.0**	**0%**
7 File System	**0**	**0**	**0**	**0**	**0.0**	**0.0**	**0%**
8 Wired Network (IEEE 802.3) Policies	**0**	**0**	**0**	**0**	**0.0**	**0.0**	**0%**
9 Windows Firewall with Advanced Security	**0**	**26**	**0**	**0**	**0.0**	**26.0**	**0%**
9.1 Domain Profile	0	8	0	0	0.0	8.0	0%
9.2 Private Profile	0	8	0	0	0.0	8.0	0%
9.3 Public Profile	0	10	0	0	0.0	10.0	0%
10 Network List Manager Policies	**0**	**0**	**0**	**0**	**0.0**	**0.0**	**0%**
11 Wireless Network (IEEE 802.11) Policies	**0**	**0**	**0**	**0**	**0.0**	**0.0**	**0%**
12 Public Key Policies	**0**	**0**	**0**	**0**	**0.0**	**0.0**	**0%**
13 Software Restriction Policies	**0**	**0**	**0**	**0**	**0.0**	**0.0**	**0%**
14 Network Access Protection NAP Client Configuration	**0**	**0**	**0**	**0**	**0.0**	**0.0**	**0%**
15 Application Control Policies	**0**	**0**	**0**	**0**	**0.0**	**0.0**	**0%**
16 IP Security Policies	**0**	**0**	**0**	**0**	**0.0**	**0.0**	**0%**
17 Advanced Audit Policy Configuration	**8**	**20**	**0**	**0**	**8.0**	**28.0**	**29%**
17.1 Account Logon	0	1	0	0	0.0	1.0	0%
17.2 Account Management	1	3	0	0	1.0	4.0	25%
17.3 Detailed Tracking	0	2	0	0	0.0	2.0	0%
17.4 DS Access	0	0	0	0	0.0	0.0	0%
17.5 Logon/Logoff	2	4	0	0	2.0	6.0	33%
17.6 Object Access	0	4	0	0	0.0	4.0	0%
17.7 Policy Change	2	3	0	0	2.0	5.0	40%
17.8 Privilege Use	0	1	0	0	0.0	1.0	0%
17.9 System	3	2	0	0	3.0	5.0	60%
18 Administrative Templates (Computer)	**7**	**130**	**0**	**0**	**7.0**	**137.0**	**5%**
18.1 Control Panel	0	3	0	0	0.0	3.0	0%
18.1.1 Personalization	0	2	0	0	0.0	2.0	0%

Description	Tests				Scoring		
	Pass	Fail	Error	Unkn.	Score	Max	Percent
18.1.2 Regional and Language Options	0	1	0	0	0.0	1.0	0%
18.1.2.1 Handwriting personalization	0	0	0	0	0.0	0.0	0%
18.2 LAPS	0	6	0	0	0.0	6.0	0%
18.3 MS Security Guide	0	6	0	0	0.0	6.0	0%
18.4 MSS (Legacy)	0	8	0	0	0.0	8.0	0%
18.5 Network	1	9	0	0	1.0	10.0	10%
18.5.1 Background Intelligent Transfer Service (BITS)	0	0	0	0	0.0	0.0	0%
18.5.2 BranchCache	0	0	0	0	0.0	0.0	0%
18.5.3 DirectAccess Client Experience Settings	0	0	0	0	0.0	0.0	0%
18.5.4 DNS Client	1	1	0	0	1.0	2.0	50%
18.5.5 Fonts	0	0	0	0	0.0	0.0	0%
18.5.6 Hotspot Authentication	0	0	0	0	0.0	0.0	0%
18.5.7 Lanman Server	0	0	0	0	0.0	0.0	0%
18.5.8 Lanman Workstation	0	1	0	0	0.0	1.0	0%
18.5.9 Link-Layer Topology Discovery	0	0	0	0	0.0	0.0	0%
18.5.10 Microsoft Peer-to-Peer Networking Services	0	0	0	0	0.0	0.0	0%
18.5.10.1 Peer Name Resolution Protocol	0	0	0	0	0.0	0.0	0%
18.5.11 Network Connections	0	3	0	0	0.0	3.0	0%
18.5.11.1 Windows Defender Firewall (formerly Windows Firewall)	0	0	0	0	0.0	0.0	0%
18.5.12 Network Connectivity Status Indicator	0	0	0	0	0.0	0.0	0%
18.5.13 Network Isolation	0	0	0	0	0.0	0.0	0%
18.5.14 Network Provider	0	1	0	0	0.0	1.0	0%
18.5.15 Offline Files	0	0	0	0	0.0	0.0	0%
18.5.16 QoS Packet Scheduler	0	0	0	0	0.0	0.0	0%
18.5.17 SNMP	0	0	0	0	0.0	0.0	0%
18.5.18 SSL Configuration Settings	0	0	0	0	0.0	0.0	0%
18.5.19 TCPIP Settings	0	0	0	0	0.0	0.0	0%
18.5.19.1 IPv6 Transition Technologies	0	0	0	0	0.0	0.0	0%
18.5.19.2 Parameters	0	0	0	0	0.0	0.0	0%
18.5.20 Windows Connect Now	0	0	0	0	0.0	0.0	0%
18.5.21 Windows Connection Manager	0	2	0	0	0.0	2.0	0%
18.5.22 Wireless Display	0	0	0	0	0.0	0.0	0%
18.5.23 WLAN Service	0	1	0	0	0.0	1.0	0%
18.5.23.1 WLAN Media Cost	0	0	0	0	0.0	0.0	0%
18.5.23.2 WLAN Settings	0	1	0	0	0.0	1.0	0%
18.6 Printers	0	0	0	0	0.0	0.0	0%
18.7 Start Menu and Taskbar	0	0	0	0	0.0	0.0	0%
18.7.1 Notifications	0	0	0	0	0.0	0.0	0%
18.8 System	2	23	0	0	2.0	25.0	8%
18.8.1 Access-Denied Assistance	0	0	0	0	0.0	0.0	0%
18.8.2 App-V	0	0	0	0	0.0	0.0	0%
18.8.3 Audit Process Creation	0	1	0	0	0.0	1.0	0%
18.8.4 Credentials Delegation	0	2	0	0	0.0	2.0	0%
18.8.5 Device Guard	0	0	0	0	0.0	0.0	0%
18.8.6 Device Health Attestation Service	0	0	0	0	0.0	0.0	0%
18.8.7 Device Installation	0	0	0	0	0.0	0.0	0%
18.8.7.1 Device Installation Restrictions	0	0	0	0	0.0	0.0	0%
18.8.8 Device Redirection	0	0	0	0	0.0	0.0	0%
18.8.9 Disk NV Cache	0	0	0	0	0.0	0.0	0%
18.8.10 Disk Quotas	0	0	0	0	0.0	0.0	0%
18.8.11 Display	0	0	0	0	0.0	0.0	0%
18.8.12 Distributed COM	0	0	0	0	0.0	0.0	0%
18.8.13 Driver Installation	0	0	0	0	0.0	0.0	0%
18.8.14 Early Launch Antimalware	0	1	0	0	0.0	1.0	0%
18.8.15 Enhanced Storage Access	0	0	0	0	0.0	0.0	0%
18.8.16 File Classification Infrastructure	0	0	0	0	0.0	0.0	0%
18.8.17 File Share Shadow Copy Agent	0	0	0	0	0.0	0.0	0%
18.8.18 File Share Shadow Copy Provider	0	0	0	0	0.0	0.0	0%

Description	Tests				Scoring		
	Pass	Fail	Error	Unkn.	Score	Max	Percent
18.8.19 Filesystem (formerly NTFS Filesystem)	0	0	0	0	0.0	0.0	0%
18.8.20 Folder Redirection	0	0	0	0	0.0	0.0	0%
18.8.21 Group Policy	1	3	0	0	1.0	4.0	25%
18.8.21.1 Logging and tracing	0	0	0	0	0.0	0.0	0%
18.8.22 Internet Communication Management	0	2	0	0	0.0	2.0	0%
18.8.22.1 Internet Communication settings	0	2	0	0	0.0	2.0	0%
18.8.23 iSCSI	0	0	0	0	0.0	0.0	0%
18.8.24 KDC	0	0	0	0	0.0	0.0	0%
18.8.25 Kerberos	0	0	0	0	0.0	0.0	0%
18.8.26 Locale Services	0	0	0	0	0.0	0.0	0%
18.8.27 Logon	1	6	0	0	1.0	7.0	14%
18.8.28 Mitigation Options	0	0	0	0	0.0	0.0	0%
18.8.29 Net Logon	0	0	0	0	0.0	0.0	0%
18.8.30 OS Policies	0	0	0	0	0.0	0.0	0%
18.8.31 Performance Control Panel	0	0	0	0	0.0	0.0	0%
18.8.32 PIN Complexity	0	0	0	0	0.0	0.0	0%
18.8.33 Power Management	0	4	0	0	0.0	4.0	0%
18.8.33.1 Button Settings	0	0	0	0	0.0	0.0	0%
18.8.33.2 Energy Saver Settings	0	0	0	0	0.0	0.0	0%
18.8.33.3 Hard Disk Settings	0	0	0	0	0.0	0.0	0%
18.8.33.4 Notification Settings	0	0	0	0	0.0	0.0	0%
18.8.33.5 Power Throttling Settings	0	0	0	0	0.0	0.0	0%
18.8.33.6 Sleep Settings	0	4	0	0	0.0	4.0	0%
18.8.34 Recovery	0	0	0	0	0.0	0.0	0%
18.8.35 Remote Assistance	0	2	0	0	0.0	2.0	0%
18.8.36 Remote Procedure Call	0	2	0	0	0.0	2.0	0%
18.8.37 Removable Storage Access	0	0	0	0	0.0	0.0	0%
18.8.38 Scripts	0	0	0	0	0.0	0.0	0%
18.8.39 Server Manager	0	0	0	0	0.0	0.0	0%
18.8.40 Shutdown	0	0	0	0	0.0	0.0	0%
18.8.41 Shutdown Options	0	0	0	0	0.0	0.0	0%
18.8.42 Storage Health	0	0	0	0	0.0	0.0	0%
18.8.43 System Restore	0	0	0	0	0.0	0.0	0%
18.8.44 Troubleshooting and Diagnostics	0	0	0	0	0.0	0.0	0%
18.8.44.1 Application Compatibility Diagnostics	0	0	0	0	0.0	0.0	0%
18.8.44.2 Corrupted File Recovery	0	0	0	0	0.0	0.0	0%
18.8.44.3 Disk Diagnostic	0	0	0	0	0.0	0.0	0%
18.8.44.4 Fault Tolerant Heap	0	0	0	0	0.0	0.0	0%
18.8.44.5 Microsoft Support Diagnostic Tool	0	0	0	0	0.0	0.0	0%
18.8.44.6 MSI Corrupted File Recovery	0	0	0	0	0.0	0.0	0%
18.8.44.7 Scheduled Maintenance	0	0	0	0	0.0	0.0	0%
18.8.44.8 Scripted Diagnostics	0	0	0	0	0.0	0.0	0%
18.8.44.9 Windows Boot Performance Diagnostics	0	0	0	0	0.0	0.0	0%
18.8.44.10 Windows Memory Leak Diagnosis	0	0	0	0	0.0	0.0	0%
18.8.44.11 Windows Performance PerfTrack	0	0	0	0	0.0	0.0	0%
18.8.45 Trusted Platform Module Services	0	0	0	0	0.0	0.0	0%
18.8.46 User Profiles	0	0	0	0	0.0	0.0	0%
18.8.47 Windows File Protection	0	0	0	0	0.0	0.0	0%
18.8.48 Windows HotStart	0	0	0	0	0.0	0.0	0%
18.8.49 Windows Time Service	0	0	0	0	0.0	0.0	0%
18.8.49.1 Time Providers	0	0	0	0	0.0	0.0	0%
18.9 Windows Components	4	75	0	0	4.0	79.0	5%
18.9.1 Active Directory Federation Services	0	0	0	0	0.0	0.0	0%
18.9.2 ActiveX Installer Service	0	0	0	0	0.0	0.0	0%
18.9.3 Add features to Windows 8 / 8.1 / 10 (formerly Windows Anytime Upgrade)	0	0	0	0	0.0	0.0	0%
18.9.4 App Package Deployment	0	0	0	0	0.0	0.0	0%
18.9.5 App Privacy	0	0	0	0	0.0	0.0	0%
18.9.6 App runtime	0	1	0	0	0.0	1.0	0%

Description	Tests				Scoring		
	Pass	Fail	Error	Unkn.	Score	Max	Percent
18.9.7 Application Compatibility	0	0	0	0	0.0	0.0	0%
18.9.8 AutoPlay Policies	0	3	0	0	0.0	3.0	0%
18.9.9 Backup	0	0	0	0	0.0	0.0	0%
18.9.10 Biometrics	0	1	0	0	0.0	1.0	0%
18.9.10.1 Facial Features	0	1	0	0	0.0	1.0	0%
18.9.11 BitLocker Drive Encryption	0	0	0	0	0.0	0.0	0%
18.9.11.1 Fixed Data Drives	0	0	0	0	0.0	0.0	0%
18.9.11.2 Operating System Drives	0	0	0	0	0.0	0.0	0%
18.9.11.3 Removable Data Drives	0	0	0	0	0.0	0.0	0%
18.9.12 Camera	0	0	0	0	0.0	0.0	0%
18.9.13 Cloud Content	0	1	0	0	0.0	1.0	0%
18.9.14 Connect	0	1	0	0	0.0	1.0	0%
18.9.15 Credential User Interface	0	2	0	0	0.0	2.0	0%
18.9.16 Data Collection and Preview Builds	0	3	0	0	0.0	3.0	0%
18.9.17 Delivery Optimization	1	0	0	0	1.0	1.0	100%
18.9.18 Desktop Gadgets	0	0	0	0	0.0	0.0	0%
18.9.19 Desktop Window Manager	0	0	0	0	0.0	0.0	0%
18.9.20 Device and Driver Compatibility	0	0	0	0	0.0	0.0	0%
18.9.21 Device Registration (formerly Workplace Join)	0	0	0	0	0.0	0.0	0%
18.9.22 Digital Locker	0	0	0	0	0.0	0.0	0%
18.9.23 Edge UI	0	0	0	0	0.0	0.0	0%
18.9.24 EMET	0	0	0	0	0.0	0.0	0%
18.9.25 Event Forwarding	0	0	0	0	0.0	0.0	0%
18.9.26 Event Log Service	0	8	0	0	0.0	8.0	0%
18.9.26.1 Application	0	2	0	0	0.0	2.0	0%
18.9.26.2 Security	0	2	0	0	0.0	2.0	0%
18.9.26.3 Setup	0	2	0	0	0.0	2.0	0%
18.9.26.4 System	0	2	0	0	0.0	2.0	0%
18.9.27 Event Logging	0	0	0	0	0.0	0.0	0%
18.9.28 Event Viewer	0	0	0	0	0.0	0.0	0%
18.9.29 Family Safety (formerly Parental Controls)	0	0	0	0	0.0	0.0	0%
18.9.30 File Explorer (formerly Windows Explorer)	0	3	0	0	0.0	3.0	0%
18.9.30.1 Previous Versions	0	0	0	0	0.0	0.0	0%
18.9.31 File History	0	0	0	0	0.0	0.0	0%
18.9.32 Find My Device	0	0	0	0	0.0	0.0	0%
18.9.33 Game Explorer	0	0	0	0	0.0	0.0	0%
18.9.34 Handwriting	0	0	0	0	0.0	0.0	0%
18.9.35 HomeGroup	0	1	0	0	0.0	1.0	0%
18.9.36 Import Video	0	0	0	0	0.0	0.0	0%
18.9.37 Internet Explorer	0	0	0	0	0.0	0.0	0%
18.9.38 Internet Information Services	0	0	0	0	0.0	0.0	0%
18.9.39 Location and Sensors	0	0	0	0	0.0	0.0	0%
18.9.39.1 Windows Location Provider	0	0	0	0	0.0	0.0	0%
18.9.40 Maintenance Scheduler	0	0	0	0	0.0	0.0	0%
18.9.41 Maps	0	0	0	0	0.0	0.0	0%
18.9.42 MDM	0	0	0	0	0.0	0.0	0%
18.9.43 Messaging	0	0	0	0	0.0	0.0	0%
18.9.44 Microsoft account	0	1	0	0	0.0	1.0	0%
18.9.45 Microsoft Edge	0	3	0	0	0.0	3.0	0%
18.9.46 Microsoft FIDO Authentication	0	0	0	0	0.0	0.0	0%
18.9.47 Microsoft Secondary Authentication Factor	0	0	0	0	0.0	0.0	0%
18.9.48 Microsoft User Experience Virtualization	0	0	0	0	0.0	0.0	0%
18.9.49 NetMeeting	0	0	0	0	0.0	0.0	0%
18.9.50 Network Access Protection	0	0	0	0	0.0	0.0	0%
18.9.51 Network Projector	0	0	0	0	0.0	0.0	0%
18.9.52 OneDrive (formerly SkyDrive)	1	0	0	0	1.0	1.0	100%
18.9.53 Online Assistance	0	0	0	0	0.0	0.0	0%
18.9.54 Password Synchronization	0	0	0	0	0.0	0.0	0%

Description	Tests				Scoring		
	Pass	Fail	Error	Unkn.	Score	Max	Percent
18.9.55 Portable Operating System	0	0	0	0	0.0	0.0	0%
18.9.56 Presentation Settings	0	0	0	0	0.0	0.0	0%
18.9.57 Push To Install	0	0	0	0	0.0	0.0	0%
18.9.58 Remote Desktop Services (formerly Terminal Services)	0	9	0	0	0.0	9.0	0%
18.9.58.1 RD Licensing (formerly TS Licensing)	0	0	0	0	0.0	0.0	0%
18.9.58.2 Remote Desktop Connection Client	0	1	0	0	0.0	1.0	0%
18.9.58.2.1 RemoteFX USB Device Redirection	0	0	0	0	0.0	0.0	0%
18.9.58.3 Remote Desktop Session Host (formerly Terminal Server)	0	8	0	0	0.0	8.0	0%
18.9.58.3.1 Application Compatibility	0	0	0	0	0.0	0.0	0%
18.9.58.3.2 Connections	0	0	0	0	0.0	0.0	0%
18.9.58.3.3 Device and Resource Redirection	0	1	0	0	0.0	1.0	0%
18.9.58.3.4 Licensing	0	0	0	0	0.0	0.0	0%
18.9.58.3.5 Printer Redirection	0	0	0	0	0.0	0.0	0%
18.9.58.3.6 Profiles	0	0	0	0	0.0	0.0	0%
18.9.58.3.7 RD Connection Broker (formerly TS Connection Broker)	0	0	0	0	0.0	0.0	0%
18.9.58.3.8 Remote Session Environment	0	0	0	0	0.0	0.0	0%
18.9.58.3.9 Security	0	5	0	0	0.0	5.0	0%
18.9.58.3.10 Session Time Limits	0	0	0	0	0.0	0.0	0%
18.9.58.3.11 Temporary folders	0	2	0	0	0.0	2.0	0%
18.9.59 RSS Feeds	0	1	0	0	0.0	1.0	0%
18.9.60 Search	0	4	0	0	0.0	4.0	0%
18.9.60.1 OCR	0	0	0	0	0.0	0.0	0%
18.9.61 Security Center	0	0	0	0	0.0	0.0	0%
18.9.62 Server for NIS	0	0	0	0	0.0	0.0	0%
18.9.63 Shutdown Options	0	0	0	0	0.0	0.0	0%
18.9.64 Smart Card	0	0	0	0	0.0	0.0	0%
18.9.65 Software Protection Platform	0	0	0	0	0.0	0.0	0%
18.9.66 Sound Recorder	0	0	0	0	0.0	0.0	0%
18.9.67 Speech	0	0	0	0	0.0	0.0	0%
18.9.68 Store	0	3	0	0	0.0	3.0	0%
18.9.69 Sync your settings	0	0	0	0	0.0	0.0	0%
18.9.70 Tablet PC	0	0	0	0	0.0	0.0	0%
18.9.71 Task Scheduler	0	0	0	0	0.0	0.0	0%
18.9.72 Text Input	0	0	0	0	0.0	0.0	0%
18.9.73 Windows Calendar	0	0	0	0	0.0	0.0	0%
18.9.74 Windows Color System	0	0	0	0	0.0	0.0	0%
18.9.75 Windows Customer Experience Improvement Program	0	0	0	0	0.0	0.0	0%
18.9.76 Windows Defender Antivirus (formerly Windows Defender)	0	8	0	0	0.0	8.0	0%
18.9.76.1 Client Interface	0	0	0	0	0.0	0.0	0%
18.9.76.2 Exclusions	0	0	0	0	0.0	0.0	0%
18.9.76.3 MAPS	0	1	0	0	0.0	1.0	0%
18.9.76.4 MpEngine	0	0	0	0	0.0	0.0	0%
18.9.76.5 Network Inspection System	0	0	0	0	0.0	0.0	0%
18.9.76.6 Quarantine	0	0	0	0	0.0	0.0	0%
18.9.76.7 Real-time Protection	0	1	0	0	0.0	1.0	0%
18.9.76.8 Remediation	0	0	0	0	0.0	0.0	0%
18.9.76.9 Reporting	0	0	0	0	0.0	0.0	0%
18.9.76.10 Scan	0	2	0	0	0.0	2.0	0%
18.9.76.11 Signature Updates	0	0	0	0	0.0	0.0	0%
18.9.76.12 Threats	0	0	0	0	0.0	0.0	0%
18.9.76.13 Windows Defender Exploit Guard	0	3	0	0	0.0	3.0	0%
18.9.76.13.1 Attack Surface Reduction	0	2	0	0	0.0	2.0	0%
18.9.76.13.2 Controlled Folder Access	0	0	0	0	0.0	0.0	0%
18.9.76.13.3 Network Protection	0	1	0	0	0.0	1.0	0%
18.9.77 Windows Defender Application Guard	0	0	0	0	0.0	0.0	0%
18.9.78 Windows Defender Exploit Guard	0	0	0	0	0.0	0.0	0%
18.9.79 Windows Defender Security Center	0	1	0	0	0.0	1.0	0%
18.9.79.1 Account protection	0	0	0	0	0.0	0.0	0%

Description	Tests				Scoring		
	Pass	Fail	Error	Unkn.	Score	Max	Percent
18.9.79.2 App and browser protection	0	1	0	0	0.0	1.0	0%
18.9.80 Windows Defender SmartScreen	0	4	0	0	0.0	4.0	0%
18.9.80.1 Explorer	0	1	0	0	0.0	1.0	0%
18.9.80.2 Microsoft Edge	0	3	0	0	0.0	3.0	0%
18.9.81 Windows Error Reporting	0	0	0	0	0.0	0.0	0%
18.9.82 Windows Game Recording and Broadcasting	0	1	0	0	0.0	1.0	0%
18.9.83 Windows Hello for Business (formerly Microsoft Passport for Work)	0	0	0	0	0.0	0.0	0%
18.9.84 Windows Ink Workspace	0	1	0	0	0.0	1.0	0%
18.9.85 Windows Installer	0	2	0	0	0.0	2.0	0%
18.9.86 Windows Logon Options	0	1	0	0	0.0	1.0	0%
18.9.87 Windows Mail	0	0	0	0	0.0	0.0	0%
18.9.88 Windows Media Center	0	0	0	0	0.0	0.0	0%
18.9.89 Windows Media Digital Rights Management	0	0	0	0	0.0	0.0	0%
18.9.90 Windows Media Player	0	0	0	0	0.0	0.0	0%
18.9.91 Windows Meeting Space	0	0	0	0	0.0	0.0	0%
18.9.92 Windows Messenger	0	0	0	0	0.0	0.0	0%
18.9.93 Windows Mobility Center	0	0	0	0	0.0	0.0	0%
18.9.94 Windows Movie Maker	0	0	0	0	0.0	0.0	0%
18.9.95 Windows PowerShell	0	2	0	0	0.0	2.0	0%
18.9.96 Windows Reliability Analysis	0	0	0	0	0.0	0.0	0%
18.9.97 Windows Remote Management (WinRM)	0	6	0	0	0.0	6.0	0%
18.9.97.1 WinRM Client	0	3	0	0	0.0	3.0	0%
18.9.97.2 WinRM Service	0	3	0	0	0.0	3.0	0%
18.9.98 Windows Remote Shell	0	0	0	0	0.0	0.0	0%
18.9.99 Windows SideShow	0	0	0	0	0.0	0.0	0%
18.9.100 Windows System Resource Manager	0	0	0	0	0.0	0.0	0%
18.9.101 Windows Update	2	4	0	0	2.0	6.0	33%
18.9.101.1 Windows Update for Business (formerly Defer Windows Updates)	0	3	0	0	0.0	3.0	0%
19 Administrative Templates (User)	**0**	**11**	**0**	**0**	**0.0**	**11.0**	**0%**
19.1 Control Panel	0	4	0	0	0.0	4.0	0%
19.1.1 Add or Remove Programs	0	0	0	0	0.0	0.0	0%
19.1.2 Display	0	0	0	0	0.0	0.0	0%
19.1.3 Personalization (formerly Desktop Themes)	0	4	0	0	0.0	4.0	0%
19.2 Desktop	0	0	0	0	0.0	0.0	0%
19.3 Network	0	0	0	0	0.0	0.0	0%
19.4 Shared Folders	0	0	0	0	0.0	0.0	0%
19.5 Start Menu and Taskbar	0	1	0	0	0.0	1.0	0%
19.5.1 Notifications	0	1	0	0	0.0	1.0	0%
19.6 System	0	0	0	0	0.0	0.0	0%
19.6.1 Ctrl+Alt+Del Options	0	0	0	0	0.0	0.0	0%
19.6.2 Display	0	0	0	0	0.0	0.0	0%
19.6.3 Driver Installation	0	0	0	0	0.0	0.0	0%
19.6.4 Folder Redirection	0	0	0	0	0.0	0.0	0%
19.6.5 Group Policy	0	0	0	0	0.0	0.0	0%
19.6.6 Internet Communication Management	0	0	0	0	0.0	0.0	0%
19.6.6.1 Internet Communication settings	0	0	0	0	0.0	0.0	0%
19.7 Windows Components	0	6	0	0	0.0	6.0	0%
19.7.1 Add features to Windows 8 / 8.1 / 10 (formerly Windows Anytime Upgrade)	0	0	0	0	0.0	0.0	0%
19.7.2 App runtime	0	0	0	0	0.0	0.0	0%
19.7.3 Application Compatibility	0	0	0	0	0.0	0.0	0%
19.7.4 Attachment Manager	0	2	0	0	0.0	2.0	0%
19.7.5 AutoPlay Policies	0	0	0	0	0.0	0.0	0%
19.7.6 Backup	0	0	0	0	0.0	0.0	0%
19.7.7 Cloud Content	0	2	0	0	0.0	2.0	0%
19.7.8 Credential User Interface	0	0	0	0	0.0	0.0	0%
19.7.9 Data Collection and Preview Builds	0	0	0	0	0.0	0.0	0%
19.7.10 Desktop Gadgets	0	0	0	0	0.0	0.0	0%
19.7.11 Desktop Window Manager	0	0	0	0	0.0	0.0	0%

Description	Tests				Scoring		
	Pass	Fail	Error	Unkn.	Score	Max	Percent
19.7.12 Digital Locker	0	0	0	0	0.0	0.0	0%
19.7.13 Edge UI	0	0	0	0	0.0	0.0	0%
19.7.14 File Explorer (formerly Windows Explorer)	0	0	0	0	0.0	0.0	0%
19.7.15 File Revocation	0	0	0	0	0.0	0.0	0%
19.7.16 IME	0	0	0	0	0.0	0.0	0%
19.7.17 Import Video	0	0	0	0	0.0	0.0	0%
19.7.18 Instant Search	0	0	0	0	0.0	0.0	0%
19.7.19 Internet Explorer	0	0	0	0	0.0	0.0	0%
19.7.20 Location and Sensors	0	0	0	0	0.0	0.0	0%
19.7.21 Microsoft Edge	0	0	0	0	0.0	0.0	0%
19.7.22 Microsoft Management Console	0	0	0	0	0.0	0.0	0%
19.7.23 Microsoft User Experience Virtualization	0	0	0	0	0.0	0.0	0%
19.7.24 NetMeeting	0	0	0	0	0.0	0.0	0%
19.7.25 Network Projector	0	0	0	0	0.0	0.0	0%
19.7.26 Network Sharing	0	1	0	0	0.0	1.0	0%
19.7.27 Presentation Settings	0	0	0	0	0.0	0.0	0%
19.7.28 Remote Desktop Services (formerly Terminal Services)	0	0	0	0	0.0	0.0	0%
19.7.29 RSS Feeds	0	0	0	0	0.0	0.0	0%
19.7.30 Search	0	0	0	0	0.0	0.0	0%
19.7.31 Sound Recorder	0	0	0	0	0.0	0.0	0%
19.7.32 Store	0	0	0	0	0.0	0.0	0%
19.7.33 Tablet PC	0	0	0	0	0.0	0.0	0%
19.7.34 Task Scheduler	0	0	0	0	0.0	0.0	0%
19.7.35 Windows Calendar	0	0	0	0	0.0	0.0	0%
19.7.36 Windows Color System	0	0	0	0	0.0	0.0	0%
19.7.37 Windows Defender SmartScreen	0	0	0	0	0.0	0.0	0%
19.7.38 Windows Error Reporting	0	0	0	0	0.0	0.0	0%
19.7.39 Windows Hello for Business (formerly Microsoft Passport for Work)	0	0	0	0	0.0	0.0	0%
19.7.40 Windows Installer	0	1	0	0	0.0	1.0	0%
19.7.41 Windows Logon Options	0	0	0	0	0.0	0.0	0%
19.7.42 Windows Mail	0	0	0	0	0.0	0.0	0%
19.7.43 Windows Media Center	0	0	0	0	0.0	0.0	0%
19.7.44 Windows Media Player	0	0	0	0	0.0	0.0	0%
19.7.44.1 Networking	0	0	0	0	0.0	0.0	0%
19.7.44.2 Playback	0	0	0	0	0.0	0.0	0%
Total	**84**	**245**	**0**	**3**	**84.0**	**332.0**	**25%**

Note: Actual scores are subject to rounding errors. The sum of these values may not result in the exact overall score.

Profiles

This benchmark contains 10 profiles.The **Level 1 (L1) - Corporate/Enterprise Environment (general use)** profile was used for this assessment.

Title	Description
Level 1 (L1) - Corporate/Enterprise Environment (general use)	Items in this profile intend to: • be the starting baseline for most organizations; • be practical and prudent; • provide a clear security benefit; and • not inhibit the utility of the technology beyond acceptable means.
Level 1 (L1) + BitLocker (BL)	This profile extends the "Level 1 (L1)" profile and includes BitLocker-related recommendations.
Level 1 (L1) + Next Generation Windows Security (NG)	This profile extends the "Level 1 (L1)" profile and includes Next Generation Windows Security-related recommendations.
Level 1 (L1) + BitLocker (BL) + Next Generation Windows Security (NG)	This profile extends the "Level 1 (L1)" profile and includes BitLocker and Next Generation Windows Security-related recommendations.

Title	Description
Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)	This profile extends the "Level 1 (L1)" profile. Items in this profile exhibit one or more of the following characteristics: • are intended for environments or use cases where security is more critical than manageability and usability; • may negatively inhibit the utility or performance of the technology; and • limit the ability of remote management/access. **Note:** Implementation of Level 2 requires that **both** Level 1 and Level 2 settings are applied.
Level 2 (L2) + BitLocker (BL)	This profile extends the "Level 2 (L2)" profile and includes BitLocker-related recommendations.
Level 2 (L2) + Next Generation Windows Security (NG)	This profile extends the "Level 2 (L2)" profile and includes Next Generation Windows Security-related recommendations.
Level 2 (L2) + BitLocker (BL) + Next Generation Windows Security (NG)	This profile extends the "Level 2 (L2)" profile and includes BitLocker and Next Generation Windows Security-related recommendations.
BitLocker (BL) - optional add-on for when BitLocker is deployed	This profile contains BitLocker-related recommendations, if your organization chooses to use it. It is intended be an optional "add-on" to the Level 1 (L1) or Level 2 (L2) profiles.
Next Generation Windows Security (NG) - optional add-on for use in the newest hardware and configuration environments	This profile contains advanced Windows security features that have specific configuration dependencies, and may not be compatible with all systems. It therefore requires special attention to detail and testing before implementation. If your environment supports these features, they are highly recommended as they have tangible security benefits. This profile is intended to be an optional "add-on" to the Level 1 (L1) or Level 2 (L2) profiles.

⇧

Assessment Results

Display Failures Only

w	Benchmark Item	Result
1 Account Policies		
1.1 Password Policy		
1.0	1.1.1 (L1) Ensure 'Enforce password history' is set to '24 or more password(s)'	Fail
1.0	1.1.2 (L1) Ensure 'Maximum password age' is set to '60 or fewer days, but not 0'	Fail
1.0	1.1.3 (L1) Ensure 'Minimum password age' is set to '1 or more day(s)'	Fail
1.0	1.1.4 (L1) Ensure 'Minimum password length' is set to '14 or more character(s)'	Fail
1.0	1.1.5 (L1) Ensure 'Password must meet complexity requirements' is set to 'Enabled'	Unknown
1.0	1.1.6 (L1) Ensure 'Store passwords using reversible encryption' is set to 'Disabled'	Unknown
1.2 Account Lockout Policy		
1.0	1.2.1 (L1) Ensure 'Account lockout duration' is set to '15 or more minute(s)'	Pass
1.0	1.2.2 (L1) Ensure 'Account lockout threshold' is set to '10 or fewer invalid logon attempt(s), but not 0'	Fail
1.0	1.2.3 (L1) Ensure 'Reset account lockout counter after' is set to '15 or more minute(s)'	Pass
2 Local Policies		
2.1 Audit Policy		
2.2 User Rights Assignment		
1.0	2.2.1 (L1) Ensure 'Access Credential Manager as a trusted caller' is set to 'No One'	Pass
1.0	2.2.2 (L1) Ensure 'Access this computer from the network' is set to 'Administrators, Remote Desktop Users'	Fail
1.0	2.2.3 (L1) Ensure 'Act as part of the operating system' is set to 'No One'	Pass
1.0	2.2.4 (L1) Ensure 'Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE'	Pass
1.0	2.2.5 (L1) Ensure 'Allow log on locally' is set to 'Administrators, Users'	Fail
1.0	2.2.6 (L1) Ensure 'Allow log on through Remote Desktop Services' is set to 'Administrators, Remote Desktop Users'	Pass
1.0	2.2.7 (L1) Ensure 'Back up files and directories' is set to 'Administrators'	Fail
1.0	2.2.8 (L1) Ensure 'Change the system time' is set to 'Administrators, LOCAL SERVICE'	Pass
1.0	2.2.9 (L1) Ensure 'Change the time zone' is set to 'Administrators, LOCAL SERVICE, Users'	Pass
1.0	2.2.10 (L1) Ensure 'Create a pagefile' is set to 'Administrators'	Pass
1.0	2.2.11 (L1) Ensure 'Create a token object' is set to 'No One'	Pass

w	**Benchmark Item**	**Result**
1.0	2.2.12 (L1) Ensure 'Create global objects' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE'	Pass
1.0	2.2.13 (L1) Ensure 'Create permanent shared objects' is set to 'No One'	Pass
1.0	2.2.14 (L1) Configure 'Create symbolic links'	Pass
1.0	2.2.15 (L1) Ensure 'Debug programs' is set to 'Administrators'	Pass
1.0	2.2.16 (L1) Ensure 'Deny access to this computer from the network' to include 'Guests, Local account'	Fail
1.0	2.2.17 (L1) Ensure 'Deny log on as a batch job' to include 'Guests'	Fail
1.0	2.2.18 (L1) Ensure 'Deny log on as a service' to include 'Guests'	Fail
1.0	2.2.19 (L1) Ensure 'Deny log on locally' to include 'Guests'	Fail
1.0	2.2.20 (L1) Ensure 'Deny log on through Remote Desktop Services' to include 'Guests, Local account'	Fail
1.0	2.2.21 (L1) Ensure 'Enable computer and user accounts to be trusted for delegation' is set to 'No One'	Pass
1.0	2.2.22 (L1) Ensure 'Force shutdown from a remote system' is set to 'Administrators'	Pass
1.0	2.2.23 (L1) Ensure 'Generate security audits' is set to 'LOCAL SERVICE, NETWORK SERVICE'	Pass
1.0	2.2.24 (L1) Ensure 'Impersonate a client after authentication' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE'	Fail
1.0	2.2.25 (L1) Ensure 'Increase scheduling priority' is set to 'Administrators, Window Manager\Window Manager Group'	Pass
1.0	2.2.26 (L1) Ensure 'Load and unload device drivers' is set to 'Administrators'	Pass
1.0	2.2.27 (L1) Ensure 'Lock pages in memory' is set to 'No One'	Pass
1.0	2.2.30 (L1) Ensure 'Manage auditing and security log' is set to 'Administrators'	Pass
1.0	2.2.31 (L1) Ensure 'Modify an object label' is set to 'No One'	Pass
1.0	2.2.32 (L1) Ensure 'Modify firmware environment values' is set to 'Administrators'	Pass
1.0	2.2.33 (L1) Ensure 'Perform volume maintenance tasks' is set to 'Administrators'	Pass
1.0	2.2.34 (L1) Ensure 'Profile single process' is set to 'Administrators'	Pass
1.0	2.2.35 (L1) Ensure 'Profile system performance' is set to 'Administrators, NT SERVICE\WdiServiceHost'	Pass
1.0	2.2.36 (L1) Ensure 'Replace a process level token' is set to 'LOCAL SERVICE, NETWORK SERVICE'	Pass
1.0	2.2.37 (L1) Ensure 'Restore files and directories' is set to 'Administrators'	Fail
1.0	2.2.38 (L1) Ensure 'Shut down the system' is set to 'Administrators, Users'	Fail
1.0	2.2.39 (L1) Ensure 'Take ownership of files or other objects' is set to 'Administrators'	Pass
2.3 Security Options		
2.3.1 Accounts		
1.0	2.3.1.1 (L1) Ensure 'Accounts: Administrator account status' is set to 'Disabled'	Pass
1.0	2.3.1.2 (L1) Ensure 'Accounts: Block Microsoft accounts' is set to 'Users can't add or log on with Microsoft accounts'	Fail
1.0	2.3.1.3 (L1) Ensure 'Accounts: Guest account status' is set to 'Disabled'	Pass
1.0	2.3.1.4 (L1) Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled'	Fail
1.0	2.3.1.5 (L1) Configure 'Accounts: Rename administrator account'	Fail
1.0	2.3.1.6 (L1) Configure 'Accounts: Rename guest account'	Fail
2.3.2 Audit		
1.0	2.3.2.1 (L1) Ensure 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' is set to 'Enabled'	Fail
1.0	2.3.2.2 (L1) Ensure 'Audit: Shut down system immediately if unable to log security audits' is set to 'Disabled'	Pass
2.3.3 DCOM		
2.3.4 Devices		
1.0	2.3.4.1 (L1) Ensure 'Devices: Allowed to format and eject removable media' is set to 'Administrators and Interactive Users'	Fail
2.3.5 Domain controller		
2.3.6 Domain member		
1.0	2.3.6.1 (L1) Ensure 'Domain member: Digitally encrypt or sign secure channel data (always)' is set to 'Enabled'	Pass
1.0	2.3.6.2 (L1) Ensure 'Domain member: Digitally encrypt secure channel data (when possible)' is set to 'Enabled'	Pass
1.0	2.3.6.3 (L1) Ensure 'Domain member: Digitally sign secure channel data (when possible)' is set to 'Enabled'	Pass
1.0	2.3.6.4 (L1) Ensure 'Domain member: Disable machine account password changes' is set to 'Disabled'	Pass
1.0	2.3.6.5 (L1) Ensure 'Domain member: Maximum machine account password age' is set to '30 or fewer days, but not 0'	Pass
1.0	2.3.6.6 (L1) Ensure 'Domain member: Require strong (Windows 2000 or later) session key' is set to 'Enabled'	Pass
2.3.7 Interactive logon		
1.0	2.3.7.1 (L1) Ensure 'Interactive logon: Do not require CTRL+ALT+DEL' is set to 'Disabled'	Fail
1.0	2.3.7.2 (L1) Ensure 'Interactive logon: Don't display last signed-in' is set to 'Enabled'	Fail

w	Benchmark Item	Result
1.0	2.3.7.4 (L1) Ensure 'Interactive logon: Machine inactivity limit' is set to '900 or fewer second(s), but not 0'	Fail
1.0	2.3.7.5 (L1) Configure 'Interactive logon: Message text for users attempting to log on'	Fail
1.0	2.3.7.6 (L1) Configure 'Interactive logon: Message title for users attempting to log on'	Fail
1.0	2.3.7.8 (L1) Ensure 'Interactive logon: Prompt user to change password before expiration' is set to 'between 5 and 14 days'	Pass
1.0	2.3.7.9 (L1) Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or higher	Fail
2.3.8 Microsoft network client		
1.0	2.3.8.1 (L1) Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled'	Fail
1.0	2.3.8.2 (L1) Ensure 'Microsoft network client: Digitally sign communications (if server agrees)' is set to 'Enabled'	Pass
1.0	2.3.8.3 (L1) Ensure 'Microsoft network client: Send unencrypted password to third-party SMB servers' is set to 'Disabled'	Pass
2.3.9 Microsoft network server		
1.0	2.3.9.1 (L1) Ensure 'Microsoft network server: Amount of idle time required before suspending session' is set to '15 or fewer minute(s)'	Pass
1.0	2.3.9.2 (L1) Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled'	Fail
1.0	2.3.9.3 (L1) Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled'	Fail
1.0	2.3.9.4 (L1) Ensure 'Microsoft network server: Disconnect clients when logon hours expire' is set to 'Enabled'	Pass
1.0	2.3.9.5 (L1) Ensure 'Microsoft network server: Server SPN target name validation level' is set to 'Accept if provided by client' or higher	Fail
2.3.10 Network access		
1.0	2.3.10.1 (L1) Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled'	Unknown
1.0	2.3.10.2 (L1) Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts' is set to 'Enabled'	Pass
1.0	2.3.10.3 (L1) Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled'	Fail
1.0	2.3.10.4 (L1) Ensure 'Network access: Do not allow storage of passwords and credentials for network authentication' is set to 'Enabled'	Fail
1.0	2.3.10.5 (L1) Ensure 'Network access: Let Everyone permissions apply to anonymous users' is set to 'Disabled'	Pass
1.0	2.3.10.6 (L1) Ensure 'Network access: Named Pipes that can be accessed anonymously' is set to 'None'	Pass
1.0	2.3.10.7 (L1) Ensure 'Network access: Remotely accessible registry paths'	Pass
1.0	2.3.10.8 (L1) Ensure 'Network access: Remotely accessible registry paths and sub-paths'	Pass
1.0	2.3.10.9 (L1) Ensure 'Network access: Restrict anonymous access to Named Pipes and Shares' is set to 'Enabled'	Pass
1.0	2.3.10.10 (L1) Ensure 'Network access: Restrict clients allowed to make remote calls to SAM' is set to 'Administrators: Remote Access: Allow'	Fail
1.0	2.3.10.11 (L1) Ensure 'Network access: Shares that can be accessed anonymously' is set to 'None'	Pass
1.0	2.3.10.12 (L1) Ensure 'Network access: Sharing and security model for local accounts' is set to 'Classic - local users authenticate as themselves'	Pass
2.3.11 Network security		
1.0	2.3.11.1 (L1) Ensure 'Network security: Allow Local System to use computer identity for NTLM' is set to 'Enabled'	Fail
1.0	2.3.11.2 (L1) Ensure 'Network security: Allow LocalSystem NULL session fallback' is set to 'Disabled'	Fail
1.0	2.3.11.3 (L1) Ensure 'Network Security: Allow PKU2U authentication requests to this computer to use online identities' is set to 'Disabled'	Fail
1.0	2.3.11.4 (L1) Ensure 'Network security: Configure encryption types allowed for Kerberos' is set to 'AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types'	Fail
1.0	2.3.11.5 (L1) Ensure 'Network security: Do not store LAN Manager hash value on next password change' is set to 'Enabled'	Pass
1.0	2.3.11.6 (L1) Ensure 'Network security: Force logoff when logon hours expire' is set to 'Enabled'	Pass
1.0	2.3.11.7 (L1) Ensure 'Network security: LAN Manager authentication level' is set to 'Send NTLMv2 response only. Refuse LM&NTLM'	Fail
1.0	2.3.11.8 (L1) Ensure 'Network security: LDAP client signing requirements' is set to 'Negotiate signing' or higher	Pass
1.0	2.3.11.9 (L1) Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' is set to 'Require NTLMv2 session security, Require 128-bit encryption'	Fail
1.0	2.3.11.10 (L1) Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require NTLMv2 session security, Require 128-bit encryption'	Fail
2.3.12 Recovery console		
2.3.13 Shutdown		
2.3.14 System cryptography		
2.3.15 System objects		
1.0	2.3.15.1 (L1) Ensure 'System objects: Require case insensitivity for non-Windows subsystems' is set to 'Enabled'	Pass
1.0	2.3.15.2 (L1) Ensure 'System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)' is set to 'Enabled'	Pass
2.3.16 System settings		

w	Benchmark Item	Result
	2.3.17 User Account Control	
1.0	2.3.17.1 (L1) Ensure 'User Account Control: Admin Approval Mode for the Built-in Administrator account' is set to 'Enabled'	Fail
1.0	2.3.17.2 (L1) Ensure 'User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop' is set to 'Disabled'	Pass
1.0	2.3.17.3 (L1) Ensure 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' is set to 'Prompt for consent on the secure desktop'	Fail
1.0	2.3.17.4 (L1) Ensure 'User Account Control: Behavior of the elevation prompt for standard users' is set to 'Automatically deny elevation requests'	Fail
1.0	2.3.17.5 (L1) Ensure 'User Account Control: Detect application installations and prompt for elevation' is set to 'Enabled'	Pass
1.0	2.3.17.6 (L1) Ensure 'User Account Control: Only elevate UIAccess applications that are installed in secure locations' is set to 'Enabled'	Pass
1.0	2.3.17.7 (L1) Ensure 'User Account Control: Run all administrators in Admin Approval Mode' is set to 'Enabled'	Pass
1.0	2.3.17.8 (L1) Ensure 'User Account Control: Switch to the secure desktop when prompting for elevation' is set to 'Enabled'	Pass
1.0	2.3.17.9 (L1) Ensure 'User Account Control: Virtualize file and registry write failures to per-user locations' is set to 'Enabled'	Pass
	3 Event Log	
	4 Restricted Groups	
	5 System Services	
1.0	5.3 (L1) Ensure 'Computer Browser (Browser)' is set to 'Disabled' or 'Not Installed'	Fail
1.0	5.6 (L1) Ensure 'IIS Admin Service (IISADMIN)' is set to 'Disabled' or 'Not Installed'	Pass
1.0	5.7 (L1) Ensure 'Infrared monitor service (irmon)' is set to 'Disabled'	Fail
1.0	5.8 (L1) Ensure 'Internet Connection Sharing (ICS) (SharedAccess) ' is set to 'Disabled'	Fail
1.0	5.10 (L1) Ensure 'LxssManager (LxssManager)' is set to 'Disabled' or 'Not Installed'	Pass
1.0	5.11 (L1) Ensure 'Microsoft FTP Service (FTPSVC)' is set to 'Disabled' or 'Not Installed'	Pass
1.0	5.14 (L1) Ensure 'OpenSSH SSH Server (sshd)' is set to 'Disabled' or 'Not Installed'	Pass
1.0	5.24 (L1) Ensure 'Remote Procedure Call (RPC) Locator (RpcLocator)' is set to 'Disabled'	Fail
1.0	5.26 (L1) Ensure 'Routing and Remote Access (RemoteAccess)' is set to 'Disabled'	Pass
1.0	5.28 (L1) Ensure 'Simple TCP/IP Services (simptcp)' is set to 'Disabled' or 'Not Installed'	Pass
1.0	5.30 (L1) Ensure 'SSDP Discovery (SSDPSRV)' is set to 'Disabled'	Fail
1.0	5.31 (L1) Ensure 'UPnP Device Host (upnphost)' is set to 'Disabled'	Fail
1.0	5.32 (L1) Ensure 'Web Management Service (WMSvc)' is set to 'Disabled' or 'Not Installed'	Pass
1.0	5.35 (L1) Ensure 'Windows Media Player Network Sharing Service (WMPNetworkSvc)' is set to 'Disabled' or 'Not Installed'	Pass
1.0	5.36 (L1) Ensure 'Windows Mobile Hotspot Service (icssvc)' is set to 'Disabled'	Fail
1.0	5.40 (L1) Ensure 'World Wide Web Publishing Service (W3SVC)' is set to 'Disabled' or 'Not Installed'	Fail
1.0	5.41 (L1) Ensure 'Xbox Accessory Management Service (XboxGipSvc)' is set to 'Disabled'	Fail
1.0	5.42 (L1) Ensure 'Xbox Game Monitoring (xbgm)' is set to 'Disabled'	Fail
1.0	5.43 (L1) Ensure 'Xbox Live Auth Manager (XblAuthManager)' is set to 'Disabled'	Fail
1.0	5.44 (L1) Ensure 'Xbox Live Game Save (XblGameSave)' is set to 'Disabled'	Fail
1.0	5.45 (L1) Ensure 'Xbox Live Networking Service (XboxNetApiSvc)' is set to 'Disabled'	Fail
	6 Registry	
	7 File System	
	8 Wired Network (IEEE 802.3) Policies	
	9 Windows Firewall with Advanced Security	
	9.1 Domain Profile	
1.0	9.1.1 (L1) Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)'	Fail
1.0	9.1.2 (L1) Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)'	Fail
1.0	9.1.3 (L1) Ensure 'Windows Firewall: Domain: Outbound connections' is set to 'Allow (default)'	Fail
1.0	9.1.4 (L1) Ensure 'Windows Firewall: Domain: Settings: Display a notification' is set to 'No'	Fail
1.0	9.1.5 (L1) Ensure 'Windows Firewall: Domain: Logging: Name' is set to '%SYSTEMROOT%\System32\logfiles\firewall\domainfw.log'	Fail
1.0	9.1.6 (L1) Ensure 'Windows Firewall: Domain: Logging: Size limit (KB)' is set to '16,384 KB or greater'	Fail
1.0	9.1.7 (L1) Ensure 'Windows Firewall: Domain: Logging: Log dropped packets' is set to 'Yes'	Fail
1.0	9.1.8 (L1) Ensure 'Windows Firewall: Domain: Logging: Log successful connections' is set to 'Yes'	Fail
	9.2 Private Profile	
1.0	9.2.1 (L1) Ensure 'Windows Firewall: Private: Firewall state' is set to 'On (recommended)'	Fail
1.0	9.2.2 (L1) Ensure 'Windows Firewall: Private: Inbound connections' is set to 'Block (default)'	Fail

w	Benchmark Item	Result
1.0	9.2.3 (L1) Ensure 'Windows Firewall: Private: Outbound connections' is set to 'Allow (default)'	Fail
1.0	9.2.4 (L1) Ensure 'Windows Firewall: Private: Settings: Display a notification' is set to 'No'	Fail
1.0	9.2.5 (L1) Ensure 'Windows Firewall: Private: Logging: Name' is set to '%SYSTEMROOT%\System32\logfiles\firewall\privatefw.log'	Fail
1.0	9.2.6 (L1) Ensure 'Windows Firewall: Private: Logging: Size limit (KB)' is set to '16,384 KB or greater'	Fail
1.0	9.2.7 (L1) Ensure 'Windows Firewall: Private: Logging: Log dropped packets' is set to 'Yes'	Fail
1.0	9.2.8 (L1) Ensure 'Windows Firewall: Private: Logging: Log successful connections' is set to 'Yes'	Fail
9.3 Public Profile		
1.0	9.3.1 (L1) Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)'	Fail
1.0	9.3.2 (L1) Ensure 'Windows Firewall: Public: Inbound connections' is set to 'Block (default)'	Fail
1.0	9.3.3 (L1) Ensure 'Windows Firewall: Public: Outbound connections' is set to 'Allow (default)'	Fail
1.0	9.3.4 (L1) Ensure 'Windows Firewall: Public: Settings: Display a notification' is set to 'No'	Fail
1.0	9.3.5 (L1) Ensure 'Windows Firewall: Public: Settings: Apply local firewall rules' is set to 'No'	Fail
1.0	9.3.6 (L1) Ensure 'Windows Firewall: Public: Settings: Apply local connection security rules' is set to 'No'	Fail
1.0	9.3.7 (L1) Ensure 'Windows Firewall: Public: Logging: Name' is set to '%SYSTEMROOT%\System32\logfiles\firewall\publicfw.log'	Fail
1.0	9.3.8 (L1) Ensure 'Windows Firewall: Public: Logging: Size limit (KB)' is set to '16,384 KB or greater'	Fail
1.0	9.3.9 (L1) Ensure 'Windows Firewall: Public: Logging: Log dropped packets' is set to 'Yes'	Fail
1.0	9.3.10 (L1) Ensure 'Windows Firewall: Public: Logging: Log successful connections' is set to 'Yes'	Fail
10 Network List Manager Policies		
11 Wireless Network (IEEE 802.11) Policies		
12 Public Key Policies		
13 Software Restriction Policies		
14 Network Access Protection NAP Client Configuration		
15 Application Control Policies		
16 IP Security Policies		
17 Advanced Audit Policy Configuration		
17.1 Account Logon		
1.0	17.1.1 (L1) Ensure 'Audit Credential Validation' is set to 'Success and Failure'	Fail
17.2 Account Management		
1.0	17.2.1 (L1) Ensure 'Audit Application Group Management' is set to 'Success and Failure'	Fail
1.0	17.2.2 (L1) Ensure 'Audit Computer Account Management' is set to 'Success and Failure'	Fail
1.0	17.2.3 (L1) Ensure 'Audit Security Group Management' is set to include 'Success'	Pass
1.0	17.2.4 (L1) Ensure 'Audit User Account Management' is set to 'Success and Failure'	Fail
17.3 Detailed Tracking		
1.0	17.3.1 (L1) Ensure 'Audit PNP Activity' is set to include 'Success'	Fail
1.0	17.3.2 (L1) Ensure 'Audit Process Creation' is set to include 'Success'	Fail
17.4 DS Access		
17.5 Logon/Logoff		
1.0	17.5.1 (L1) Ensure 'Audit Account Lockout' is set to include 'Failure'	Fail
1.0	17.5.2 (L1) Ensure 'Audit Group Membership' is set to include 'Success'	Fail
1.0	17.5.3 (L1) Ensure 'Audit Logoff' is set to include 'Success'	Pass
1.0	17.5.4 (L1) Ensure 'Audit Logon' is set to 'Success and Failure'	Fail
1.0	17.5.5 (L1) Ensure 'Audit Other Logon/Logoff Events' is set to 'Success and Failure'	Fail
1.0	17.5.6 (L1) Ensure 'Audit Special Logon' is set to include 'Success'	Pass
17.6 Object Access		
1.0	17.6.1 (L1) Ensure 'Audit Detailed File Share' is set to include 'Failure'	Fail
1.0	17.6.2 (L1) Ensure 'Audit File Share' is set to 'Success and Failure'	Fail
1.0	17.6.3 (L1) Ensure 'Audit Other Object Access Events' is set to 'Success and Failure'	Fail
1.0	17.6.4 (L1) Ensure 'Audit Removable Storage' is set to 'Success and Failure'	Fail
17.7 Policy Change		
1.0	17.7.1 (L1) Ensure 'Audit Audit Policy Change' is set to include 'Success'	Pass
1.0	17.7.2 (L1) Ensure 'Audit Authentication Policy Change' is set to include 'Success'	Pass
1.0	17.7.3 (L1) Ensure 'Audit Authorization Policy Change' is set to include 'Success'	Fail
1.0	17.7.4 (L1) Ensure 'Audit MPSSVC Rule-Level Policy Change' is set to 'Success and Failure'	Fail
1.0	17.7.5 (L1) Ensure 'Audit Other Policy Change Events' is set to include 'Failure'	Fail

w	Benchmark Item	Result
	17.8 Privilege Use	
1.0	17.8.1 (L1) Ensure 'Audit Sensitive Privilege Use' is set to 'Success and Failure'	Fail
	17.9 System	
1.0	17.9.1 (L1) Ensure 'Audit IPsec Driver' is set to 'Success and Failure'	Fail
1.0	17.9.2 (L1) Ensure 'Audit Other System Events' is set to 'Success and Failure'	Pass
1.0	17.9.3 (L1) Ensure 'Audit Security State Change' is set to include 'Success'	Pass
1.0	17.9.4 (L1) Ensure 'Audit Security System Extension' is set to include 'Success'	Fail
1.0	17.9.5 (L1) Ensure 'Audit System Integrity' is set to 'Success and Failure'	Pass
	18 Administrative Templates (Computer)	
	18.1 Control Panel	
	18.1.1 Personalization	
1.0	18.1.1.1 (L1) Ensure 'Prevent enabling lock screen camera' is set to 'Enabled'	Fail
1.0	18.1.1.2 (L1) Ensure 'Prevent enabling lock screen slide show' is set to 'Enabled'	Fail
	18.1.2 Regional and Language Options	
	18.1.2.1 Handwriting personalization	
1.0	18.1.2.2 (L1) Ensure 'Allow input personalization' is set to 'Disabled'	Fail
	18.2 LAPS	
1.0	18.2.1 (L1) Ensure LAPS AdmPwd GPO Extension / CSE is installed	Fail
1.0	18.2.2 (L1) Ensure 'Do not allow password expiration time longer than required by policy' is set to 'Enabled'	Fail
1.0	18.2.3 (L1) Ensure 'Enable Local Admin Password Management' is set to 'Enabled'	Fail
1.0	18.2.4 (L1) Ensure 'Password Settings: Password Complexity' is set to 'Enabled: Large letters + small letters + numbers + special characters'	Fail
1.0	18.2.5 (L1) Ensure 'Password Settings: Password Length' is set to 'Enabled: 15 or more'	Fail
1.0	18.2.6 (L1) Ensure 'Password Settings: Password Age (Days)' is set to 'Enabled: 30 or fewer'	Fail
	18.3 MS Security Guide	
1.0	18.3.1 (L1) Ensure 'Apply UAC restrictions to local accounts on network logons' is set to 'Enabled'	Fail
1.0	18.3.2 (L1) Ensure 'Configure SMB v1 client driver' is set to 'Enabled: Disable driver'	Fail
1.0	18.3.3 (L1) Ensure 'Configure SMB v1 server' is set to 'Disabled'	Fail
1.0	18.3.4 (L1) Ensure 'Enable Structured Exception Handling Overwrite Protection (SEHOP)' is set to 'Enabled'	Fail
1.0	18.3.5 (L1) Ensure 'Turn on Windows Defender protection against Potentially Unwanted Applications' is set to 'Enabled'	Fail
1.0	18.3.6 (L1) Ensure 'WDigest Authentication' is set to 'Disabled'	Fail
	18.4 MSS (Legacy)	
1.0	18.4.1 (L1) Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled'	Fail
1.0	18.4.2 (L1) Ensure 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled'	Fail
1.0	18.4.3 (L1) Ensure 'MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled'	Fail
1.0	18.4.5 (L1) Ensure 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' is set to 'Disabled'	Fail
1.0	18.4.7 (L1) Ensure 'MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers' is set to 'Enabled'	Fail
1.0	18.4.9 (L1) Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' is set to 'Enabled'	Fail
1.0	18.4.10 (L1) Ensure 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)' is set to 'Enabled: 5 or fewer seconds'	Fail
1.0	18.4.13 (L1) Ensure 'MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning' is set to 'Enabled: 90% or less'	Fail
	18.5 Network	
	18.5.1 Background Intelligent Transfer Service (BITS)	
	18.5.2 BranchCache	
	18.5.3 DirectAccess Client Experience Settings	
	18.5.4 DNS Client	
1.0	18.5.4.1 (L1) Set 'NetBIOS node type' to 'P-node' (Ensure NetBT Parameter 'NodeType' is set to '0x2 (2)')	Fail
1.0	18.5.4.2 (L1) Ensure 'Turn off multicast name resolution' is set to 'Enabled'	Pass
	18.5.5 Fonts	
	18.5.6 Hotspot Authentication	
	18.5.7 Lanman Server	
	18.5.8 Lanman Workstation	

w	Benchmark Item	Result
1.0	18.5.8.1 (L1) Ensure 'Enable insecure guest logons' is set to 'Disabled'	Fail
	18.5.9 Link-Layer Topology Discovery	
	18.5.10 Microsoft Peer-to-Peer Networking Services	
	18.5.10.1 Peer Name Resolution Protocol	
	18.5.11 Network Connections	
	18.5.11.1 Windows Defender Firewall (formerly Windows Firewall)	
1.0	18.5.11.2 (L1) Ensure 'Prohibit installation and configuration of Network Bridge on your DNS domain network' is set to 'Enabled'	Fail
1.0	18.5.11.3 (L1) Ensure 'Prohibit use of Internet Connection Sharing on your DNS domain network' is set to 'Enabled'	Fail
1.0	18.5.11.4 (L1) Ensure 'Require domain users to elevate when setting a network's location' is set to 'Enabled'	Fail
	18.5.12 Network Connectivity Status Indicator	
	18.5.13 Network Isolation	
	18.5.14 Network Provider	
1.0	18.5.14.1 (L1) Ensure 'Hardened UNC Paths' is set to 'Enabled, with "Require Mutual Authentication" and "Require Integrity" set for all NETLOGON and SYSVOL shares'	Fail
	18.5.15 Offline Files	
	18.5.16 QoS Packet Scheduler	
	18.5.17 SNMP	
	18.5.18 SSL Configuration Settings	
	18.5.19 TCPIP Settings	
	18.5.19.1 IPv6 Transition Technologies	
	18.5.19.2 Parameters	
	18.5.20 Windows Connect Now	
	18.5.21 Windows Connection Manager	
1.0	18.5.21.1 (L1) Ensure 'Minimize the number of simultaneous connections to the Internet or a Windows Domain' is set to 'Enabled'	Fail
1.0	18.5.21.2 (L1) Ensure 'Prohibit connection to non-domain networks when connected to domain authenticated network' is set to 'Enabled'	Fail
	18.5.22 Wireless Display	
	18.5.23 WLAN Service	
	18.5.23.1 WLAN Media Cost	
	18.5.23.2 WLAN Settings	
1.0	18.5.23.2.1 (L1) Ensure 'Allow Windows to automatically connect to suggested open hotspots, to networks shared by contacts, and to hotspots offering paid services' is set to 'Disabled'	Fail
	18.6 Printers	
	18.7 Start Menu and Taskbar	
	18.7.1 Notifications	
	18.8 System	
	18.8.1 Access-Denied Assistance	
	18.8.2 App-V	
	18.8.3 Audit Process Creation	
1.0	18.8.3.1 (L1) Ensure 'Include command line in process creation events' is set to 'Disabled'	Fail
	18.8.4 Credentials Delegation	
1.0	18.8.4.1 (L1) Ensure 'Encryption Oracle Remediation' is set to 'Enabled: Force Updated Clients'	Fail
1.0	18.8.4.2 (L1) Ensure 'Remote host allows delegation of non-exportable credentials' is set to 'Enabled'	Fail
	18.8.5 Device Guard	
	18.8.6 Device Health Attestation Service	
	18.8.7 Device Installation	
	18.8.7.1 Device Installation Restrictions	
	18.8.8 Device Redirection	
	18.8.9 Disk NV Cache	
	18.8.10 Disk Quotas	
	18.8.11 Display	
	18.8.12 Distributed COM	
	18.8.13 Driver Installation	
	18.8.14 Early Launch Antimalware	
1.0	18.8.14.1 (L1) Ensure 'Boot-Start Driver Initialization Policy' is set to 'Enabled: Good, unknown and bad but critical'	Fail
	18.8.15 Enhanced Storage Access	
	18.8.16 File Classification Infrastructure	
	18.8.17 File Share Shadow Copy Agent	

w	Benchmark Item	Result
	18.8.18 File Share Shadow Copy Provider	
	18.8.19 Filesystem (formerly NTFS Filesystem)	
	18.8.20 Folder Redirection	
	18.8.21 Group Policy	
	18.8.21.1 Logging and tracing	
1.0	18.8.21.2 (L1) Ensure 'Configure registry policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE'	Fail
1.0	18.8.21.3 (L1) Ensure 'Configure registry policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE'	Fail
1.0	18.8.21.4 (L1) Ensure 'Continue experiences on this device' is set to 'Disabled'	Fail
1.0	18.8.21.5 (L1) Ensure 'Turn off background refresh of Group Policy' is set to 'Disabled'	Pass
	18.8.22 Internet Communication Management	
	18.8.22.1 Internet Communication settings	
1.0	18.8.22.1.6 (L1) Ensure 'Turn off Internet download for Web publishing and online ordering wizards' is set to 'Enabled'	Fail
1.0	18.8.22.1.7 (L1) Ensure 'Turn off printing over HTTP' is set to 'Enabled'	Fail
	18.8.23 iSCSI	
	18.8.24 KDC	
	18.8.25 Kerberos	
	18.8.26 Locale Services	
	18.8.27 Logon	
1.0	18.8.27.1 (L1) Ensure 'Block user from showing account details on sign-in' is set to 'Enabled'	Fail
1.0	18.8.27.2 (L1) Ensure 'Do not display network selection UI' is set to 'Enabled'	Pass
1.0	18.8.27.3 (L1) Ensure 'Do not enumerate connected users on domain-joined computers' is set to 'Enabled'	Fail
1.0	18.8.27.4 (L1) Ensure 'Enumerate local users on domain-joined computers' is set to 'Disabled'	Fail
1.0	18.8.27.5 (L1) Ensure 'Turn off app notifications on the lock screen' is set to 'Enabled'	Fail
1.0	18.8.27.6 (L1) Ensure 'Turn off picture password sign-in' is set to 'Enabled'	Fail
1.0	18.8.27.7 (L1) Ensure 'Turn on convenience PIN sign-in' is set to 'Disabled'	Fail
	18.8.28 Mitigation Options	
	18.8.29 Net Logon	
	18.8.30 OS Policies	
	18.8.31 Performance Control Panel	
	18.8.32 PIN Complexity	
	18.8.33 Power Management	
	18.8.33.1 Button Settings	
	18.8.33.2 Energy Saver Settings	
	18.8.33.3 Hard Disk Settings	
	18.8.33.4 Notification Settings	
	18.8.33.5 Power Throttling Settings	
	18.8.33.6 Sleep Settings	
1.0	18.8.33.6.1 (L1) Ensure 'Allow network connectivity during connected-standby (on battery)' is set to 'Disabled'	Fail
1.0	18.8.33.6.2 (L1) Ensure 'Allow network connectivity during connected-standby (plugged in)' is set to 'Disabled'	Fail
1.0	18.8.33.6.5 (L1) Ensure 'Require a password when a computer wakes (on battery)' is set to 'Enabled'	Fail
1.0	18.8.33.6.6 (L1) Ensure 'Require a password when a computer wakes (plugged in)' is set to 'Enabled'	Fail
	18.8.34 Recovery	
	18.8.35 Remote Assistance	
1.0	18.8.35.1 (L1) Ensure 'Configure Offer Remote Assistance' is set to 'Disabled'	Fail
1.0	18.8.35.2 (L1) Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled'	Fail
	18.8.36 Remote Procedure Call	
1.0	18.8.36.1 (L1) Ensure 'Enable RPC Endpoint Mapper Client Authentication' is set to 'Enabled'	Fail
1.0	18.8.36.2 (L1) Ensure 'Restrict Unauthenticated RPC clients' is set to 'Enabled: Authenticated'	Fail
	18.8.37 Removable Storage Access	
	18.8.38 Scripts	
	18.8.39 Server Manager	
	18.8.40 Shutdown	
	18.8.41 Shutdown Options	
	18.8.42 Storage Health	

w	Benchmark Item	Result
	18.8.43 System Restore	
	18.8.44 Troubleshooting and Diagnostics	
	18.8.44.1 Application Compatibility Diagnostics	
	18.8.44.2 Corrupted File Recovery	
	18.8.44.3 Disk Diagnostic	
	18.8.44.4 Fault Tolerant Heap	
	18.8.44.5 Microsoft Support Diagnostic Tool	
	18.8.44.6 MSI Corrupted File Recovery	
	18.8.44.7 Scheduled Maintenance	
	18.8.44.8 Scripted Diagnostics	
	18.8.44.9 Windows Boot Performance Diagnostics	
	18.8.44.10 Windows Memory Leak Diagnosis	
	18.8.44.11 Windows Performance PerfTrack	
	18.8.45 Trusted Platform Module Services	
	18.8.46 User Profiles	
	18.8.47 Windows File Protection	
	18.8.48 Windows HotStart	
	18.8.49 Windows Time Service	
	18.8.49.1 Time Providers	
	18.9 Windows Components	
	18.9.1 Active Directory Federation Services	
	18.9.2 ActiveX Installer Service	
	18.9.3 Add features to Windows 8 / 8.1 / 10 (formerly Windows Anytime Upgrade)	
	18.9.4 App Package Deployment	
	18.9.5 App Privacy	
	18.9.6 App runtime	
1.0	18.9.6.1 (L1) Ensure 'Allow Microsoft accounts to be optional' is set to 'Enabled'	Fail
	18.9.7 Application Compatibility	
	18.9.8 AutoPlay Policies	
1.0	18.9.8.1 (L1) Ensure 'Disallow Autoplay for non-volume devices' is set to 'Enabled'	Fail
1.0	18.9.8.2 (L1) Ensure 'Set the default behavior for AutoRun' is set to 'Enabled: Do not execute any autorun commands'	Fail
1.0	18.9.8.3 (L1) Ensure 'Turn off Autoplay' is set to 'Enabled: All drives'	Fail
	18.9.9 Backup	
	18.9.10 Biometrics	
	18.9.10.1 Facial Features	
1.0	18.9.10.1.1 (L1) Ensure 'Configure enhanced anti-spoofing' is set to 'Enabled'	Fail
	18.9.11 BitLocker Drive Encryption	
	18.9.11.1 Fixed Data Drives	
	18.9.11.2 Operating System Drives	
	18.9.11.3 Removable Data Drives	
	18.9.12 Camera	
	18.9.13 Cloud Content	
1.0	18.9.13.1 (L1) Ensure 'Turn off Microsoft consumer experiences' is set to 'Enabled'	Fail
	18.9.14 Connect	
1.0	18.9.14.1 (L1) Ensure 'Require pin for pairing' is set to 'Enabled'	Fail
	18.9.15 Credential User Interface	
1.0	18.9.15.1 (L1) Ensure 'Do not display the password reveal button' is set to 'Enabled'	Fail
1.0	18.9.15.2 (L1) Ensure 'Enumerate administrator accounts on elevation' is set to 'Disabled'	Fail
	18.9.16 Data Collection and Preview Builds	
1.0	18.9.16.1 (L1) Ensure 'Allow Telemetry' is set to 'Enabled: 0 - Security [Enterprise Only]' or 'Enabled: 1 - Basic'	Fail
1.0	18.9.16.3 (L1) Ensure 'Do not show feedback notifications' is set to 'Enabled'	Fail
1.0	18.9.16.4 (L1) Ensure 'Toggle user control over Insider builds' is set to 'Disabled'	Fail
	18.9.17 Delivery Optimization	
1.0	18.9.17.1 (L1) Ensure 'Download Mode' is NOT set to 'Enabled: Internet'	Pass
	18.9.18 Desktop Gadgets	
	18.9.19 Desktop Window Manager	
	18.9.20 Device and Driver Compatibility	

w	Benchmark Item	Result
	18.9.21 Device Registration (formerly Workplace Join)	
	18.9.22 Digital Locker	
	18.9.23 Edge UI	
	18.9.24 EMET	
	18.9.25 Event Forwarding	
	18.9.26 Event Log Service	
	18.9.26.1 Application	
1.0	18.9.26.1.1 (L1) Ensure 'Application: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'	Fail
1.0	18.9.26.1.2 (L1) Ensure 'Application: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'	Fail
	18.9.26.2 Security	
1.0	18.9.26.2.1 (L1) Ensure 'Security: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'	Fail
1.0	18.9.26.2.2 (L1) Ensure 'Security: Specify the maximum log file size (KB)' is set to 'Enabled: 196,608 or greater'	Fail
	18.9.26.3 Setup	
1.0	18.9.26.3.1 (L1) Ensure 'Setup: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'	Fail
1.0	18.9.26.3.2 (L1) Ensure 'Setup: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'	Fail
	18.9.26.4 System	
1.0	18.9.26.4.1 (L1) Ensure 'System: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'	Fail
1.0	18.9.26.4.2 (L1) Ensure 'System: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'	Fail
	18.9.27 Event Logging	
	18.9.28 Event Viewer	
	18.9.29 Family Safety (formerly Parental Controls)	
	18.9.30 File Explorer (formerly Windows Explorer)	
	18.9.30.1 Previous Versions	
1.0	18.9.30.2 (L1) Ensure 'Turn off Data Execution Prevention for Explorer' is set to 'Disabled'	Fail
1.0	18.9.30.3 (L1) Ensure 'Turn off heap termination on corruption' is set to 'Disabled'	Fail
1.0	18.9.30.4 (L1) Ensure 'Turn off shell protocol protected mode' is set to 'Disabled'	Fail
	18.9.31 File History	
	18.9.32 Find My Device	
	18.9.33 Game Explorer	
	18.9.34 Handwriting	
	18.9.35 HomeGroup	
1.0	18.9.35.1 (L1) Ensure 'Prevent the computer from joining a homegroup' is set to 'Enabled'	Fail
	18.9.36 Import Video	
	18.9.37 Internet Explorer	
	18.9.38 Internet Information Services	
	18.9.39 Location and Sensors	
	18.9.39.1 Windows Location Provider	
	18.9.40 Maintenance Scheduler	
	18.9.41 Maps	
	18.9.42 MDM	
	18.9.43 Messaging	
	18.9.44 Microsoft account	
1.0	18.9.44.1 (L1) Ensure 'Block all consumer Microsoft account user authentication' is set to 'Enabled'	Fail
	18.9.45 Microsoft Edge	
1.0	18.9.45.4 (L1) Ensure 'Configure cookies' is set to 'Enabled: Block only 3rd-party cookies' or higher	Fail
1.0	18.9.45.5 (L1) Ensure 'Configure Password Manager' is set to 'Disabled'	Fail
1.0	18.9.45.8 (L1) Ensure 'Configure the Adobe Flash Click-to-Run setting' is set to 'Enabled'	Fail
	18.9.46 Microsoft FIDO Authentication	
	18.9.47 Microsoft Secondary Authentication Factor	
	18.9.48 Microsoft User Experience Virtualization	
	18.9.49 NetMeeting	
	18.9.50 Network Access Protection	
	18.9.51 Network Projector	
	18.9.52 OneDrive (formerly SkyDrive)	
1.0	18.9.52.1 (L1) Ensure 'Prevent the usage of OneDrive for file storage' is set to 'Enabled'	Pass
	18.9.53 Online Assistance	

w	Benchmark Item	Result
	18.9.54 Password Synchronization	
	18.9.55 Portable Operating System	
	18.9.56 Presentation Settings	
	18.9.57 Push To Install	
	18.9.58 Remote Desktop Services (formerly Terminal Services)	
	18.9.58.1 RD Licensing (formerly TS Licensing)	
	18.9.58.2 Remote Desktop Connection Client	
	18.9.58.2.1 RemoteFX USB Device Redirection	
1.0	18.9.58.2.2 (L1) Ensure 'Do not allow passwords to be saved' is set to 'Enabled'	Fail
	18.9.58.3 Remote Desktop Session Host (formerly Terminal Server)	
	18.9.58.3.1 Application Compatibility	
	18.9.58.3.2 Connections	
	18.9.58.3.3 Device and Resource Redirection	
1.0	18.9.58.3.3.2 (L1) Ensure 'Do not allow drive redirection' is set to 'Enabled'	Fail
	18.9.58.3.4 Licensing	
	18.9.58.3.5 Printer Redirection	
	18.9.58.3.6 Profiles	
	18.9.58.3.7 RD Connection Broker (formerly TS Connection Broker)	
	18.9.58.3.8 Remote Session Environment	
	18.9.58.3.9 Security	
1.0	18.9.58.3.9.1 (L1) Ensure 'Always prompt for password upon connection' is set to 'Enabled'	Fail
1.0	18.9.58.3.9.2 (L1) Ensure 'Require secure RPC communication' is set to 'Enabled'	Fail
1.0	18.9.58.3.9.3 (L1) Ensure 'Require use of specific security layer for remote (RDP) connections' is set to 'Enabled: SSL'	Fail
1.0	18.9.58.3.9.4 (L1) Ensure 'Require user authentication for remote connections by using Network Level Authentication' is set to 'Enabled'	Fail
1.0	18.9.58.3.9.5 (L1) Ensure 'Set client connection encryption level' is set to 'Enabled: High Level'	Fail
	18.9.58.3.10 Session Time Limits	
	18.9.58.3.11 Temporary folders	
1.0	18.9.58.3.11.1 (L1) Ensure 'Do not delete temp folders upon exit' is set to 'Disabled'	Fail
1.0	18.9.58.3.11.2 (L1) Ensure 'Do not use temporary folders per session' is set to 'Disabled'	Fail
	18.9.59 RSS Feeds	
1.0	18.9.59.1 (L1) Ensure 'Prevent downloading of enclosures' is set to 'Enabled'	Fail
	18.9.60 Search	
	18.9.60.1 OCR	
1.0	18.9.60.3 (L1) Ensure 'Allow Cortana' is set to 'Disabled'	Fail
1.0	18.9.60.4 (L1) Ensure 'Allow Cortana above lock screen' is set to 'Disabled'	Fail
1.0	18.9.60.5 (L1) Ensure 'Allow indexing of encrypted files' is set to 'Disabled'	Fail
1.0	18.9.60.6 (L1) Ensure 'Allow search and Cortana to use location' is set to 'Disabled'	Fail
	18.9.61 Security Center	
	18.9.62 Server for NIS	
	18.9.63 Shutdown Options	
	18.9.64 Smart Card	
	18.9.65 Software Protection Platform	
	18.9.66 Sound Recorder	
	18.9.67 Speech	
	18.9.68 Store	
1.0	18.9.68.2 (L1) Ensure 'Only display the private store within the Microsoft Store' is set to 'Enabled'	Fail
1.0	18.9.68.3 (L1) Ensure 'Turn off Automatic Download and Install of updates' is set to 'Disabled'	Fail
1.0	18.9.68.4 (L1) Ensure 'Turn off the offer to update to the latest version of Windows' is set to 'Enabled'	Fail
	18.9.69 Sync your settings	
	18.9.70 Tablet PC	
	18.9.71 Task Scheduler	
	18.9.72 Text Input	
	18.9.73 Windows Calendar	
	18.9.74 Windows Color System	
	18.9.75 Windows Customer Experience Improvement Program	
	18.9.76 Windows Defender Antivirus (formerly Windows Defender)	

w	Benchmark Item	Result
	18.9.76.1 Client Interface	
	18.9.76.2 Exclusions	
	18.9.76.3 MAPS	
1.0	18.9.76.3.1 (L1) Ensure 'Configure local setting override for reporting to Microsoft MAPS' is set to 'Disabled'	Fail
	18.9.76.4 MpEngine	
	18.9.76.5 Network Inspection System	
	18.9.76.6 Quarantine	
	18.9.76.7 Real-time Protection	
1.0	18.9.76.7.1 (L1) Ensure 'Turn on behavior monitoring' is set to 'Enabled'	Fail
	18.9.76.8 Remediation	
	18.9.76.9 Reporting	
	18.9.76.10 Scan	
1.0	18.9.76.10.1 (L1) Ensure 'Scan removable drives' is set to 'Enabled'	Fail
1.0	18.9.76.10.2 (L1) Ensure 'Turn on e-mail scanning' is set to 'Enabled'	Fail
	18.9.76.11 Signature Updates	
	18.9.76.12 Threats	
	18.9.76.13 Windows Defender Exploit Guard	
	18.9.76.13.1 Attack Surface Reduction	
1.0	18.9.76.13.1.1 (L1) Ensure 'Configure Attack Surface Reduction rules' is set to 'Enabled'	Fail
1.0	18.9.76.13.1.2 (L1) Ensure 'Configure Attack Surface Reduction rules: Set the state for each ASR rule' is 'configured'	Fail
	18.9.76.13.2 Controlled Folder Access	
	18.9.76.13.3 Network Protection	
1.0	18.9.76.13.3.1 (L1) Ensure 'Prevent users and apps from accessing dangerous websites' is set to 'Enabled: Block'	Fail
1.0	18.9.76.14 (L1) Ensure 'Turn off Windows Defender AntiVirus' is set to 'Disabled'	Fail
	18.9.77 Windows Defender Application Guard	
	18.9.78 Windows Defender Exploit Guard	
	18.9.79 Windows Defender Security Center	
	18.9.79.1 Account protection	
	18.9.79.2 App and browser protection	
1.0	18.9.79.2.1 (L1) Ensure 'Prevent users from modifying settings' is set to 'Enabled'	Fail
	18.9.80 Windows Defender SmartScreen	
	18.9.80.1 Explorer	
1.0	18.9.80.1.1 (L1) Ensure 'Configure Windows Defender SmartScreen' is set to 'Enabled: Warn and prevent bypass'	Fail
	18.9.80.2 Microsoft Edge	
1.0	18.9.80.2.1 (L1) Ensure 'Configure Windows Defender SmartScreen' is set to 'Enabled'	Fail
1.0	18.9.80.2.2 (L1) Ensure 'Prevent bypassing Windows Defender SmartScreen prompts for files' is set to 'Enabled'	Fail
1.0	18.9.80.2.3 (L1) Ensure 'Prevent bypassing Windows Defender SmartScreen prompts for sites' is set to 'Enabled'	Fail
	18.9.81 Windows Error Reporting	
	18.9.82 Windows Game Recording and Broadcasting	
1.0	18.9.82.1 (L1) Ensure 'Enables or disables Windows Game Recording and Broadcasting' is set to 'Disabled'	Fail
	18.9.83 Windows Hello for Business (formerly Microsoft Passport for Work)	
	18.9.84 Windows Ink Workspace	
1.0	18.9.84.2 (L1) Ensure 'Allow Windows Ink Workspace' is set to 'Enabled: On, but disallow access above lock' OR 'Disabled' but not 'Enabled: On'	Fail
	18.9.85 Windows Installer	
1.0	18.9.85.1 (L1) Ensure 'Allow user control over installs' is set to 'Disabled'	Fail
1.0	18.9.85.2 (L1) Ensure 'Always install with elevated privileges' is set to 'Disabled'	Fail
	18.9.86 Windows Logon Options	
1.0	18.9.86.1 (L1) Ensure 'Sign-in last interactive user automatically after a system-initiated restart' is set to 'Disabled'	Fail
	18.9.87 Windows Mail	
	18.9.88 Windows Media Center	
	18.9.89 Windows Media Digital Rights Management	
	18.9.90 Windows Media Player	
	18.9.91 Windows Meeting Space	
	18.9.92 Windows Messenger	
	18.9.93 Windows Mobility Center	
	18.9.94 Windows Movie Maker	

w	Benchmark Item	Result
	18.9.95 Windows PowerShell	
1.0	18.9.95.1 (L1) Ensure 'Turn on PowerShell Script Block Logging' is set to 'Disabled'	Fail
1.0	18.9.95.2 (L1) Ensure 'Turn on PowerShell Transcription' is set to 'Disabled'	Fail
	18.9.96 Windows Reliability Analysis	
	18.9.97 Windows Remote Management (WinRM)	
	18.9.97.1 WinRM Client	
1.0	18.9.97.1.1 (L1) Ensure 'Allow Basic authentication' is set to 'Disabled'	Fail
1.0	18.9.97.1.2 (L1) Ensure 'Allow unencrypted traffic' is set to 'Disabled'	Fail
1.0	18.9.97.1.3 (L1) Ensure 'Disallow Digest authentication' is set to 'Enabled'	Fail
	18.9.97.2 WinRM Service	
1.0	18.9.97.2.1 (L1) Ensure 'Allow Basic authentication' is set to 'Disabled'	Fail
1.0	18.9.97.2.3 (L1) Ensure 'Allow unencrypted traffic' is set to 'Disabled'	Fail
1.0	18.9.97.2.4 (L1) Ensure 'Disallow WinRM from storing RunAs credentials' is set to 'Enabled'	Fail
	18.9.98 Windows Remote Shell	
	18.9.99 Windows SideShow	
	18.9.100 Windows System Resource Manager	
	18.9.101 Windows Update	
	18.9.101.1 Windows Update for Business (formerly Defer Windows Updates)	
1.0	18.9.101.1.1 (L1) Ensure 'Manage preview builds' is set to 'Enabled: Disable preview builds'	Fail
1.0	18.9.101.1.2 (L1) Ensure 'Select when Preview Builds and Feature Updates are received' is set to 'Enabled: Semi-Annual Channel, 180 or more days'	Fail
1.0	18.9.101.1.3 (L1) Ensure 'Select when Quality Updates are received' is set to 'Enabled: 0 days'	Fail
1.0	18.9.101.2 (L1) Ensure 'Configure Automatic Updates' is set to 'Enabled'	Pass
1.0	18.9.101.3 (L1) Ensure 'Configure Automatic Updates: Scheduled install day' is set to '0 - Every day'	Pass
1.0	18.9.101.4 (L1) Ensure 'No auto-restart with logged on users for scheduled automatic updates installations' is set to 'Disabled'	Fail
	19 Administrative Templates (User)	
	19.1 Control Panel	
	19.1.1 Add or Remove Programs	
	19.1.2 Display	
	19.1.3 Personalization (formerly Desktop Themes)	
1.0	19.1.3.1 (L1) Ensure 'Enable screen saver' is set to 'Enabled'	Fail
1.0	19.1.3.2 (L1) Ensure 'Force specific screen saver: Screen saver executable name' is set to 'Enabled: scrnsave.scr'	Fail
1.0	19.1.3.3 (L1) Ensure 'Password protect the screen saver' is set to 'Enabled'	Fail
1.0	19.1.3.4 (L1) Ensure 'Screen saver timeout' is set to 'Enabled: 900 seconds or fewer, but not 0'	Fail
	19.2 Desktop	
	19.3 Network	
	19.4 Shared Folders	
	19.5 Start Menu and Taskbar	
	19.5.1 Notifications	
1.0	19.5.1.1 (L1) Ensure 'Turn off toast notifications on the lock screen' is set to 'Enabled'	Fail
	19.6 System	
	19.6.1 Ctrl+Alt+Del Options	
	19.6.2 Display	
	19.6.3 Driver Installation	
	19.6.4 Folder Redirection	
	19.6.5 Group Policy	
	19.6.6 Internet Communication Management	
	19.6.6.1 Internet Communication settings	
	19.7 Windows Components	
	19.7.1 Add features to Windows 8 / 8.1 / 10 (formerly Windows Anytime Upgrade)	
	19.7.2 App runtime	
	19.7.3 Application Compatibility	
	19.7.4 Attachment Manager	
1.0	19.7.4.1 (L1) Ensure 'Do not preserve zone information in file attachments' is set to 'Disabled'	Fail
1.0	19.7.4.2 (L1) Ensure 'Notify antivirus programs when opening attachments' is set to 'Enabled'	Fail
	19.7.5 AutoPlay Policies	

w	Benchmark Item	Result
	19.7.6 Backup	
	19.7.7 Cloud Content	
1.0	19.7.7.1 (L1) Ensure 'Configure Windows spotlight on lock screen' is set to Disabled'	Fail
1.0	19.7.7.2 (L1) Ensure 'Do not suggest third-party content in Windows spotlight' is set to 'Enabled'	Fail
	19.7.8 Credential User Interface	
	19.7.9 Data Collection and Preview Builds	
	19.7.10 Desktop Gadgets	
	19.7.11 Desktop Window Manager	
	19.7.12 Digital Locker	
	19.7.13 Edge UI	
	19.7.14 File Explorer (formerly Windows Explorer)	
	19.7.15 File Revocation	
	19.7.16 IME	
	19.7.17 Import Video	
	19.7.18 Instant Search	
	19.7.19 Internet Explorer	
	19.7.20 Location and Sensors	
	19.7.21 Microsoft Edge	
	19.7.22 Microsoft Management Console	
	19.7.23 Microsoft User Experience Virtualization	
	19.7.24 NetMeeting	
	19.7.25 Network Projector	
	19.7.26 Network Sharing	
1.0	19.7.26.1 (L1) Ensure 'Prevent users from sharing files within their profile.' is set to 'Enabled'	Fail
	19.7.27 Presentation Settings	
	19.7.28 Remote Desktop Services (formerly Terminal Services)	
	19.7.29 RSS Feeds	
	19.7.30 Search	
	19.7.31 Sound Recorder	
	19.7.32 Store	
	19.7.33 Tablet PC	
	19.7.34 Task Scheduler	
	19.7.35 Windows Calendar	
	19.7.36 Windows Color System	
	19.7.37 Windows Defender SmartScreen	
	19.7.38 Windows Error Reporting	
	19.7.39 Windows Hello for Business (formerly Microsoft Passport for Work)	
	19.7.40 Windows Installer	
1.0	19.7.40.1 (L1) Ensure 'Always install with elevated privileges' is set to 'Disabled'	Fail
	19.7.41 Windows Logon Options	
	19.7.42 Windows Mail	
	19.7.43 Windows Media Center	
	19.7.44 Windows Media Player	
	19.7.44.1 Networking	
	19.7.44.2 Playback	

⇧

Assessment Details

1 Account Policies

This section contains recommendations for account policies.

1.1 Password Policy

This section contains recommendations for password policy.

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

Fail

Description:

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

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

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.

Remediation:

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

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

Impact:

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

Assessment:

Ensure 'Password Hist Len' is 'Greater Than Or Equal' to '24' -- Less

CIS-CAT Expected...	CIS-CAT Collected...
the *Enforce Password History* to be greater than or equal to **24**	0

References:

- **CCE-IDv5:** CCE-35219-5 -- More

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

1.1.2 (L1) Ensure 'Maximum password age' is set to '60 or fewer days, but not 0'

Fail

Description:

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

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

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

The recommended state for this setting is `60 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.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `60 or fewer days, but not 0`:

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

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.

Assessment:

All of the following tests or sub-groups must pass:

Ensure 'Max Passwd Age' is 'Less Than Or Equal' to '5184000' -- More

Ensure 'Max Passwd Age' is 'Greater Than' to '0' -- Less

CIS-CAT Expected...	CIS-CAT Collected...
the *Max Password Age* to be greater than **0**	0

References:

- **CCE-IDv5:** CCE-34907-6 -- More

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

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

Fail

Description:

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

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

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 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.

Remediation:

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

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

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.

Assessment:

Ensure 'Min Passwd Age' is 'Greater Than Or Equal' to '86400' -- Less

CIS-CAT Expected...	CIS-CAT Collected...
the *Min Password Age* to be greater than or equal to **86400**	0

References:

- **CCE-IDv5:** CCE-35366-4 -- More

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

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

Fail

Description:

This policy setting determines the least number of characters that make up a password for a user account. There are many different theories about how to determine the best password length for an organization, but perhaps "pass phrase" is a better term than "password." In Microsoft Windows 2000 and newer, pass phrases can be quite long and can include spaces. Therefore, a phrase such as "I want to drink a $5 milkshake" is a valid pass phrase; it is a considerably stronger password than an 8 or 10 character string of random numbers and letters, and yet is easier to remember. Users must be educated about the proper selection and maintenance of passwords, especially with regard to password length.

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.

Remediation:

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

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

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 pass phrases, which are often easier to remember and, due to the larger number of character combinations, much harder to discover.

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

Assessment:

Ensure 'Min Passwd Len' is 'Greater Than Or Equal' to '14' -- Less

CIS-CAT Expected...	CIS-CAT Collected...
the *Min Password Length* to be greater than or equal to **14**	0

References:

- **CCE-IDv5:** CCE-33789-9 -- More

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More
- **Control 16: Account Monitoring and Control:** -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More
- **Control 5: Controlled Use of Administrative Privileges:** -- More
- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

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

Unknown

Description:

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

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

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

Each additional character in a password increases its complexity exponentially. For instance, a seven-character, all lower-case alphabetic password would have 267 (approximately 8 x 109 or 8 billion) possible combinations. At 1,000,000 attempts per second (a capability of many password-cracking utilities), it would only take 133 minutes to crack. A seven-character alphabetic password with case sensitivity has 527 combinations. A seven-character case-sensitive alphanumeric password without punctuation has 627 combinations. An eight-character password has 268 (or 2 x 1011) possible combinations. Although this might seem to be a large number, at 1,000,000 attempts per second it would take only 59 hours to try all possible passwords. Remember, these times will significantly increase for passwords that use ALT characters and other special keyboard characters such as "!" or "@". Proper use of the password settings can help make it difficult to mount a brute force attack.

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

Rationale:

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

Remediation:

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

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

Impact:

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

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

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

Assessment:

Ensure Password Policy Setting equals 1 (boolean) -- More

References:

- **CCE-IDv5:** CCE-33777-4 -- More

Back to Summary

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

Unknown

Description:

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

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

Rationale:

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

Remediation:

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

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

Impact:

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

Assessment:

Ensure 'Reversible Encryption' is 'Equals' to '0' -- More

References:

- **CCE-IDv5:** CCE-35370-6 -- More

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More
- **Control 16: Account Monitoring and Control:** -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More
- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

1.2 Account Lockout Policy

This section contains recommendations for account lockout policy.

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

Pass

Description:

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

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

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

Rationale:

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

Remediation:

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

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

Impact:

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

Assessment:

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

References:

- **CCE-IDv5:** CCE-35409-2 -- More

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More
- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

1.2.2 (L1) Ensure 'Account lockout threshold' is set to '10 or fewer invalid logon attempt(s), but not 0'

Fail

Description:

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

The recommended state for this setting is: `10 or fewer invalid logon attempt(s), but not 0`.

Rationale:

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

Remediation:

To establish the recommended configuration via GP, set the following UI path to `10 or fewer invalid login attempt(s), but not 0`:

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

Impact:

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

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

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

Assessment:

All of the following tests or sub-groups must pass:

Ensure 'Account lockout threshold' is set to '10 or fewer invalid logon attempt(s)' -- More

Ensure 'Account lockout threshold' is set to 'Not 0' -- Less

CIS-CAT Expected...	CIS-CAT Collected...
the *Account Lockout Threshold* to be greater than **0**	0

References:

- **CCE-IDv5:** CCE-33728-7 -- More

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More
- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

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

Pass

Description:

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

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

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

Rationale:

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

Remediation:

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

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

Impact:

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

Assessment:

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

References:

- **CCE-IDv5:** CCE-35408-4 -- More

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More
- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

2 Local Policies

This section contains recommendations for local policies.

2.1 Audit Policy

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

2.2 User Rights Assignment

This section contains recommendations for user rights assignments.

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

Pass

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.

Remediation:

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

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

Impact:

None - this is the default behavior.

Assessment:

Ensure 'setrustedcredmanaccessnameright' is set to 'No One' -- More

References:

- **CCE-IDv5:** CCE-35457-1 -- More

CIS Controls V6.1:

- **Control 5: Controlled Use of Administrative Privileges:** -- More

Back to Summary

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

Fail

Description:

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

The recommended state for this setting is: `Administrators, Remote Desktop Users`.

Rationale:

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

Remediation:

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

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

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.

Assessment:

Ensure 'senetworklogonright' is set to 'Administrators, Remote Desktop Users' -- Less

Check:	All Must Pass	
User Right:	SE_NETWORK_LOGON_NAME	
CIS-CAT Expected...		CIS-CAT Collected...
the *Trustee SID* matches the regular expression **S-1-5-32-(544|555)**		S-1-5-32-551
User Right:	SE_NETWORK_LOGON_NAME	
CIS-CAT Expected...		CIS-CAT Collected...
the *Trustee SID* matches the regular expression **S-1-5-32-(544|555)**		S-1-5-32-545
User Right:	SE_NETWORK_LOGON_NAME	
CIS-CAT Expected...		CIS-CAT Collected...

References:

- **CCE-IDv5:** CCE-32928-4 -- More

CIS Controls V6.1:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

Back to Summary

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

Pass

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.

Remediation:

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

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

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.

Assessment:

Ensure 'setcbprivilege' is set to 'No one' -- More

References:

- **CCE-IDv5:** CCE-35403-5 -- More

CIS Controls V6.1:

- **Control 5: Controlled Use of Administrative Privileges:** -- More

Back to Summary

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

Pass

Description:

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

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

Rationale:

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

Remediation:

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

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

Impact:

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

Assessment:

Ensure 'seincreasequotaprivilege' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE' -- More

References:

- **CCE-IDv5:** CCE-35490-2 -- More

CIS Controls V6.1:

- **Control 5: Controlled Use of Administrative Privileges:** -- More

Back to Summary

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

Fail

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 `Guest` account is assigned this user right by default. Although this account is disabled by default, it's recommended that you enable 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.

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

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.

Remediation:

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

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

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.

Assessment:

Ensure 'seinteractivelogonright' is set to 'Administrators, Users' -- Less

Check:	All Must Pass	
User Right:	SE_INTERACTIVE_LOGON_NAME	
CIS-CAT Expected...		CIS-CAT Collected...
the *Trustee SID* matches the regular expression **S-1-5-32-(544|545)**		S-1-5-32-551
User Right:	SE_INTERACTIVE_LOGON_NAME	
CIS-CAT Expected...		CIS-CAT Collected...
the *Trustee SID* matches the regular expression **S-1-5-32-(544|545)**		S-1-5-32-545
User Right:	SE_INTERACTIVE_LOGON_NAME	
CIS-CAT Expected...		CIS-CAT Collected...

References:

- **CCE-IDv5:** CCE-35640-2 -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

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

Pass

Description:

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

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

The recommended state for this setting is: `Administrators, Remote Desktop Users`.

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

Note #2: In all versions of Windows prior to Windows 7, **Remote Desktop Services** was known as **Terminal Services**, so you should substitute the older term if comparing against an older OS.

Rationale:

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

Remediation:

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

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

Impact:

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

Assessment:

Ensure 'seremoteinteractivelogonright' is set to 'Administrators, Remote Desktop Users' -- More

References:

- **CCE-IDv5:** CCE-33035-7 -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

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

Fail

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.

Remediation:

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

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

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.

Assessment:

Ensure 'sebackupprivilege' is set to ' S-1-5-32-544' -- Less

Check:	All Must Pass	
User Right:	SE_BACKUP_NAME	
CIS-CAT Expected...		CIS-CAT Collected...
the *Trustee SID* to be set to **S-1-5-32-544**		S-1-5-32-551
User Right:	SE_BACKUP_NAME	
CIS-CAT Expected...		CIS-CAT Collected...
the *Trustee SID* to be set to **S-1-5-32-544**		S-1-5-32-544

References:

- **CCE-IDv5:** CCE-35699-8 -- More

CIS Controls V6.1:

- **Control 5: Controlled Use of Administrative Privileges:** -- More

Back to Summary

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

Pass

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.

Remediation:

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

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

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.

Assessment:

Ensure 'sesystemtimeprivilege' is set to 'Administrators, LOCAL SERVICE' -- More

References:

- **CCE-IDv5:** CCE-33094-4 -- More

CIS Controls V6.1:

- **Control 5: Controlled Use of Administrative Privileges:** -- More

Back to Summary

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

Pass

Description:

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

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

Rationale:

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

Remediation:

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

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

Impact:

None - this is the default behavior.

Assessment:

Ensure 'setimezoneprivilege' is set to 'Administrators, LOCAL SERVICE, Users' -- More

References:

- **CCE-IDv5:** CCE-33431-8 -- More

CIS Controls V6.1:

- **Control 5: Controlled Use of Administrative Privileges:** -- More

Back to Summary

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

Pass

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.

Remediation:

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

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

Impact:

None - this is the default behavior.

Assessment:

Ensure 'secreatepagefileprivilege' is set to 'Administrators' -- More

References:

- **CCE-IDv5:** CCE-33051-4 -- More

CIS Controls V6.1:

- **Control 5: Controlled Use of Administrative Privileges:** -- More

Back to Summary

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

Pass

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.

Remediation:

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

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

Impact:

None - this is the default behavior.

Assessment:

Ensure 'secreatetokenprivilege' is set to 'No One' -- More

References:

- **CCE-IDv5:** CCE-33779-0 -- More

CIS Controls V6.1:

- **Control 5: Controlled Use of Administrative Privileges:** -- More

Back to Summary

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

Pass

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.

Remediation:

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

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

Impact:

None - this is the default behavior.

Assessment:

Ensure 'secreateglobalprivilege' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' -- More

References:

- **CCE-IDv5:** CCE-33095-1 -- More

CIS Controls V6.1:

- **Control 5: Controlled Use of Administrative Privileges:** -- More

Back to Summary

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

Pass

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.

Remediation:

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

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

Impact:

None - this is the default behavior.

Assessment:

Ensure 'secreatepermanentprivilege' is set to 'No One' -- More

References:

- **CCE-IDv5:** CCE-33780-8 -- More

CIS Controls V6.1:

- **Control 5: Controlled Use of Administrative Privileges:** -- More

Back to Summary

2.2.14 (L1) Configure 'Create symbolic links'

Pass

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.

Remediation:

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

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

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.

Assessment:

Ensure 'secreatesymboliclinkprivilege' is set to 'Administrators, NT VIRTUAL MACHINE\Virtual Machines' -- More

References:

- **CCE-IDv5:** CCE-33053-0 -- More

CIS Controls V6.1:

- **Control 5: Controlled Use of Administrative Privileges:** -- More

Back to Summary

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

Pass

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.

Remediation:

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

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

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.

Assessment:

Ensure 'sedebugprivilege' is set to 'Administrators' -- More

References:

- **CCE-IDv5:** CCE-33157-9 -- More

CIS Controls V6.1:

- **Control 5: Controlled Use of Administrative Privileges:** -- More

Back to Summary

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

Fail

Description:

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

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

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

Note: The security identifier `Local account` is not available in Windows 7 and Windows 8.0 unless MSKB 2871997 has been installed.

Rationale:

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

Remediation:

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

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

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.

Assessment:

All of the following tests or sub-groups must pass:

Ensure 'Deny access to this computer from the network' to include 'Guests, Local account' -- Less

Check:	At Least One Must Pass
User Right:	SE_DENY_NETWORK_LOGON_NAME

CIS-CAT Expected (At least one of)...	CIS-CAT Collected...
the *Trustee SID* to be set to **S-1-5-32-546**	S-1-5-21-358118824-3846515562-1363085019-501

Ensure 'Deny access to this computer from the network' to include 'Guests, Local account' -- Less

Check:	At Least One Must Pass
User Right:	SE_DENY_NETWORK_LOGON_NAME

CIS-CAT Expected (At least one of)...	CIS-CAT Collected...
the *Trustee SID* to be set to **S-1-5-113**	S-1-5-21-358118824-3846515562-1363085019-501

References:

- **CCE-IDv5:** CCE-34173-5 -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

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

Fail

Description:

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

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

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

Rationale:

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

Remediation:

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

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

Impact:

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

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

Assessment:

Ensure 'sedenybatchLogonright' to include 'Guests' -- Less

```
CIS-CAT expected to collect at least 1 matching User Rights item, and found 0 items.
User Right: SE_DENY_BATCH_LOGON_NAME                                                  does not exist
```

References:

- **CCE-IDv5:** CCE-35461-3 -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

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

Fail

Description:

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

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

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

Rationale:

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

Remediation:

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

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

Impact:

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

Assessment:

Ensure 'SE_DENY_SERVICE_LOGON_NAME' to include 'Guests' -- Less

```
CIS-CAT expected to collect at least 1 matching User Rights item, and found 0 items.
User Right: SE_DENY_SERVICE_LOGON_NAME                                                does not exist
```

References:

- **CCE-IDv5:** CCE-35404-3 -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

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

Fail

Description:

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

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

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

Rationale:

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

Remediation:

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

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

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.

Assessment:

Ensure 'sedenyinteractivelogonright' to include 'Guests' -- Less

Check:	At Least One Must Pass	
User Right:	SE_DENY_INTERACTIVE_LOGON_NAME	
CIS-CAT Expected (At least one of)...		CIS-CAT Collected...
the *Trustee SID* to be set to **S-1-5-32-546**		S-1-5-21-358118824-3846515562-1363085019-501

References:

- **CCE-IDv5:** CCE-35293-0 -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

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

Fail

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.

Remediation:

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

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

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.

Assessment:

All of the following tests or sub-groups must pass:

Ensure 'sedenyremoteInteractivelogonright' to include 'Guests, Local account' -- Less

CIS-CAT expected to collect at least 1 matching User Rights item, and found 0 items.

User Right: SE_DENY_REMOTE_INTERACTIVE_LOGON_NAME does not exist

Ensure 'sedenyremoteInteractivelogonright' to include 'Guests, Local account' -- Less

CIS-CAT expected to collect at least 1 matching User Rights item, and found 0 items.

User Right: SE_DENY_REMOTE_INTERACTIVE_LOGON_NAME does not exist

References:

- **CCE-IDv5:** CCE-33787-3 -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

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

Pass

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.

Remediation:

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

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

Impact:

None - this is the default behavior.

Assessment:

Ensure 'seenabledelegationprivilege' is set to 'No One' -- More

References:

- **CCE-IDv5:** CCE-33778-2 -- More

CIS Controls V6.1:

- **Control 5: Controlled Use of Administrative Privileges:** -- More

Back to Summary

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

Pass

Description:

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

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

Rationale:

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

Remediation:

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

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

Impact:

If you remove the **Force shutdown from a remote system** user right from the Server Operator 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.

Assessment:

Ensure 'seremoteshutdownprivilege' is set to 'Administrators' -- More

References:

- **CCE-IDv5:** CCE-33715-4 -- More

CIS Controls V6.1:

- **Control 5: Controlled Use of Administrative Privileges:** -- More

Back to Summary

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

Pass

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.

Remediation:

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

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

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.

Assessment:

Ensure 'seauditprivilege' is set to 'LOCAL SERVICE, NETWORK SERVICE' -- More

References:

- **CCE-IDv5:** CCE-35363-1 -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

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

Fail

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.

Remediation:

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

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

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`.

Assessment:

Ensure 'seimpersonateprivilege' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' -- Less

Check:	All Must Pass	
User Right:	SE_IMPERSONATE_NAME	
CIS-CAT Expected...		CIS-CAT Collected...
the *Trustee SID* matches the regular expression **S-1-5-(32-544|19|20|6)**		S-1-5-6
User Right:	SE_IMPERSONATE_NAME	
CIS-CAT Expected...		CIS-CAT Collected...
the *Trustee SID* matches the regular expression **S-1-5-(32-544|19|20|6)**		S-1-5-32-568
User Right:	SE_IMPERSONATE_NAME	

CIS-CAT Expected	CIS-CAT Collected

References:

- **CCE-IDv5:** CCE-34021-6 -- More

CIS Controls V6.1:

- **Control 5: Controlled Use of Administrative Privileges:** -- More

Back to Summary

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

Pass

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.

Remediation:

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

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

Impact:

None - this is the default behavior.

Assessment:

Ensure 'seincreasebasepriorityprivilege' is set to 'Administrators, Window Manager\Window Manager Group' -- More

References:

- **CCE-IDv5:** CCE-35178-3 -- More

CIS Controls V6.1:

- **Control 5: Controlled Use of Administrative Privileges:** -- More

Back to Summary

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

Pass

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.

Remediation:

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

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

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.

Assessment:

Ensure 'seloaddriverprivilege' is set to 'Administrators' -- More

References:

- **CCE-IDv5:** CCE-34903-5 -- More

CIS Controls V6.1:

- **Control 5: Controlled Use of Administrative Privileges:** -- More

Back to Summary

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

Pass

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.

Remediation:

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

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

Impact:

None - this is the default behavior.

Assessment:

Ensure 'selockmemoryprivilege' is set to 'No One' -- More

References:

- **CCE-IDv5:** CCE-33807-9 -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

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

Pass

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.

Remediation:

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

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

Impact:

None - this is the default behavior.

Assessment:

Ensure 'sesecurityprivilege' is set to 'Administrators' -- More

References:

- **CCE-IDv5:** CCE-35275-7 -- More

CIS Controls V6.1:

- **Control 5: Controlled Use of Administrative Privileges:** -- More

Back to Summary

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

Pass

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.

Remediation:

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

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

Impact:

None - this is the default behavior.

Assessment:

Ensure 'serelabelprivilege' is set to 'No One' -- More

References:

- **CCE-IDv5:** CCE-34913-4 -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

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

Pass

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.

Remediation:

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

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

Impact:

None - this is the default behavior.

Assessment:

Ensure 'sesystemenvironmentprivilege' is set to 'Administrators' -- More

References:

- **CCE-IDv5:** CCE-35183-3 -- More

CIS Controls V6.1:

- **Control 5: Controlled Use of Administrative Privileges:** -- More

Back to Summary

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

Pass

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`.

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.

Remediation:

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

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

Impact:

None - this is the default behavior.

Assessment:

Ensure 'semanagevolumeprivilege' is set to 'Administrators' -- More

References:

- **CCE-IDv5:** CCE-35369-8 -- More

CIS Controls V6.1:

- **Control 5: Controlled Use of Administrative Privileges:** -- More

Back to Summary

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

Pass

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.

Remediation:

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

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

Impact:

If you remove the **Profile single process** user right from the `Power Users` 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.

Assessment:

Ensure 'seprofilesingleprocessprivilege' is set to 'Administrators' -- More

References:

- **CCE-IDv5:** CCE-35000-9 -- More

CIS Controls V6.1:

- **Control 5: Controlled Use of Administrative Privileges:** -- More

Back to Summary

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

Pass

Description:

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

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

Rationale:

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

Remediation:

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

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

Impact:

None - this is the default behavior.

Assessment:

Ensure 'sesystemprofileprivilege' is set to 'Administrators, NT SERVICE\WdiServiceHost' -- More

References:

- **CCE-IDv5:** CCE-35001-7 -- More

CIS Controls V6.1:

- **Control 5: Controlled Use of Administrative Privileges:** -- More

Back to Summary

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

Pass

Description:

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

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

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

Rationale:

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

Remediation:

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

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

Impact:

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

Assessment:

Ensure 'seassignprimarytokenprivilege' is set to 'LOCAL SERVICE, NETWORK SERVICE' -- More

References:

- **CCE-IDv5:** CCE-35003-3 -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

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

Fail

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.

Remediation:

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

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

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.

Assessment:

Ensure 'serestoreprivilege' is set to 'Administrators' -- Less

Check:	All Must Pass	
User Right:	SE_RESTORE_NAME	
CIS-CAT Expected...		CIS-CAT Collected...
the *Trustee SID* to be set to **S-1-5-32-544**		S-1-5-32-551
User Right:	SE_RESTORE_NAME	
CIS-CAT Expected...		CIS-CAT Collected...
the *Trustee SID* to be set to **S-1-5-32-544**		S-1-5-32-544

References:

- **CCE-IDv5:** CCE-35067-8 -- More

CIS Controls V6.1:

- **Control 5: Controlled Use of Administrative Privileges:** -- More

Back to Summary

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

Fail

Description:

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

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

Rationale:

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

Remediation:

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

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

Impact:

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

Assessment:

Ensure 'seshutdownprivilege' is set to 'Users, Administrators' -- Less

Check:	All Must Pass	
User Right:	SE_SHUTDOWN_NAME	
CIS-CAT Expected...		CIS-CAT Collected...
the *Trustee SID* matches the regular expression **S-1-5-32-(544|545)**		S-1-5-32-551
User Right:	SE_SHUTDOWN_NAME	
CIS-CAT Expected...		CIS-CAT Collected...
the *Trustee SID* matches the regular expression **S-1-5-32-(544|545)**		S-1-5-32-545
User Right:	SE_SHUTDOWN_NAME	
CIS-CAT Expected...		CIS-CAT Collected...

References:

- **CCE-IDv5:** CCE-35004-1 -- More

CIS Controls V6.1:

- **Control 5: Controlled Use of Administrative Privileges:** -- More

Back to Summary

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

Pass

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.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights
Assignment\Take ownership of files or other objects
```

Impact:

None - this is the default behavior.

Assessment:

Ensure 'setakeownershipprivilege' is set to 'Administrators' -- More

References:

- **CCE-IDv5:** CCE-35009-0 -- More

CIS Controls V6.1:

- **Control 5: Controlled Use of Administrative Privileges:** -- More

Back to Summary

2.3 Security Options

This section contains recommendations for security options.

2.3.1 Accounts

This section contains recommendations related to default accounts.

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

Pass

Description:

This policy setting enables or disables the Administrator account during normal operation. When a computer is booted into safe mode, the Administrator account is always enabled, regardless of how this setting is configured. Note that this setting will have no impact when applied to the Domain Controllers organizational unit via group policy because Domain Controllers have no local account database. It can be configured at the domain level via group policy, similar to account lockout and password policy settings.

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

Rationale:

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

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security
Options\Accounts: Administrator account status
```

Impact:

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

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

Assessment:

Ensure '^S\-1\-5\-21\-\d+\-\d+\-\d+\-500$' is 'Equals' to '0' -- More

References:

- **CCE-IDv5:** CCE-33511-7 -- More

CIS Controls V6.1:

- **Control 5: Controlled Use of Administrative Privileges:** -- More

Back to Summary

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

Fail

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.

Remediation:

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

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

Impact:

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

Assessment:

Ensure 'NoConnectedUser' is 'Windows: Registry Value' to '3' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System:NoConnectedUser          does not exist
```

References:

- **CCE-IDv5:** CCE-35487-8 -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

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

Pass

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.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security
Options\Accounts: Guest account status
```

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.

Assessment:

Ensure '^S\-1\-5\-21\-\d+\-\d+\-\d+\-501$' is 'Equals' to '0' -- More

References:

- **CCE-IDv5:** CCE-33949-9 -- More

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

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

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security
Options\Accounts: Limit local account use of blank passwords to console logon only
```

Impact:

None - this is the default behavior.

Assessment:

Ensure 'LimitBlankPasswordUse' is 'Windows: Registry Value' to '1' -- Less

Check:	All Must Pass
Registry Key:	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa
Registry Value:	LimitBlankPasswordUse

CIS-CAT Expected...	CIS-CAT Collected...
the registry key's *type* to be set to **reg_dword**	reg_dword
the registry key's *value* to be set to **1**	0

References:

- **CCE-IDv5:** CCE-32929-2 -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

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

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security
Options\Accounts: Rename administrator account
```

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.)

Assessment:

Ensure '^S\-1\-5\-21\-\d+\-\d+\-\d+\-500$' is 'case insensitive not equal' 'Administrator' -- Less

Check:	All Must Pass
Trustee SID:	S-1-5-21-358118824-3846515562-1363085019-500
CIS-CAT Expected...	CIS-CAT Collected...
the *Trustee Name* to not be set to **Administrator**	Administrator

References:

- **CCE-IDv5:** CCE-33034-0 -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

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

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security
Options\Accounts: Rename guest account
```

Impact:

There should be little impact, because the Guest account is disabled by default.

Assessment:

Ensure 'Guest' is 'Null Test' to '' -- Less

Check:	All Must Pass
Trustee SID:	S-1-5-21-358118824-3846515562-1363085019-501
CIS-CAT Expected...	CIS-CAT Collected...
the *Trustee Name* to not be set to **Guest**	Guest

References:

- **CCE-IDv5:** CCE-35488-6 -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

2.3.2 Audit

This section contains recommendations related to auditing controls.

2.3.2.1 (L1) Ensure 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' is set to 'Enabled'

Fail

Description:

This policy setting allows administrators to enable the more precise auditing capabilities present in Windows Vista.

The Audit Policy settings available in Windows Server 2003 Active Directory do not yet contain settings for managing the new auditing subcategories. To properly apply the auditing policies prescribed in this baseline, the Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings setting needs to be configured to Enabled.

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

Important: Be very cautious about audit settings that can generate a large volume of traffic. For example, if you enable either success or failure auditing for all of the Privilege Use subcategories, the high volume of audit events generated can make it difficult to find other types of entries in the Security log. Such a configuration could also have a significant impact on system performance.

Rationale:

Prior to the introduction of auditing subcategories in Windows Vista, it was difficult to track events at a per-system or per-user level. The larger event categories created too many events and the key information that needed to be audited was difficult to find.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security
Options\Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy
category settings
```

Impact:

None - this is the default behavior.

Assessment:

Ensure 'SCENoApplyLegacyAuditPolicy' is 'Windows: Registry Value' to '1' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa:SCENoApplyLegacyAuditPolicy        does not exist
```

References:

- **CCE-IDv5:** CCE-35533-9 -- More

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More
- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More

CIS Controls V6.1:

- **Control 6: Maintenance, Monitoring, and Analysis of Audit Logs:** -- More

Back to Summary

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

Pass

Description:

This policy setting determines whether the system shuts down if it is unable to log Security events. It is a requirement for Trusted Computer System Evaluation Criteria (TCSEC)-C2 and Common Criteria certification to prevent auditable events from occurring if the audit system is unable to log them. Microsoft has chosen to meet this requirement by halting the system and displaying a stop message if the auditing system experiences a failure. When this policy setting is enabled, the system will be shut down if a security audit cannot be logged for any reason.

If the Audit: Shut down system immediately if unable to log security audits setting is enabled, unplanned system failures can occur. The administrative burden can be significant, especially if you also configure the Retention method for the Security log to Do not overwrite events (clear log manually). This configuration causes a repudiation threat (a backup operator could deny that they backed up or restored data) to become a denial of service (DoS) vulnerability, because a server could be forced to shut down if it is overwhelmed with logon events and other security events that are written to the Security log. Also, because the shutdown is not graceful, it is possible that irreparable damage to the operating system, applications, or data could result. Although the NTFS file system guarantees its integrity when an ungraceful computer shutdown occurs, it cannot guarantee that every data file for every application will still be in a usable form when the computer restarts.

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

Rationale:

If the computer is unable to record events to the Security log, critical evidence or important troubleshooting information may not be available for review after a security incident. Also, an attacker could potentially generate a large volume of Security log events to purposely force a computer shutdown.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security
Options\Audit: Shut down system immediately if unable to log security audits
```

Impact:

None - this is the default behavior.

Assessment:

Ensure 'CrashOnAuditFail' is 'Windows: Registry Value' to '0' -- More

References:

- **CCE-IDv5:** CCE-33046-4 -- More

CIS Controls V6.1:

- **Control 6: Maintenance, Monitoring, and Analysis of Audit Logs:** -- More

Back to Summary

2.3.3 DCOM

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

2.3.4 Devices

This section contains recommendations related to managing devices.

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

Fail

Description:

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

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

Rationale:

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

Remediation:

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

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

Impact:

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

Assessment:

Ensure 'AllocateDASD' is 'Windows: Registry Value' to '2' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon:AllocateDASD          does not exist
```

References:

- **CCE-IDv5:** CCE-34355-8 -- More

CIS Controls V6.1:

- **Control 5: Controlled Use of Administrative Privileges:** -- More

Back to Summary

2.3.5 Domain controller

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

2.3.6 Domain member

This section contains recommendations related to domain membership.

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

Pass

Description:

This policy setting determines whether all secure channel traffic that is initiated by the domain member must be signed or encrypted.

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

Rationale:

When a computer joins a domain, a computer account is created. After it joins the domain, the computer uses the password for that account to create a secure channel with the Domain Controller for its domain every time that it restarts. Requests that are sent on the secure channel are authenticated—and sensitive information such as passwords are encrypted—but the channel is not integrity-checked, and not all information is encrypted.

Digital encryption and signing of the secure channel is a good idea where it is supported. The secure channel protects domain credentials as they are sent to the Domain Controller.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security
Options\Domain member: Digitally encrypt or sign secure channel data (always)
```

Impact:

None - this is the default behavior. However, only Windows NT 4.0 with Service Pack 6a (SP6a) and subsequent versions of the Windows operating system support digital encryption and signing of the secure channel. Windows 98 Second Edition clients do not support it unless they have `Dsclient` installed. Therefore, you cannot enable the Domain member: Digitally encrypt or sign secure channel data (always) setting on Domain Controllers that support Windows 98 clients as members of the domain. Potential impacts can include the following:

- The ability to create or delete trust relationships with clients running versions of Windows earlier than Windows NT 4.0 with SP6a will be disabled.
- Logons from clients running versions of Windows earlier than Windows NT 4.0 with SP6a will be disabled.
- The ability to authenticate other domains' users from a Domain Controller running a version of Windows earlier than Windows NT 4.0 with SP6a in a trusted domain will be disabled.

You can enable this policy setting after you eliminate all Windows 9x clients from the domain and upgrade all Windows NT 4.0 servers and Domain Controllers from trusted/trusting domains to Windows NT 4.0 with SP6a.

Assessment:

Ensure 'RequireSignOrSeal' is 'Windows: Registry Value' to '1' -- More

References:

- **CCE-IDv5:** CCE-34892-0 -- More

CIS Controls V6.1:

- **Control 13: Data Protection:** -- More

Back to Summary

2.3.6.2 (L1) Ensure 'Domain member: Digitally encrypt secure channel data (when

possible)' is set to 'Enabled'

Pass

Description:

This policy setting determines whether a domain member should attempt to negotiate encryption for all secure channel traffic that it initiates.

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

Rationale:

When a computer joins a domain, a computer account is created. After it joins the domain, the computer uses the password for that account to create a secure channel with the Domain Controller for its domain every time that it restarts. Requests that are sent on the secure channel are authenticated—and sensitive information such as passwords are encrypted—but the channel is not integrity-checked, and not all information is encrypted.

Digital encryption and signing of the secure channel is a good idea where it is supported. The secure channel protects domain credentials as they are sent to the Domain Controller.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security
Options\Domain member: Digitally encrypt secure channel data (when possible)
```

Impact:

None - this is the default behavior. However, only Windows NT 4.0 Service Pack 6a (SP6a) and subsequent versions of the Windows operating system support digital encryption and signing of the secure channel. Windows 98 Second Edition clients do not support it unless they have `Dsclient` installed.

Assessment:

Ensure 'SealSecureChannel' is 'Windows: Registry Value' to '1' -- More

References:

- **CCE-IDv5:** CCE-35273-2 -- More

CIS Controls V6.1:

- **Control 13: Data Protection:** -- More

Back to Summary

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

Pass

Description:

This policy setting determines whether a domain member should attempt to negotiate whether all secure channel traffic that it initiates must be digitally signed. Digital signatures protect the traffic from being modified by anyone who captures the data as it traverses the network.

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

Rationale:

When a computer joins a domain, a computer account is created. After it joins the domain, the computer uses the password for that account to create a secure channel with the Domain Controller for its domain every time that it restarts. Requests that are sent on the secure channel are authenticated—and sensitive information such as passwords are encrypted—but the channel is not integrity-checked, and not all information is encrypted.

Digital encryption and signing of the secure channel is a good idea where it is supported. The secure channel protects domain credentials as they are sent to the Domain Controller.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security
Options\Domain member: Digitally sign secure channel data (when possible)
```

Impact:

None - this is the default behavior. However, only Windows NT 4.0 with Service Pack 6a (SP6a) and subsequent versions of the Windows operating system support digital encryption and signing of the secure channel. Windows 98 Second Edition clients do not support it unless they have `Dsclient` installed.

Assessment:

Ensure 'SignSecureChannel' is 'Windows: Registry Value' to '1' -- More

References:

- **CCE-IDv5:** CCE-34893-8 -- More

CIS Controls V6.1:

- **Control 13: Data Protection:** -- More

Back to Summary

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

Pass

Description:

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

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

Rationale:

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

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security
Options\Domain member: Disable machine account password changes
```

Impact:

None - this is the default behavior.

Assessment:

Ensure 'DisablePasswordChange' is 'Windows: Registry Value' to '0' -- More

References:

- **CCE-IDv5:** CCE-34986-0 -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

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

Pass

Description:

This policy setting determines the maximum allowable age for a computer account password. By default, domain members automatically change their domain passwords every 30 days. If you increase this interval significantly so that the computers no longer change their passwords, an attacker would have more time to undertake a brute force attack against one of the computer accounts.

The recommended state for this setting is: `30 or fewer days, but not 0`.

Note: A value of `0` does not conform to the benchmark as it disables maximum password age.

Rationale:

In Active Directory-based domains, each computer has an account and password just like every user. By default, the domain members automatically change their domain password every 30 days. If you increase this interval significantly, or set it to 0 so that the computers no longer change their passwords, an attacker will have more time to undertake a brute force attack to guess the password of one or more computer accounts.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `30 or fewer days, but not 0`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security
Options\Domain member: Maximum machine account password age
```

Impact:

None - this is the default behavior.

Assessment:

All of the following tests or sub-groups must pass:

Ensure 'MaximumPasswordAge' is 'Windows: Registry Value' to '30' -- More

Ensure 'MaximumPasswordAge' is 'Windows: Registry Value' to '0' -- More

References:

- **CCE-IDv5:** CCE-34894-6 -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

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

Pass

Description:

When this policy setting is enabled, a secure channel can only be established with Domain Controllers that are capable of encrypting secure channel data with a strong (128-bit) session key.

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

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

Rationale:

Session keys that are used to establish secure channel communications between Domain Controllers and member computers are much stronger in Windows 2000 than they were in previous Microsoft operating systems. Whenever possible, you should take advantage of these stronger session keys to help protect secure channel communications from attacks that attempt to hijack network sessions and eavesdropping. (Eavesdropping is a form of hacking in which network data is read or altered in transit. The data can be modified to hide or change the sender, or be redirected.)

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security
Options\Domain member: Require strong (Windows 2000 or later) session key
```

Impact:

None - this is the default behavior. However, computers will not be able to join Windows NT 4.0 domains, and trusts between Active Directory domains and Windows NT-style domains may not work properly.

Assessment:

Ensure 'RequireStrongKey' is 'Windows: Registry Value' to '1' -- More

References:

- **CCE-IDv5:** CCE-35177-5 -- More

CIS Controls V6.1:

- **Control 13: Data Protection:** -- More

Back to Summary

2.3.7 Interactive logon

This section contains recommendations related to interactive logons.

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

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security
Options\Interactive logon: Do not require CTRL+ALT+DEL
```

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.

Assessment:

Ensure 'DisableCAD' is 'Windows: Registry Value' to '0' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System:DisableCAD          does not exist
```

References:

- **CCE-IDv5:** CCE-35099-1 -- More

CIS Controls V6.1:

- **Control 8: Malware Defenses:** -- More

Back to Summary

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

Fail

Description:

This policy setting determines whether the account name of the last user to log on to the client computers in your organization will be displayed in each computer's respective Windows logon screen. Enable this policy setting to prevent intruders from collecting account names visually from the screens of desktop or laptop computers in your organization.

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

Rationale:

An attacker with access to the console (for example, someone with physical access or someone who is able to connect to the server through Remote Desktop Services) could view the name of the last user who logged on to the server. The attacker could then try to guess the password, use a dictionary, or use a brute-force attack to try and log on.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security
Options\Interactive logon: Don't display last signed-in
```

Note: In older versions of Microsoft Windows, this setting was named *Interactive logon: Do not display last user name*, but it was renamed starting with Windows 10 Release 1703.

Impact:

The name of the last user to successfully log on will not be displayed in the Windows logon screen.

Assessment:

Ensure 'DontDisplayLastUserName' is 'Windows: Registry Value' to '1' -- Less

Check:	All Must Pass
Registry Key:	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System
Registry Value:	DontDisplayLastUserName

CIS-CAT Expected...	CIS-CAT Collected...
the registry key's *type* to be set to **reg_dword**	reg_dword
the registry key's *value* to be set to **1**	0

References:

- **CCE-IDv5:** CCE-34898-7 -- More

CIS Controls V6.1:

- **Control 13: Data Protection:** -- More

Back to Summary

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

Fail

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.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `900 or fewer seconds, but not 0`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security
Options\Interactive logon: Machine inactivity limit
```

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.

Assessment:

All of the following tests or sub-groups must pass:

Ensure 'InactivityTimeoutSecs' is 'Windows: Registry Value' to '0' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System:InactivityTimeoutSecs does not exist

Ensure 'InactivityTimeoutSecs' is 'Windows: Registry Value' to '900' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System:InactivityTimeoutSecs does not exist

References:

- **CCE-IDv5:** CCE-34900-1 -- More

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

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

Fail

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.

Remediation:

To establish the recommended configuration via GP, configure the following UI path to a value that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security
Options\Interactive logon: Message text for users attempting to log on
```

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.

Assessment:

Ensure 'LegalNoticeText' is 'Windows: Registry Value' to '.+' -- Less

Check:	All Must Pass
Registry Key:	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System
Registry Value:	LegalNoticeText

CIS-CAT Expected...	CIS-CAT Collected...
the registry key's *type* to be set to **reg_sz**	reg_sz
the registry key's *value* matches the regular expression **.+**	No Value

References:

- **CCE-IDv5:** CCE-35064-5 -- More

Back to Summary

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

Fail

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.

Remediation:

To establish the recommended configuration via GP, configure the following UI path to a value that is consistent with the security and operational requirements of your organization:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security
Options\Interactive logon: Message title for users attempting to log on
```

Impact:

Users will have to acknowledge a dialog box with the configured title before they can log on to the computer.

Assessment:

Ensure 'LegalNoticeCaption' is pattern match to '[a-zA-Z]' -- Less

Check:	All Must Pass
Registry Key:	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System
Registry Value:	LegalNoticeCaption

CIS-CAT Expected...	CIS-CAT Collected...
the registry key's *type* to be set to **reg_sz**	reg_sz
the registry key's *value* matches the regular expression **.+**	No Value

References:

- **CCE-IDv5:** CCE-35179-1 -- More

Back to Summary

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

Pass

Description:

This policy setting determines how far in advance users are warned that their password will expire. It is recommended that you configure this policy setting to at least 5 days but no more than 14 days to sufficiently warn users when their passwords will expire.

The recommended state for this setting is: `between 5 and 14 days`.

Rationale:

Users will need to be warned that their passwords are going to expire, or they may inadvertently be locked out of the computer when their passwords expire. This condition could lead to confusion for users who access the network locally, or make it impossible for users to access your organization's network through dial-up or virtual private network (VPN) connections.

Remediation:

To establish the recommended configuration via GP, set the following UI path to a value `between 5 and 14 days`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security
Options\Interactive logon: Prompt user to change password before expiration
```

Impact:

Users will see a dialog box prompt to change their password each time that they log on to the domain when their password is configured to expire between 5 and 14 days.

Assessment:

All of the following tests or sub-groups must pass:

Ensure 'PasswordExpiryWarning' is 'Windows: Registry Value' to '14' -- More
Ensure 'passwordexpirywarning' is 'Windows: Registry Value' to '5' -- More

References:

- **CCE-IDv5:** CCE-35274-0 -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

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

Fail

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.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Lock Workstation` (or, if applicable for your environment, `Force Logoff` or `Disconnect if a Remote Desktop Services session`):

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security
Options\Interactive logon: Smart card removal behavior
```

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.

Assessment:

Ensure 'ScRemoveOption' is 'Windows: Registry Value' to '^(1|2|3)$' -- Less

Check:	All Must Pass
Registry Key:	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
Registry Value:	ScRemoveOption

CIS-CAT Expected...	CIS-CAT Collected...
the registry key's *type* to be set to **reg_sz**	reg_sz
the registry key's *value* matches the regular expression **^(1|2|3)$**	0

References:

- **CCE-IDv5:** CCE-34988-6 -- More

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

2.3.8 Microsoft network client

This section contains recommendations related to configuring the Microsoft network client.

2.3.8.1 (L1) Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled'

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security
Options\Microsoft network client: Digitally sign communications (always)
```

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.

Assessment:

Ensure 'RequireSecuritySignature' is 'Windows: Registry Value' to '1' -- Less

Check:	All Must Pass
Registry Key:	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters
Registry Value:	RequireSecuritySignature

CIS-CAT Expected...	CIS-CAT Collected...
the registry key's *type* to be set to **reg_dword**	reg_dword
the registry key's *value* to be set to **1**	0

References:

- **CCE-IDv5:** CCE-35222-9 -- More

CIS Controls V6.1:

- **Control 13: Data Protection:** -- More

Back to Summary

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

Pass

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.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security
Options\Microsoft network client: Digitally sign communications (if server agrees)
```

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.

Assessment:

Ensure 'EnableSecuritySignature' is 'Windows: Registry Value' to '1' -- More

References:

- **CCE-IDv5:** CCE-34908-4 -- More

CIS Controls V6.1:

- **Control 13: Data Protection:** -- More

Back to Summary

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

Pass

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.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security
Options\Microsoft network client: Send unencrypted password to third-party SMB servers
```

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.

Assessment:

Ensure 'EnablePlainTextPassword' is 'Windows: Registry Value' to '0' -- More

References:

- **CCE-IDv5:** CCE-33717-0 -- More

CIS Controls V6.1:

- **Control 13: Data Protection:** -- More

Back to Summary

2.3.9 Microsoft network server

This section contains recommendations related to configuring the Microsoft network server.

2.3.9.1 (L1) Ensure 'Microsoft network server: Amount of idle time required before suspending session' is set to '15 or fewer minute(s)'

Pass

Description:

This policy setting allows you to specify the amount of continuous idle time that must pass in an SMB session before the session is suspended because of inactivity. Administrators can use this policy setting to control when a computer suspends an inactive SMB session. If client activity resumes, the session is automatically reestablished.

The maximum value is 99999, which is over 69 days; in effect, this value disables the setting.

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

Rationale:

Each SMB session consumes server resources, and numerous null sessions will slow the server or possibly cause it to fail. An attacker could repeatedly establish SMB sessions until the server's SMB services become slow or unresponsive.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security
Options\Microsoft network server: Amount of idle time required before suspending session
```

Impact:

There will be little impact because SMB sessions will be re-established automatically if the client resumes activity.

Assessment:

Ensure 'AutoDisconnect' is 'Windows: Registry Value' to less than or equal to '15' -- More

References:

- **CCE-IDv5:** CCE-34909-2 -- More

CIS Controls V6.1:

- **Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers:** -- More

Back to Summary

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

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security
Options\Microsoft network server: Digitally sign communications (always)
```

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.

Assessment:

Ensure 'RequireSecuritySignature' is 'Windows: Registry Value' to '1' -- Less

Check:	All Must Pass
Registry Key:	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters
Registry Value:	RequireSecuritySignature

CIS-CAT Expected...	CIS-CAT Collected...
the registry key's *type* to be set to **reg_dword**	reg_dword
the registry key's *value* to be set to **1**	0

References:

- **CCE-IDv5:** CCE-35065-2 -- More

CIS Controls V6.1:

- **Control 13: Data Protection:** -- More

Back to Summary

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

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security
Options\Microsoft network server: Digitally sign communications (if client agrees)
```

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.

Assessment:

Ensure 'EnableSecuritySignature' is 'Windows: Registry Value' to '1' -- Less

Check:	All Must Pass
Registry Key:	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters
Registry Value:	EnableSecuritySignature

CIS-CAT Expected...	CIS-CAT Collected...
the registry key's *type* to be set to **reg_dword**	reg_dword
the registry key's *value* to be set to **1**	0

References:

- **CCE-IDv5:** CCE-35182-5 -- More

CIS Controls V6.1:

- **Control 13: Data Protection:** -- More

Back to Summary

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

Pass

Description:

This security setting determines whether to disconnect users who are connected to the local computer outside their user account's valid logon hours. This setting affects the Server Message Block (SMB) component. If you enable this policy setting you should also enable *Network security: Force logoff when logon hours expire* (Rule 2.3.11.6).

If your organization configures logon hours for users, this policy setting is necessary to ensure they are effective.

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

Rationale:

If your organization configures logon hours for users, then it makes sense to enable this policy setting. Otherwise, users who should not have access to network resources outside of their logon hours may actually be able to continue to use those resources with sessions that were established during allowed hours.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security
Options\Microsoft network server: Disconnect clients when logon hours expire
```

Impact:

None - this is the default behavior. If logon hours are not used in your organization, this policy setting will have no impact. If logon hours are used, existing user sessions will be forcibly terminated when their logon hours expire.

Assessment:

Ensure 'enableforcedlogoff' is 'Windows: Registry Value' to '1' -- More

References:

- **CCE-IDv5:** CCE-34911-8 -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

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

Fail

Description:

This policy setting controls the level of validation a computer with shared folders or printers (the server) performs on the service principal name (SPN) that is provided by the client computer when it establishes a session using the server message block (SMB) protocol.

The server message block (SMB) protocol provides the basis for file and print sharing and other networking operations, such as remote Windows administration. The SMB protocol supports validating the SMB server service principal name (SPN) within the authentication blob provided by a SMB client to prevent a class of attacks against SMB servers referred to as SMB relay attacks. This setting will affect both SMB1 and SMB2.

The recommended state for this setting is: `Accept if provided by client`. Configuring this setting to `Required from client` also conforms to the benchmark.

Rationale:

The identity of a computer can be spoofed to gain unauthorized access to network resources.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Accept if provided by client` (configuring to `Required from client` also conforms to the benchmark):

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security
Options\Microsoft network server: Server SPN target name validation level
```

Impact:

All Windows operating systems support both a client-side SMB component and a server-side SMB component. This setting affects the server SMB behavior, and its implementation should be carefully evaluated and tested to prevent disruptions to file and print serving capabilities.

If configured to `Accept if provided by client`, the SMB server will accept and validate the SPN provided by the SMB client and allow a session to be established if it matches the SMB server's list of SPN's for itself. If the SPN does NOT match, the session request for that SMB client will be denied.

If configured to `Required from client`, the SMB client MUST send a SPN name in session setup, and the SPN name provided MUST match the SMB server that is being requested to establish a connection. If no SPN is provided by client, or the SPN provided does not match, the session is denied.

Assessment:

Ensure 'SMBServerNameHardeningLevel' is 'Windows: Registry Value' to '1' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters:SMBServerNameHardeningLevel          does not exist
```

References:

- **CCE-IDv5:** CCE-35299-7 -- More

CIS Controls V6.1:

- **Control 14: Controlled Access Based on the Need to Know:** -- More

Back to Summary

2.3.10 Network access

This section contains recommendations related to network access.

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

Unknown

Description:

This policy setting determines whether an anonymous user can request security identifier (SID) attributes for another user, or use a SID to obtain its corresponding user name.

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

Rationale:

If this policy setting is enabled, a user with local access could use the well-known Administrator's SID to learn the real name of the built-in Administrator account, even if it has been renamed. That person could then use the account name to initiate a password guessing attack.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security
Options\Network access: Allow anonymous SID/Name translation
```

Impact:

None - this is the default behavior.

Assessment:

Ensure 'LSAAnonymousNameLookup' is 'Equals' to 'False' -- More

References:

- **CCE-IDv5:** CCE-34914-2 -- More

CIS Controls V6.1:

- **Control 13: Data Protection:** -- More

Back to Summary

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

Pass

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.)

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security
Options\Network access: Do not allow anonymous enumeration of SAM accounts
```

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.

Assessment:

Ensure 'RestrictAnonymousSAM' is 'Windows: Registry Value' to '1' -- More

References:

- **CCE-IDv5:** CCE-34631-2 -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

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

Fail

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.)

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security
Options\Network access: Do not allow anonymous enumeration of SAM accounts and shares
```

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`.

Assessment:

Ensure 'RestrictAnonymous' is 'Windows: Registry Value' to '1' -- Less

Check:	All Must Pass
Registry Key:	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa
Registry Value:	RestrictAnonymous

CIS-CAT Expected...	CIS-CAT Collected...
the registry key's *type* to be set to **reg_dword**	reg_dword
the registry key's *value* to be set to **1**	0

References:

- **CCE-IDv5:** CCE-34723-7 -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

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

Fail

Description:

This policy setting determines whether Credential Manager (formerly called Stored User Names and Passwords) saves passwords or credentials for later use when it gains domain authentication.

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

Note: Changes to this setting will not take effect until Windows is restarted.

Rationale:

Passwords that are cached can be accessed by the user when logged on to the computer. Although this information may sound obvious, a problem can arise if the user unknowingly executes hostile code that reads the passwords and forwards them to another, unauthorized user.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security
Options\Network access: Do not allow storage of passwords and credentials for network authentication
```

Impact:

Credential Manager will not store passwords and credentials on the computer. Users will be forced to enter passwords whenever they log on to their Passport account or other network resources that aren't accessible to their domain account. Testing has shown that clients running Windows Vista or Windows Server 2008 will be unable to connect to Distributed File System (DFS) shares in untrusted domains. Enabling this setting also makes it impossible to specify alternate credentials for scheduled tasks, this can cause a variety of problems. For example, some third party backup products will no longer work. This policy setting should have no impact on users who access network resources that are configured to allow access with their Active Directory-based domain account.

Assessment:

Ensure 'DisableDomainCreds' is 'Windows: Registry Value' to '1' -- Less

Check:	All Must Pass
Registry Key:	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa
Registry Value:	DisableDomainCreds

CIS-CAT Expected...	CIS-CAT Collected...
the registry key's *type* to be set to **reg_dword**	reg_dword
the registry key's *value* to be set to **1**	0

References:

- **CCE-IDv5:** CCE-33718-8 -- More

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

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

Pass

Description:

This policy setting determines what additional permissions are assigned for anonymous connections to the computer.

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

Rationale:

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

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security
Options\Network access: Let Everyone permissions apply to anonymous users
```

Impact:

None - this is the default behavior.

Assessment:

Ensure 'EveryoneIncludesAnonymous' is 'Windows: Registry Value' to '0' -- More

References:

- **CCE-IDv5:** CCE-35367-2 -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More
- **Control 14: Controlled Access Based on the Need to Know:** -- More

Back to Summary

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

Pass

Description:

This policy setting determines which communication sessions, or pipes, will have attributes and permissions that allow anonymous access.

The recommended state for this setting is: `<blank>` (i.e. None).

Rationale:

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

Remediation:

To establish the recommended configuration via GP, set the following UI path to `<blank>` (i.e. None):

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security
Options\Network access: Named Pipes that can be accessed anonymously
```

Impact:

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

Assessment:

Ensure 'NullSessionPipes' is 'Windows: Registry Value' to '' -- More

References:

- **CCE-IDv5:** CCE-34965-4 -- More

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More
- **Control 14: Controlled Access Based on the Need to Know:** -- More

CIS Controls V6.1:

- **Control 14: Controlled Access Based on the Need to Know:** -- More

Back to Summary

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

Pass

Description:

This policy setting determines which registry paths will be accessible over the network, regardless of the users or groups listed in the access control list (ACL) of the `winreg` registry key.

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

Note #2: When you configure this setting you specify a list of one or more objects. The delimiter used when entering the list is a line feed or carriage return, that is, type the first object on the list, press the Enter button, type the next object, press Enter again, etc. The setting value is stored as a comma-delimited list in group policy security templates. It is also rendered as a comma-delimited list in Group Policy Editor's display pane and the Resultant Set of Policy console. It is recorded in the registry as a line-feed delimited list in a REG_MULTI_SZ value.

The recommended state for this setting is:

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

Rationale:

The registry is a database that contains computer configuration information, and much of the information is sensitive. An attacker could use this information to facilitate unauthorized activities. To reduce the risk of such an attack, suitable ACLs are assigned throughout the registry to help protect it from access by unauthorized users.

Remediation:

To establish the recommended configuration via GP, set the following UI path to: `System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Control\Server Applications SOFTWARE\Microsoft\Windows NT\CurrentVersion`

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security
Options\Network access: Remotely accessible registry paths
```

Impact:

None - this is the default behavior. However, if you remove the default registry paths from the list of accessible ones, remote management tools such as the Microsoft Baseline Security Analyzer and Microsoft Systems Management Server could fail, as they require remote access to the registry to properly monitor and manage computers.

Note: If you want to allow remote access, you must also enable the Remote Registry service.

Assessment:

Ensure 'Machine' is 'Windows: Registry Value' to 'System\CurrentControlSet\Control\ProductOptions,System\CurrentControlSet\Control\Server Applications,Software\Microsoft\Windows NT\CurrentVersion' -- More

References:

- **CCE-IDv5:** CCE-33976-2 -- More

CIS Controls V6.1:

- **Control 14: Controlled Access Based on the Need to Know:** -- More
- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

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

Pass

Description:

This policy setting determines which registry paths and sub-paths will be accessible over the network, regardless of the users or groups listed in the access control list (ACL) of the `winreg` registry key.

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

Note #2: When you configure this setting you specify a list of one or more objects. The delimiter used when entering the list is a line feed or carriage return, that is, type the first object on the list, press the Enter button, type the next object, press Enter again, etc. The setting value is stored as a comma-delimited list in group policy security templates. It is also rendered as a comma-delimited list in Group Policy Editor's display pane and the Resultant Set of Policy console. It is recorded in the registry as a line-feed delimited list in a REG_MULTI_SZ value.

The recommended state for this setting is:

```
System\CurrentControlSet\Control\Print\Printers
System\CurrentControlSet\Services\Eventlog
Software\Microsoft\OLAP Server
Software\Microsoft\Windows NT\CurrentVersion\Print
Software\Microsoft\Windows NT\CurrentVersion\Windows
System\CurrentControlSet\Control\ContentIndex
System\CurrentControlSet\Control\Terminal Server
System\CurrentControlSet\Control\Terminal Server\UserConfig
System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration
Software\Microsoft\Windows NT\CurrentVersion\Perflib
System\CurrentControlSet\Services\SysmonLog
```

Rationale:

The registry contains sensitive computer configuration information that could be used by an attacker to facilitate unauthorized activities. The fact that the default ACLs assigned throughout the registry are fairly restrictive and help to protect the registry from access by unauthorized users reduces the risk of such an attack.

Remediation:

To establish the recommended configuration via GP, set the following UI path to: `System\CurrentControlSet\Control\Print\Printers System\CurrentControlSet\Services\Eventlog SOFTWARE\Microsoft\OLAP Server SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows System\CurrentControlSet\Control\ContentIndex System\CurrentControlSet\Control\Terminal Server System\CurrentControlSet\Control\Terminal Server\UserConfig System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib System\CurrentControlSet\Services\SysmonLog`

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security
Options\Network access: Remotely accessible registry paths and sub-paths
```

Impact:

None - this is the default behavior. However, if you remove the default registry paths from the list of accessible ones, remote management tools such as the Microsoft Baseline Security Analyzer and Microsoft Systems Management Server could fail, as they require remote access to the registry to properly monitor and manage computers.

Note: If you want to allow remote access, you must also enable the Remote Registry service.

Assessment:

Ensure 'Machine' is 'Windows: Registry Value' to 'System\CurrentControlSet\Control\Print\Printers,System\CurrentControlSet\Services\Eventlog,Software\Microsoft\OLAP Server,Software\Microsoft\Windows NT\CurrentVersion\Print,Software\Microsoft\Windows NT\Cu -- More

References:

- **CCE-IDv5:** CCE-35300-3 -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More
- **Control 14: Controlled Access Based on the Need to Know:** -- More

Back to Summary

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

Pass

Description:

When enabled, this policy setting restricts anonymous access to only those shares and pipes that are named in the `Network access: Named pipes that can be accessed anonymously` and `Network access: Shares that can be accessed anonymously` settings. This policy setting controls null session access to shares on your computers by adding `RestrictNullSessAccess` with the value `1` in the

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters
```

registry key. This registry value toggles null session shares on or off to control whether the server service restricts unauthenticated clients' access to named resources.

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

Rationale:

Null sessions are a weakness that can be exploited through shares (including the default shares) on computers in your environment.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security
Options\Network access: Restrict anonymous access to Named Pipes and Shares
```

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.

Assessment:

Ensure 'RestrictNullSessAccess' is 'Windows: Registry Value' to '1' -- More

References:

- **CCE-IDv5:** CCE-33563-8 -- More

CIS Controls V6.1:

- **Control 14: Controlled Access Based on the Need to Know:** -- More
- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

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

Fail

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.

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.)

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security
Options\Network access: Restrict clients allowed to make remote calls to SAM
```

Impact:

None - this is the default behavior.

Assessment:

Ensure 'restrictremotesam' is 'Windows: Registry Value' to 'O:BAG:BAD:(A;;RC;;;BA)' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa:restrictremotesam                  does not exist
```

References:

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

CIS Controls V6.1:

- **Control 5: Controlled Use of Administrative Privileges:** -- More
- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

Back to Summary

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

Pass

Description:

This policy setting determines which network shares can be accessed by anonymous users. The default configuration for this policy setting has little effect because all users have to be authenticated before they can access shared resources on the server.

The recommended state for this setting is: `<blank>` (i.e. None).

Rationale:

It is very dangerous to allow any values in this setting. Any shares that are listed can be accessed by any network user, which could lead to the exposure or corruption of sensitive data.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `<blank>` (i.e. None):

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security
Options\Network access: Shares that can be accessed anonymously
```

Impact:

None - this is the default behavior.

Assessment:

Any of the following tests or sub-groups may pass:

Ensure 'NullSessionShares' is 'Existence Test' to 'none_exist' -- More

Ensure 'NullSessionShares' is 'Windows: Registry Value' to '' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters:NullSessionShares          does not exist
```

References:

- **CCE-IDv5:** CCE-34651-0 -- More

CIS Controls V6.1:

- **Control 14: Controlled Access Based on the Need to Know:** -- More
- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

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

Pass

Description:

This policy setting determines how network logons that use local accounts are authenticated. The Classic option allows precise control over access to resources, including the ability to assign different types of access to different users for the same resource. The Guest only option allows you to treat all users equally. In this context, all users authenticate as Guest only to receive the same access level to a given resource.

The recommended state for this setting is: `Classic - local users authenticate as themselves`.

Note: This setting does not affect interactive logons that are performed remotely by using such services as Telnet or Remote Desktop Services (formerly called Terminal Services).

Rationale:

With the Guest only model, any user who can authenticate to your computer over the network does so with guest privileges, which probably means that they will not have write access to shared resources on that computer. Although this restriction does increase security, it makes it more difficult for authorized users to access shared resources on those computers because ACLs on those resources must include access control entries (ACEs) for the Guest account. With the Classic model, local accounts should be password protected. Otherwise, if Guest access is enabled, anyone can use those user accounts to access shared system resources.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Classic - local users authenticate as themselves`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security
Options\Network access: Sharing and security model for local accounts
```

Impact:

None - this is the default configuration for domain-joined computers.

Assessment:

Ensure 'ForceGuest' is 'Windows: Registry Value' to '0' -- More

References:

- **CCE-IDv5:** CCE-33719-6 -- More

CIS Controls V6.1:

- **Control 14: Controlled Access Based on the Need to Know:** -- More
- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

2.3.11 Network security

This section contains recommendations related to network security.

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

Fail

Description:

This policy setting determines whether Local System services that use Negotiate when reverting to NTLM authentication can use the computer identity. This policy is supported on at least Windows 7 or Windows Server 2008 R2.

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

Rationale:

When connecting to computers running versions of Windows earlier than Windows Vista or Windows Server 2008 (non-R2), services running as Local System and using SPNEGO (Negotiate) that revert to NTLM use the computer identity. In Windows 7, if you are connecting to a computer running Windows Server 2008 or Windows Vista, then a system service uses either the computer identity or a NULL session. When connecting with a NULL session, a system-generated session key is created, which provides no protection but allows applications to sign and encrypt data without errors. When connecting with the computer identity, both signing and encryption is supported in order to provide data protection.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security
Options\Network security: Allow Local System to use computer identity for NTLM
```

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.

Assessment:

Ensure 'UseMachineId' is 'Windows: Registry Value' to '1' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa:UseMachineId                    does not exist
```

References:

- **CCE-IDv5:** CCE-33141-3 -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More
- **Control 14: Controlled Access Based on the Need to Know:** -- More

Back to Summary

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

Fail

Description:

This policy setting determines whether NTLM is allowed to fall back to a NULL session when used with LocalSystem.

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

Rationale:

NULL sessions are less secure because by definition they are unauthenticated.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security
Options\Network security: Allow LocalSystem NULL session fallback
```

Impact:

None - this is the default behavior. Any applications that require NULL sessions for LocalSystem will not work as designed.

Assessment:

Ensure 'AllowNullSessionFallback' is 'Windows: Registry Value' to '0' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0:AllowNullSessionFallback      does not exist
```

References:

- **CCE-IDv5:** CCE-35410-0 -- More

CIS Controls V6.1:

- **Control 14: Controlled Access Based on the Need to Know:** -- More

Back to Summary

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

Fail

Description:

This setting determines if online identities are able to authenticate to this computer.

The Public Key Cryptography Based User-to-User (PKU2U) protocol introduced in Windows 7 and Windows Server 2008 R2 is implemented as a security support provider (SSP). The SSP enables peer-to-peer authentication, particularly through the Windows 7 media and file sharing feature called HomeGroup, which permits sharing between computers that are not members of a domain.

With PKU2U, a new extension was introduced to the Negotiate authentication package, `Spnego.dll`. In previous versions of Windows, Negotiate decided whether to use Kerberos or NTLM for authentication. The extension SSP for Negotiate, `Negoexts.dll`, which is treated as an authentication protocol by Windows, supports Microsoft SSPs including PKU2U.

When computers are configured to accept authentication requests by using online IDs, `Negoexts.dll` calls the PKU2U SSP on the computer that is used to log on. The PKU2U SSP obtains a local certificate and exchanges the policy between the peer computers. When validated on the peer computer, the certificate within the metadata is sent to the logon peer for validation and associates the user's certificate to a security token and the logon process completes.

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

Rationale:

The PKU2U protocol is a peer-to-peer authentication protocol - authentication should be managed centrally in most managed networks.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security
Options\Network Security: Allow PKU2U authentication requests to this computer to use online identities
```

Impact:

None - this is the default configuration for domain-joined computers.

Assessment:

Ensure 'AllowOnlineID' is 'Windows: Registry Value' to '0' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\pku2u:AllowOnlineID does not exist

References:

- **CCE-IDv5:** CCE-35411-8 -- More

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

2.3.11.4 (L1) Ensure 'Network security: Configure encryption types allowed for Kerberos' is set to 'AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types'

Fail

Description:

This policy setting allows you to set the encryption types that Kerberos is allowed to use.

The recommended state for this setting is: `AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types`.

Rationale:

The strength of each encryption algorithm varies from one to the next, choosing stronger algorithms will reduce the risk of compromise however doing so may cause issues when the computer attempts to authenticate with systems that do not support them.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security
Options\Network security: Configure encryption types allowed for Kerberos
```

Impact:

If not selected, the encryption type will not be allowed. This setting may affect compatibility with client computers or services and applications. Multiple selections are permitted.

Note: Some legacy applications and OSes may require `RC4_HMAC_MD5` - we recommend you test in your environment and verify whether you can safely remove it.

Note #2: Windows Vista and below allow DES for Kerberos by default, but later OS versions do not.

Assessment:

Ensure 'SupportedEncryptionTypes' is 'Windows: Registry Value' to '2147483640' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\Kerberos\Parameters:SupportedEncryptionTypes does not exist

References:

- **CCE-IDv5:** CCE-35786-3 -- More

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

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

Pass

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.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security
Options\Network security: Do not store LAN Manager hash value on next password change
```

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.

Assessment:

Ensure 'NoLMHash' is 'Windows: Registry Value' to '1' -- More

References:

- **CCE-IDv5:** CCE-35225-2 -- More

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

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

Pass

Description:

This policy setting determines whether to disconnect users who are connected to the local computer outside their user account's valid logon hours. This setting affects the Server Message Block (SMB) component. If you enable this policy setting you should also enable *Microsoft network server: Disconnect clients when logon hours expire* (Rule 2.3.9.4).

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

Rationale:

If this setting is disabled, a user could remain connected to the computer outside of their allotted logon hours.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security
Options\Network security: Force logoff when logon hours expire
```

Impact:

None - this is the default behavior.

Assessment:

Ensure 'Forced Logoff' is 'Equals' to '0' -- More

References:

- **CCE-IDv5:** CCE-34993-6 -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

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

Fail

Description:

LAN Manager (LM) was a family of early Microsoft client/server software (predating Windows NT) that allowed users to link personal computers together on a single network. LM network capabilities included transparent file and print sharing, user security features, and network administration tools. In Active Directory domains, the Kerberos protocol is the default authentication protocol. However, if the Kerberos protocol is not negotiated for some reason, Active Directory will use LM, NTLM, or NTLMv2. LAN Manager authentication includes the LM, NTLM, and NTLM version 2 (NTLMv2) variants, and is the protocol that is used to authenticate all Windows clients when they perform the following operations:

- Join a domain
- Authenticate between Active Directory forests
- Authenticate to down-level domains
- Authenticate to computers that do not run Windows 2000, Windows Server 2003, or Windows XP
- Authenticate to computers that are not in the domain

The Network security: LAN Manager authentication level setting determines which challenge/response authentication protocol is used for network logons. This choice affects the level of authentication protocol used by clients, the level of session security negotiated, and the level of authentication accepted by servers.

The recommended state for this setting is: `Send NTLMv2 response only. Refuse LM & NTLM`.

Rationale:

Windows 2000 and Windows XP clients were configured by default to send LM and NTLM authentication responses

(Windows 95-based and Windows 98-based clients only send LM). The default settings in OSes predating Windows Vista / Windows Server 2008 (non-R2) allowed all clients to authenticate with servers and use their resources. However, this meant that LM responses - the weakest form of authentication response - were sent over the network, and it was potentially possible for attackers to sniff that traffic to more easily reproduce the user's password.

The Windows 95, Windows 98, and Windows NT operating systems cannot use the Kerberos version 5 protocol for authentication. For this reason, in a Windows Server 2003 domain, these computers authenticate by default with both the LM and NTLM protocols for network authentication. You can enforce a more secure authentication protocol for Windows 95, Windows 98, and Windows NT by using NTLMv2. For the logon process, NTLMv2 uses a secure channel to protect the authentication process. Even if you use NTLMv2 for older clients and servers, Windows-based clients and servers that are members of the domain will use the Kerberos authentication protocol to authenticate with Windows Server 2003 or newer Domain Controllers. For these reasons, it is strongly preferred to restrict the use of LM & NTLM (non-v2) as much as possible.

Remediation:

To establish the recommended configuration via GP, set the following UI path to: `Send NTLMv2 response only. Refuse LM & NTLM`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security
Options\Network security: LAN Manager authentication level
```

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.

Note: For information about a hotfix to ensure that this setting works in networks that include Windows NT 4.0-based computers along with Windows 2000, Windows XP, and Windows Server 2003-based computers, see Microsoft Knowledge Base article 305379: Authentication Problems in Windows 2000 with NTLM 2 Levels Above 2 in a Windows NT 4.0 Domain.

Assessment:

Ensure 'LmCompatibilityLevel' is 'Windows: Registry Value' to '5' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa:LmCompatibilityLevel                does not exist
```

References:

- **CCE-IDv5:** CCE-35302-9 -- More

CIS Controls V6.1:

- **Control 13: Data Protection:** -- More

Back to Summary

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

Pass

Description:

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

Note: This policy setting does not have any impact on LDAP simple bind (`ldap_simple_bind`) or LDAP simple bind through SSL (`ldap_simple_bind_s`). No Microsoft LDAP clients that are included with Windows XP Professional use `ldap_simple_bind` or `ldap_simple_bind_s` to communicate with a Domain Controller.

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

Rationale:

Unsigned network traffic is susceptible to man-in-the-middle attacks in which an intruder captures the packets between the client and server, modifies them, and then forwards them to the server. For an LDAP server, this susceptibility means that an attacker could cause a server to make decisions that are based on false or altered data from the LDAP queries. To lower this risk in your network, you can implement strong physical security measures to protect the network infrastructure. Also, you can make all types of man-in-the-middle attacks extremely difficult if you require digital signatures on all network packets by means of IPsec authentication headers.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security
Options\Network security: LDAP client signing requirements
```

Impact:

None - this is the default behavior. However, if you choose instead to configure the server to *require* LDAP signatures then you must also configure the client. If you do not configure the client it will not be able to communicate with the server, which could cause many features to fail, including user authentication, Group Policy, and logon scripts, because the caller will be told that the LDAP BIND command request failed.

Assessment:

Ensure 'LDAPClientIntegrity' is 'Windows: Registry Value' to '1' -- More

References:

- **CCE-IDv5:** CCE-33802-0 -- More

CIS Controls V6.1:

- **Control 13: Data Protection:** -- More

Back to Summary

2.3.11.9 (L1) Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' is set to 'Require NTLMv2 session security, Require 128-bit encryption'

Fail

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.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Require NTLMv2 session security, Require 128-bit encryption`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security
Options\Network security: Minimum session security for NTLM SSP based (including secure RPC) clients
```

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. This setting could impact Windows Clustering when applied to servers running Windows Server 2003, see Microsoft Knowledge Base article 890761: You receive an "Error 0x8007042b" error message when you add or join a node to a cluster if you use NTLM version 2 in Windows Server 2003 for more information on possible issues and how to resolve them.

Assessment:

Ensure 'NTLMMinClientSec' is 'Windows: Registry Value' to '537395200' -- Less

Check:	All Must Pass
Registry Key:	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0
Registry Value:	NTLMMinClientSec

CIS-CAT Expected...	CIS-CAT Collected...
the registry key's *type* to be set to **reg_dword**	reg_dword
the registry key's *value* to be set to **537395200**	536870912

References:

- **CCE-IDv5:** CCE-35447-2 -- More

CIS Controls V6.1:

- **Control 13: Data Protection:** -- More

Back to Summary

2.3.11.10 (L1) Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require NTLMv2 session security, Require 128-bit encryption'

Fail

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.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Require NTLMv2 session security, Require 128-bit encryption`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security
Options\Network security: Minimum session security for NTLM SSP based (including secure RPC) servers
```

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. This setting could impact Windows Clustering when applied to servers running Windows Server 2003, see Microsoft Knowledge Base article 890761: You receive an "Error 0x8007042b" error message when you add or join a node to a cluster if you use NTLM version 2 in Windows Server 2003 for more information on possible issues and how to resolve them.

Assessment:

Ensure 'NTLMMinServerSec' is 'Windows: Registry Value' to '537395200' -- Less

Check:	All Must Pass
Registry Key:	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0
Registry Value:	NTLMMinServerSec

CIS-CAT Expected...	CIS-CAT Collected...
the registry key's *type* to be set to **reg_dword**	reg_dword
the registry key's *value* to be set to **537395200**	536870912

References:

- **CCE-IDv5:** CCE-35108-0 -- More

CIS Controls V6.1:

- **Control 13: Data Protection:** -- More

Back to Summary

2.3.12 Recovery console

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

2.3.13 Shutdown

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

2.3.14 System cryptography

This section contains recommendations related to system cryptography.

2.3.15 System objects

This section contains recommendations related to system objects.

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

Pass

Description:

This policy setting determines whether case insensitivity is enforced for all subsystems. The Microsoft Win32 subsystem is case insensitive. However, the kernel supports case sensitivity for other subsystems, such as the

Portable Operating System Interface for UNIX (POSIX). Because Windows is case insensitive (but the POSIX subsystem will support case sensitivity), failure to enforce this policy setting makes it possible for a user of the POSIX subsystem to create a file with the same name as another file by using mixed case to label it. Such a situation can block access to these files by another user who uses typical Win32 tools, because only one of the files will be available.

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

Rationale:

Because Windows is case-insensitive but the POSIX subsystem will support case sensitivity, failure to enable this policy setting would make it possible for a user of that subsystem to create a file with the same name as another file but with a different mix of upper and lower case letters. Such a situation could potentially confuse users when they try to access such files from normal Win32 tools because only one of the files will be available.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security
Options\System objects: Require case insensitivity for non-Windows subsystems
```

Impact:

None - this is the default behavior.

Assessment:

Ensure 'ObCaseInsensitive' is equal to '1' -- More

References:

- **CCE-IDv5:** CCE-35008-2 -- More

Back to Summary

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

Pass

Description:

This policy setting determines the strength of the default discretionary access control list (DACL) for objects. Active Directory maintains a global list of shared system resources, such as DOS device names, mutexes, and semaphores. In this way, objects can be located and shared among processes. Each type of object is created with a default DACL that specifies who can access the objects and what permissions are granted.

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

Rationale:

This setting determines the strength of the default DACL for objects. Windows maintains a global list of shared computer resources so that objects can be located and shared among processes. Each type of object is created with a default DACL that specifies who can access the objects and with what permissions.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security
Options\System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)
```

Impact:

None - this is the default behavior.

Assessment:

Ensure 'ProtectionMode' is 'Windows: Registry Value' to '1' -- More

References:

- **CCE-IDv5:** CCE-35232-8 -- More

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More

CIS Controls V6.1:

- **Control 14: Controlled Access Based on the Need to Know:** -- More

Back to Summary

2.3.16 System settings

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

2.3.17 User Account Control

This section contains recommendations related to User Account Control.

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

Fail

Description:

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

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

Rationale:

One of the risks that the User Account Control feature introduced with Windows Vista is trying to mitigate is that of malicious software running under elevated credentials without the user or administrator being aware of its activity. An attack vector for these programs was to discover the password of the account named "Administrator" because that user account was created for all installations of Windows. To address this risk, in Windows Vista and newer, the built-in Administrator account is now disabled by default. In a default installation of a new computer, accounts with administrative control over the computer are initially set up in one of two ways:

- If the computer is not joined to a domain, the first user account you create has the equivalent permissions as a local administrator.
- If the computer is joined to a domain, no local administrator accounts are created. The Enterprise or Domain Administrator must log on to the computer and create one if a local administrator account is warranted.

Once Windows is installed, the built-in Administrator account may be manually enabled, but we strongly recommend that this account remain disabled.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User
Account Control: Admin Approval Mode for the Built-in Administrator account
```

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.

Assessment:

Ensure 'FilterAdministratorToken' is 'Windows: Registry Value' to '1' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System:FilterAdministratorToken          does not exist
```

References:

- **CCE-IDv5:** CCE-35338-3 -- More

CIS Controls V6.1:

- **Control 5: Controlled Use of Administrative Privileges:** -- More

Back to Summary

2.3.17.2 (L1) Ensure 'User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop' is set to 'Disabled'

Pass

Description:

This policy setting controls whether User Interface Accessibility (UIAccess or UIA) programs can automatically disable the secure desktop for elevation prompts used by a standard user.

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

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 allows the administrator to perform operations that require elevated privileges while connected via Remote Assistance. This increases security in that organizations can use UAC even when end user support is provided remotely. However, it also reduces security by adding the risk that an administrator might allow an unprivileged user to share elevated privileges for an application that the administrator needs to use during the Remote Desktop session.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User
Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop
```

Impact:

None - this is the default behavior.

Assessment:

Ensure 'EnableUIADesktopToggle' is 'Windows: Registry Value' to '0' -- More

References:

- **CCE-IDv5:** CCE-35458-9 -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

2.3.17.3 (L1) Ensure 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' is set to 'Prompt for consent on the secure desktop'

Fail

Description:

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

The recommended state for this setting is: `Prompt for consent on the secure desktop`.

Rationale:

One of the risks that the UAC feature introduced with Windows Vista is trying to mitigate is that of malicious software running under elevated credentials without the user or administrator being aware of its activity. This setting raises awareness to the administrator of elevated privilege operations and permits the administrator to prevent a malicious program from elevating its privilege when the program attempts to do so.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Prompt for consent on the secure desktop`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User
Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode
```

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.

Assessment:

Ensure 'ConsentPromptBehaviorAdmin' is 'Windows: Registry Value' to '2' -- Less

Check:	All Must Pass
Registry Key:	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System
Registry Value:	ConsentPromptBehaviorAdmin

CIS-CAT Expected...	CIS-CAT Collected...
the registry key's *type* to be set to **reg_dword**	reg_dword
the registry key's *value* to be set to **2**	5

References:

- **CCE-IDv5:** CCE-33784-0 -- More

CIS Controls V6.1:

- **Control 5: Controlled Use of Administrative Privileges:** -- More

Back to Summary

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

Fail

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.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Automatically deny elevation requests`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User
Account Control: Behavior of the elevation prompt for standard users
```

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.

Assessment:

Ensure 'ConsentPromptBehaviorUser' is 'Windows: Registry Value' to '0' -- Less

Check:	All Must Pass
Registry Key:	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System
Registry Value:	ConsentPromptBehaviorUser

CIS-CAT Expected...	CIS-CAT Collected...
the registry key's *type* to be set to **reg_dword**	reg_dword
the registry key's *value* to be set to **0**	3

References:

- **CCE-IDv5:** CCE-33785-7 -- More

CIS Controls V6.1:

- **Control 5: Controlled Use of Administrative Privileges:** -- More

Back to Summary

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

Pass

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

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User
Account Control: Detect application installations and prompt for elevation
```

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.

Assessment:

Ensure 'EnableInstallerDetection' is 'Windows: Registry Value' to '1' -- More

References:

- **CCE-IDv5:** CCE-35429-0 -- More

CIS Controls V6.1:

- **Control 5: Controlled Use of Administrative Privileges:** -- More

Back to Summary

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

Pass

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.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User
Account Control: Only elevate UIAccess applications that are installed in secure locations
```

Impact:

None - this is the default behavior.

Assessment:

Ensure 'EnableSecureUIAPaths' is 'Windows: Registry Value' to '1' -- More

References:

- **CCE-IDv5:** CCE-35401-9 -- More

CIS Controls V6.1:

- **Control 5: Controlled Use of Administrative Privileges:** -- More

Back to Summary

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

Pass

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.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User
Account Control: Run all administrators in Admin Approval Mode
```

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.

Assessment:

Ensure 'EnableLUA' is 'Windows: Registry Value' to '1' -- More

References:

- **CCE-IDv5:** CCE-33788-1 -- More

CIS Controls V6.1:

- **Control 5: Controlled Use of Administrative Privileges:** -- More

Back to Summary

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

Pass

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.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User
Account Control: Switch to the secure desktop when prompting for elevation
```

Impact:

None - this is the default behavior.

Assessment:

Ensure 'PromptOnSecureDesktop' is 'Windows: Registry Value' to '1' -- More

References:

- **CCE-IDv5:** CCE-33815-2 -- More

CIS Controls V6.1:

- **Control 5: Controlled Use of Administrative Privileges:** -- More

Back to Summary

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

Pass

Description:

This policy setting controls whether application write failures are redirected to defined registry and file system locations. This policy setting mitigates applications that run as administrator and write run-time application data to:

- `%ProgramFiles%`
- `%Windir%`
- `%Windir%\system32`
- `HKEY_LOCAL_MACHINE\Software`

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

Rationale:

This setting reduces vulnerabilities by ensuring that legacy applications only write data to permitted locations.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User
Account Control: Virtualize file and registry write failures to per-user locations
```

Impact:

None - this is the default behavior.

Assessment:

Ensure 'EnableVirtualization' is 'Windows: Registry Value' to '1' -- More

References:

- **CCE-IDv5:** CCE-35459-7 -- More

Back to Summary

3 Event Log

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

4 Restricted Groups

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

5 System Services

This section contains recommendations for system services.

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

Fail

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.

Remediation:

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

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

Impact:

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

Assessment:

Any of the following tests or sub-groups may pass:

Ensure 'Start' is 'Windows: Registry Value' to '4' -- Less

Check:	All Must Pass
Registry Key:	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Browser
Registry Value:	Start

CIS-CAT Expected...	CIS-CAT Collected...
the registry key's *type* to be set to **reg_dword**	reg_dword
the registry key's *value* to be set to **4**	3

Ensure 'Start' is 'Existence Test' to 'none_exist' -- Less

CIS-CAT did not expect to collect any matching registry items, and found 1 item.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Browser:Start	exists

References:

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

CIS Controls V6.1:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

Back to Summary

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

Pass

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.

Remediation:

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

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

Impact:

IIS will not function, including Web, SMTP or FTP services.

Assessment:

Any of the following tests or sub-groups may pass:

Ensure 'Start' is 'Windows: Registry Value' to '4' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\IISADMIN:Start	does not exist

Ensure 'Start' is 'Existence Test' to 'none_exist' -- More

References:

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

CIS Controls V6.1:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

Back to Summary

5.7 (L1) Ensure 'Infrared monitor service (irmon)' is set to 'Disabled'

Fail

Description:

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

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

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.

Remediation:

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

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

Impact:

Infrared file transfers will be prevented from working.

Assessment:

Ensure 'Start' is 'Windows: Registry Value' to '4' -- Less

Check:	All Must Pass
Registry Key:	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\irmon
Registry Value:	Start

CIS-CAT Expected...	CIS-CAT Collected...
the registry key's *type* to be set to **reg_dword**	reg_dword
the registry key's *value* to be set to **4**	3

References:

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

CIS Controls V6.1:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

Back to Summary

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

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Internet Connection
Sharing (ICS)
```

Impact:

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

Assessment:

Ensure 'Start' is 'Windows: Registry Value' to '4' -- Less

Check:	All Must Pass
Registry Key:	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess
Registry Value:	Start

CIS-CAT Expected...	CIS-CAT Collected...
the registry key's *type* to be set to **reg_dword**	reg_dword
the registry key's *value* to be set to **4**	3

References:

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

CIS Controls V6.1:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

Back to Summary

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

Pass

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.

Remediation:

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

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

Impact:

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

Assessment:

Any of the following tests or sub-groups may pass:

Ensure 'Start' is 'Windows: Registry Value' to '4' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LxssManager:Start does not exist

Ensure 'Start' is 'Existence Test' to 'none_exist' -- More

References:

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

CIS Controls V6.1:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

Back to Summary

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

Pass

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.

Remediation:

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

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

Impact:

The computer will not function as an FTP server.

Assessment:

Any of the following tests or sub-groups may pass:

Ensure 'Start' is 'Windows: Registry Value' to '4' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\FTPSVC:Start                    does not exist
```

Ensure 'Start' is 'Existence Test' to 'none_exist' -- More

References:

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

CIS Controls V6.1:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

Back to Summary

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

Pass

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.

Remediation:

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

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

Impact:

The workstation will not be permitted to be a SSH host server.

Assessment:

Any of the following tests or sub-groups may pass:

Ensure 'Start' is 'Windows: Registry Value' to '4' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\sshd:Start does not exist

Ensure 'Start' is 'Existence Test' to 'none_exist' -- More

References:

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

Back to Summary

5.24 (L1) Ensure 'Remote Procedure Call (RPC) Locator (RpcLocator)' is set to 'Disabled'

Fail

Description:

In Windows 2003 and older versions of Windows, the Remote Procedure Call (RPC) Locator service manages the RPC name service database. In Windows Vista and newer versions of Windows, this service does not provide any functionality and is present for application compatibility.

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

Rationale:

This is a legacy service that has no value or purpose other than application compatibility for very old software. It should be disabled unless there is a specific old application still in use on the system that requires it.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Remote Procedure Call
(RPC) Locator
```

Impact:

No impact, unless an old, legacy application requires it.

Assessment:

Ensure 'Start' is 'Windows: Registry Value' to '4' -- Less

Check:	All Must Pass
Registry Key:	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RpcLocator
Registry Value:	Start

CIS-CAT Expected...	CIS-CAT Collected...
the registry key's *type* to be set to **reg_dword**	reg_dword
the registry key's *value* to be set to **4**	3

References:

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

CIS Controls V6.1:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

Back to Summary

5.26 (L1) Ensure 'Routing and Remote Access (RemoteAccess)' is set to 'Disabled'

Pass

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.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Routing and Remote
Access
```

Impact:

The computer will not be able to be configured as a Windows router between different connections.

Assessment:

Ensure 'Start' is 'Windows: Registry Value' to '4' -- More

References:

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

CIS Controls V6.1:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

Back to Summary

5.28 (L1) Ensure 'Simple TCP/IP Services (simptcp)' is set to 'Disabled' or 'Not Installed'

Pass

Description:

Supports the following TCP/IP services: Character Generator, Daytime, Discard, Echo, and Quote of the Day.

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

Note: This service is not installed by default. It is supplied with Windows, but is installed by enabling an optional Windows feature (*Simple TCPIP services (i.e. echo, daytime etc)*).

Rationale:

The Simple TCP/IP Services have very little purpose in a modern enterprise environment - allowing them might increase exposure and risk for attack.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Simple TCP/IP
Services
```

Impact:

The Simple TCP/IP services (Character Generator, Daytime, Discard, Echo and Quote of the Day) will not be available.

Assessment:

Any of the following tests or sub-groups may pass:

Ensure 'Start' is 'Windows: Registry Value' to '4' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\simptcp:Start does not exist

Ensure 'Start' is 'Existence Test' to 'none_exist' -- More

References:

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

CIS Controls V6.1:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

Back to Summary

5.30 (L1) Ensure 'SSDP Discovery (SSDPSRV)' is set to 'Disabled'

Fail

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. 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.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\System Services\SSDP Discovery
```

Impact:

SSDP-based devices will not be discovered.

Assessment:

Ensure 'Start' is 'Windows: Registry Value' to '4' -- Less

Check:	All Must Pass
Registry Key:	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SSDPSRV
Registry Value:	Start

CIS-CAT Expected...	CIS-CAT Collected...
the registry key's *type* to be set to **reg_dword**	reg_dword
the registry key's *value* to be set to **4**	3

References:

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

CIS Controls V6.1:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

Back to Summary

5.31 (L1) Ensure 'UPnP Device Host (upnphost)' is set to 'Disabled'

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\System Services\UPnP Device Host
```

Impact:

Any hosted UPnP devices will stop functioning and no additional hosted devices can be added.

Assessment:

Ensure 'Start' is 'Windows: Registry Value' to '4' -- Less

Check:	All Must Pass

Registry Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\upnphost
Registry Value: Start

CIS-CAT Expected...	CIS-CAT Collected...
the registry key's *type* to be set to **reg_dword**	reg_dword
the registry key's *value* to be set to **4**	3

References:

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

CIS Controls V6.1:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

Back to Summary

5.32 (L1) Ensure 'Web Management Service (WMSvc)' is set to 'Disabled' or 'Not Installed'

Pass

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.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Web Management
Service
```

Impact:

Remote web-based management of IIS will not be available.

Assessment:

Any of the following tests or sub-groups may pass:

Ensure 'Start' is 'Windows: Registry Value' to '4' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WMSvc:Start does not exist

Ensure 'Start' is 'Existence Test' to 'none_exist' -- More

References:

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

CIS Controls V6.1:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

Back to Summary

5.35 (L1) Ensure 'Windows Media Player Network Sharing Service (WMPNetworkSvc)' is set to 'Disabled' or 'Not Installed'

Pass

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.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Windows Media Player
Network Sharing Service
```

Impact:

Windows Media Player libraries will not be shared over the network to other devices and systems.

Assessment:

Any of the following tests or sub-groups may pass:

Ensure 'Start' is 'Existence Test' to 'none_exist' -- More

Ensure 'Start' is 'Windows: Registry Value' to '4' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WMPNetworkSvc:Start                does not exist
```

References:

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

CIS Controls V6.1:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

Back to Summary

5.36 (L1) Ensure 'Windows Mobile Hotspot Service (icssvc)' is set to 'Disabled'

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Windows Mobile
Hotspot Service
```

Impact:

The Windows Mobile Hotspot feature will not be available.

Assessment:

Ensure 'Start' is 'Windows: Registry Value' to '4' -- Less

Check:	All Must Pass	
Registry Key:	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\icssvc	
Registry Value:	Start	
CIS-CAT Expected...		CIS-CAT Collected...
the registry key's *type* to be set to **reg_dword**		reg_dword
the registry key's *value* to be set to **4**		3

References:

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

CIS Controls V6.1:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

Back to Summary

5.40 (L1) Ensure 'World Wide Web Publishing Service (W3SVC)' is set to 'Disabled' or 'Not Installed'

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\System Services\World Wide Web
Publishing Service
```

Impact:

IIS Web Services will not function.

Assessment:

Any of the following tests or sub-groups may pass:

Ensure 'Start' is 'Existence Test' to 'none_exist' -- Less

CIS-CAT did not expect to collect any matching registry items, and found 1 item.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC:Start	exists

Ensure 'Start' is 'Windows: Registry Value' to '4' -- Less

Check:	All Must Pass
Registry Key:	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC
Registry Value:	Start

CIS-CAT Expected...	CIS-CAT Collected...
the registry key's *type* to be set to **reg_dword**	reg_dword
the registry key's *value* to be set to **4**	2

References:

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

CIS Controls V6.1:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

Back to Summary

5.41 (L1) Ensure 'Xbox Accessory Management Service (XboxGipSvc)' is set to 'Disabled'

Fail

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).

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Xbox Accessory
Management Service
```

Impact:

Connected Xbox accessories may not function.

Assessment:

Ensure 'Start' is 'Windows: Registry Value' to '4' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\XboxGipSvc:Start                does not exist
```

References:

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

CIS Controls V6.1:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

Back to Summary

5.42 (L1) Ensure 'Xbox Game Monitoring (xbgm)' is set to 'Disabled'

Fail

Description:

This service supports Xbox Game Monitoring.

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).

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Xbox Game Monitoring
```

Impact:

Xbox game monitoring will not be available.

Assessment:

Ensure 'Start' is 'Windows: Registry Value' to '4' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.	
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\xbgm:Start	does not exist

References:

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

CIS Controls V6.1:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

Back to Summary

5.43 (L1) Ensure 'Xbox Live Auth Manager (XblAuthManager)' is set to 'Disabled'

Fail

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).

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Xbox Live Auth
Manager
```

Impact:

Connections to Xbox Live may fail and applications that interact with that service may also fail.

Assessment:

Ensure 'Start' is 'Windows: Registry Value' to '4' -- Less

Check:	All Must Pass
Registry Key:	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\XblAuthManager
Registry Value:	Start

CIS-CAT Expected...	CIS-CAT Collected...
the registry key's *type* to be set to **reg_dword**	reg_dword
the registry key's *value* to be set to **4**	3

References:

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

CIS Controls V6.1:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

Back to Summary

5.44 (L1) Ensure 'Xbox Live Game Save (XblGameSave)' is set to 'Disabled'

Fail

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).

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Xbox Live Game Save
```

Impact:

Game save data will not upload to or download from Xbox Live.

Assessment:

Ensure 'Start' is 'Windows: Registry Value' to '4' -- Less

Check:	All Must Pass
Registry Key:	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\XblGameSave
Registry Value:	Start

CIS-CAT Expected...	CIS-CAT Collected...
the registry key's *type* to be set to **reg_dword**	reg_dword
the registry key's *value* to be set to **4**	3

References:

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

CIS Controls V6.1:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

Back to Summary

5.45 (L1) Ensure 'Xbox Live Networking Service (XboxNetApiSvc)' is set to 'Disabled'

Fail

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).

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Xbox Live Networking
Service
```

Impact:

Connections to Xbox Live may fail and applications that interact with that service may also fail.

Assessment:

Ensure 'Start' is 'Windows: Registry Value' to '4' -- Less

Check:	All Must Pass
Registry Key:	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\XboxNetApiSvc
Registry Value:	Start

CIS-CAT Expected...	CIS-CAT Collected...
the registry key's *type* to be set to **reg_dword**	reg_dword
the registry key's *value* to be set to **4**	3

References:

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

CIS Controls V6.1:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

Back to Summary

6 Registry

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

7 File System

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

8 Wired Network (IEEE 802.3) Policies

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

9 Windows Firewall with Advanced Security

This section contains recommendations for configuring the Windows Firewall.

9.1 Domain Profile

This section contains recommendations for the Domain Profile of the Windows Firewall.

9.1.1 (L1) Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)'

Fail

Description:

Select On (recommended) to have Windows Firewall with Advanced Security use the settings for this profile to filter network traffic. If you select Off, Windows Firewall with Advanced Security will not use any of the firewall rules or connection security rules for this profile.

The recommended state for this setting is: `On (recommended)`.

Rationale:

If the firewall is turned off all traffic will be able to access the system and an attacker may be more easily able to remotely exploit a weakness in a network service.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `On (recommended)`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced
Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Firewall
state
```

Impact:

None - this is the default behavior.

Assessment:

Ensure 'EnableFirewall' is 'Windows: Registry Value' to '1' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\DomainProfile:EnableFirewall        does not exist
```

References:

- **CCE-IDv5:** CCE-33160-3 -- More

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

CIS Controls V6.1:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

Back to Summary

9.1.2 (L1) Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)'

Fail

Description:

This setting determines the behavior for inbound connections that do not match an inbound firewall rule.

The recommended state for this setting is: `Block (default)`.

Rationale:

If the firewall allows all traffic to access the system then an attacker may be more easily able to remotely exploit a weakness in a network service.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Block (default)`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced
Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Inbound
connections
```

Impact:

None - this is the default behavior.

Assessment:

Ensure 'DefaultInboundAction' is 'Windows: Registry Value' to '1' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\DomainProfile:DefaultInboundAction        does not exist
```

References:

- **CCE-IDv5:** CCE-33063-9 -- More

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

CIS Controls V6.1:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

Back to Summary

9.1.3 (L1) Ensure 'Windows Firewall: Domain: Outbound connections' is set to 'Allow (default)'

Fail

Description:

This setting determines the behavior for outbound connections that do not match an outbound firewall rule.

The recommended state for this setting is: `Allow (default)`.

Rationale:

Some people believe that it is prudent to block all outbound connections except those specifically approved by the user or administrator. Microsoft disagrees with this opinion, blocking outbound connections by default will force users to deal with a large number of dialog boxes prompting them to authorize or block applications such as their web browser or instant messaging software. Additionally, blocking outbound traffic has little value because if an attacker has compromised the system they can reconfigure the firewall anyway.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Allow (default)`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced
Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Outbound
connections
```

Impact:

None - this is the default behavior.

Assessment:

Ensure 'DefaultOutboundAction' is 'Windows: Registry Value' to '0' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\DomainProfile:DefaultOutboundAction does not exist

References:

- **CCE-IDv5:** CCE-33098-5 -- More

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

CIS Controls V6.1:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

Back to Summary

9.1.4 (L1) Ensure 'Windows Firewall: Domain: Settings: Display a notification' is set to 'No'

Fail

Description:

Select this option to have Windows Firewall with Advanced Security display notifications to the user when a program is blocked from receiving inbound connections.

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

Note: When the `Apply local firewall rules` setting is configured to `No`, it's recommended to also configure the `Display a notification setting` to `No`. Otherwise, users will continue to receive messages that ask if they want to unblock a restricted inbound connection, but the user's response will be ignored.

Rationale:

Firewall notifications can be complex and may confuse the end users, who would not be able to address the alert.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced
Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Settings
Customize\Display a notification
```

Impact:

Windows Firewall will not display a notification when a program is blocked from receiving inbound connections.

Assessment:

Ensure 'DisableNotifications' is 'Windows: Registry Value' to '1' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\DomainProfile:DisableNotifications does not exist

References:

- **CCE-IDv5:** CCE-33062-1 -- More

Back to Summary

9.1.5 (L1) Ensure 'Windows Firewall: Domain: Logging: Name' is set to '%SYSTEMROOT%\System32\logfiles\firewall\domainfw.log'

Fail

Description:

Use this option to specify the path and name of the file in which Windows Firewall will write its log information.

The recommended state for this setting is: `%SYSTEMROOT%\System32\logfiles\firewall\domainfw.log`.

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `%SYSTEMROOT%\System32\logfiles\firewall\domainfw.log`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced
Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Logging
Customize\Name
```

Impact:

The log file will be stored in the specified file.

Assessment:

Ensure 'LogFilePath' is 'Windows: Registry Value' to '%SYSTEMROOT%\System32\logfiles\firewall\domainfw.log' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\DomainProfile\Logging:LogFilePath        does not exist
```

References:

- **CCE-IDv5:** CCE-34176-8 -- More

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More
- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More

CIS Controls V6.1:

- **Control 6: Maintenance, Monitoring, and Analysis of Audit Logs:** -- More

Back to Summary

9.1.6 (L1) Ensure 'Windows Firewall: Domain: Logging: Size limit (KB)' is set to '16,384 KB or greater'

Fail

Description:

Use this option to specify the size limit of the file in which Windows Firewall will write its log information.

The recommended state for this setting is: `16,384 KB or greater`.

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `16,384 KB or greater`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced
Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Logging
Customize\Size limit (KB)
```

Impact:

The log file size will be limited to the specified size, old events will be overwritten by newer ones when the limit is reached.

Assessment:

Ensure 'LogFileSize' is 'Windows: Registry Value' to '16384' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\DomainProfile\Logging:LogFileSize          does not exist
```

References:

- **CCE-IDv5:** CCE-35083-5 -- More

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More

CIS Controls V6.1:

- **Control 6: Maintenance, Monitoring, and Analysis of Audit Logs:** -- More

Back to Summary

9.1.7 (L1) Ensure 'Windows Firewall: Domain: Logging: Log dropped packets' is set to 'Yes'

Fail

Description:

Use this option to log when Windows Firewall with Advanced Security discards an inbound packet for any reason. The log records why and when the packet was dropped. Look for entries with the word `DROP` in the action column of the log.

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

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced
Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Logging
Customize\Log dropped packets
```

Impact:

Information about dropped packets will be recorded in the firewall log file.

Assessment:

Ensure 'LogDroppedPackets' is 'Windows: Registry Value' to '1' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\DomainProfile\Logging:LogDroppedPackets          does not exist
```

References:

- **CCE-IDv5:** CCE-35252-6 -- More

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More
- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More

CIS Controls V6.1:

- **Control 6: Maintenance, Monitoring, and Analysis of Audit Logs:** -- More

Back to Summary

9.1.8 (L1) Ensure 'Windows Firewall: Domain: Logging: Log successful connections' is set to 'Yes'

Fail

Description:

Use this option to log when Windows Firewall with Advanced Security allows an inbound connection. The log records why and when the connection was formed. Look for entries with the word `ALLOW` in the action column of the log.

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

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced
Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Logging
Customize\Log successful connections
```

Impact:

Information about successful connections will be recorded in the firewall log file.

Assessment:

Ensure 'LogSuccessfulConnections' is 'Windows: Registry Value' to '1' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\DomainProfile\Logging:LogSuccessfulConnections does not exist

References:

- **CCE-IDv5:** CCE-35306-0 -- More

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More
- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More

CIS Controls V6.1:

- **Control 6: Maintenance, Monitoring, and Analysis of Audit Logs:** -- More

Back to Summary

9.2 Private Profile

This section contains recommendations for the Private Profile of the Windows Firewall.

9.2.1 (L1) Ensure 'Windows Firewall: Private: Firewall state' is set to 'On (recommended)'

Fail

Description:

Select On (recommended) to have Windows Firewall with Advanced Security use the settings for this profile to filter network traffic. If you select Off, Windows Firewall with Advanced Security will not use any of the firewall rules or connection security rules for this profile.

The recommended state for this setting is: `On (recommended)`.

Rationale:

If the firewall is turned off all traffic will be able to access the system and an attacker may be more easily able to remotely exploit a weakness in a network service.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `On (recommended)`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced
Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Firewall
state
```

Impact:

None - this is the default behavior.

Assessment:

Ensure 'EnableFirewall' is 'Windows: Registry Value' to '1' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\PrivateProfile:EnableFirewall does not exist

References:

- **CCE-IDv5:** CCE-33066-2 -- More

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

CIS Controls V6.1:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

Back to Summary

9.2.2 (L1) Ensure 'Windows Firewall: Private: Inbound connections' is set to 'Block (default)'

Fail

Description:

This setting determines the behavior for inbound connections that do not match an inbound firewall rule.

The recommended state for this setting is: `Block (default)`.

Rationale:

If the firewall allows all traffic to access the system then an attacker may be more easily able to remotely exploit a weakness in a network service.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Block (default)`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced
Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Inbound
connections
```

Impact:

None - this is the default behavior.

Assessment:

Ensure 'DefaultInboundAction' is 'Windows: Registry Value' to '1' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\PrivateProfile:DefaultInboundAction          does not exist
```

References:

- **CCE-IDv5:** CCE-33161-1 -- More

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

CIS Controls V6.1:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

Back to Summary

9.2.3 (L1) Ensure 'Windows Firewall: Private: Outbound connections' is set to 'Allow (default)'

Fail

Description:

This setting determines the behavior for outbound connections that do not match an outbound firewall rule.

The recommended state for this setting is: `Allow (default)`.

Note: If you set Outbound connections to Block and then deploy the firewall policy by using a GPO, computers that receive the GPO settings cannot receive subsequent Group Policy updates unless you create and deploy an outbound rule that enables Group Policy to work. Predefined rules for Core Networking include outbound rules that enable Group Policy to work. Ensure that these outbound rules are active, and thoroughly test firewall profiles before deploying.

Rationale:

Some people believe that it is prudent to block all outbound connections except those specifically approved by the user or administrator. Microsoft disagrees with this opinion, blocking outbound connections by default will force users to deal with a large number of dialog boxes prompting them to authorize or block applications such as their web browser or instant messaging software. Additionally, blocking outbound traffic has little value because if an attacker has compromised the system they can reconfigure the firewall anyway.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Allow (default)`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced
Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Outbound
connections
```

Impact:

None - this is the default behavior.

Assessment:

Ensure 'DefaultOutboundAction' is 'Windows: Registry Value' to '0' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\PrivateProfile:DefaultOutboundAction        does not exist
```

References:

- **CCE-IDv5:** CCE-33162-9 -- More

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

CIS Controls V6.1:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

Back to Summary

9.2.4 (L1) Ensure 'Windows Firewall: Private: Settings: Display a notification' is set to 'No'

Fail

Description:

Select this option to have Windows Firewall with Advanced Security display notifications to the user when a program is blocked from receiving inbound connections.

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

Note: When the `Apply local firewall rules` setting is configured to `No`, it's recommended to also configure the `Display a notification` setting to `No`. Otherwise, users will continue to receive messages that ask if they want to unblock a restricted inbound connection, but the user's response will be ignored.

Rationale:

Firewall notifications can be complex and may confuse the end users, who would not be able to address the alert.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced
Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Settings
Customize\Display a notification
```

Impact:

Windows Firewall will not display a notification when a program is blocked from receiving inbound connections.

Assessment:

Ensure 'DisableNotifications' is 'Windows: Registry Value' to '1' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\PrivateProfile:DisableNotifications        does not exist
```

References:

- **CCE-IDv5:** CCE-33065-4 -- More

Back to Summary

9.2.5 (L1) Ensure 'Windows Firewall: Private: Logging: Name' is set to '%SYSTEMROOT%\System32\logfiles\firewall\privatefw.log'

Fail

Description:

Use this option to specify the path and name of the file in which Windows Firewall will write its log information.

The recommended state for this setting is: `%SYSTEMROOT%\System32\logfiles\firewall\privatefw.log`.

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `%SYSTEMROOT%\System32\logfiles\firewall\privatefw.log`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced
Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Logging
Customize\Name
```

Impact:

The log file will be stored in the specified file.

Assessment:

Ensure 'LogFilePath' is 'Windows: Registry Value' to '%SYSTEMROOT%\System32\logfiles\firewall\privatefw.log' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\PrivateProfile\Logging:LogFilePath does not exist

References:

- **CCE-IDv5:** CCE-33437-5 -- More

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More
- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More

CIS Controls V6.1:

- **Control 6: Maintenance, Monitoring, and Analysis of Audit Logs:** -- More

Back to Summary

9.2.6 (L1) Ensure 'Windows Firewall: Private: Logging: Size limit (KB)' is set to '16,384 KB or greater'

Fail

Description:

Use this option to specify the size limit of the file in which Windows Firewall will write its log information.

The recommended state for this setting is: `16,384 KB or greater`.

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `16,384 KB or greater`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced
Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Logging
Customize\Size limit (KB)
```

Impact:

The log file size will be limited to the specified size, old events will be overwritten by newer ones when the limit is reached.

Assessment:

Ensure 'LogFileSize' is 'Windows: Registry Value' to '16384' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\PrivateProfile\Logging:LogFileSize          does not exist
```

References:

- **CCE-IDv5:** CCE-34356-6 -- More

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More

CIS Controls V6.1:

- **Control 6: Maintenance, Monitoring, and Analysis of Audit Logs:** -- More

Back to Summary

9.2.7 (L1) Ensure 'Windows Firewall: Private: Logging: Log dropped packets' is set to 'Yes'

Fail

Description:

Use this option to log when Windows Firewall with Advanced Security discards an inbound packet for any reason. The log records why and when the packet was dropped. Look for entries with the word `DROP` in the action column of the log.

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

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced
Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Logging
Customize\Log dropped packets
```

Impact:

Information about dropped packets will be recorded in the firewall log file.

Assessment:

Ensure 'LogDroppedPackets' is 'Windows: Registry Value' to '1' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\PrivateProfile\Logging:LogDroppedPackets     does not exist
```

References:

- **CCE-IDv5:** CCE-33436-7 -- More

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More
- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More

CIS Controls V6.1:

- **Control 6: Maintenance, Monitoring, and Analysis of Audit Logs:** -- More

Back to Summary

9.2.8 (L1) Ensure 'Windows Firewall: Private: Logging: Log successful connections' is set to 'Yes'

Fail

Description:

Use this option to log when Windows Firewall with Advanced Security allows an inbound connection. The log records why and when the connection was formed. Look for entries with the word `ALLOW` in the action column of the log.

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

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced
Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Logging
Customize\Log successful connections
```

Impact:

Information about successful connections will be recorded in the firewall log file.

Assessment:

Ensure 'LogSuccessfulConnections' is 'Windows: Registry Value' to '1' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\PrivateProfile\Logging:LogSuccessfulConnections        does not exist
```

References:

- **CCE-IDv5:** CCE-34177-6 -- More

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More

CIS Controls V6.1:

- **Control 6: Maintenance, Monitoring, and Analysis of Audit Logs:** -- More

Back to Summary

9.3 Public Profile

This section contains recommendations for the Public Profile of the Windows Firewall.

9.3.1 (L1) Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)'

Fail

Description:

Select On (recommended) to have Windows Firewall with Advanced Security use the settings for this profile to filter network traffic. If you select Off, Windows Firewall with Advanced Security will not use any of the firewall rules or connection security rules for this profile.

The recommended state for this setting is: `On (recommended)`.

Rationale:

If the firewall is turned off all traffic will be able to access the system and an attacker may be more easily able to remotely exploit a weakness in a network service.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `On (recommended)`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced
Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Firewall
state
```

Impact:

None - this is the default behavior.

Assessment:

Ensure 'EnableFirewall' is 'Windows: Registry Value' to '1' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\PublicProfile:EnableFirewall          does not exist
```

References:

- **CCE-IDv5:** CCE-35703-8 -- More

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

CIS Controls V6.1:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

Back to Summary

9.3.2 (L1) Ensure 'Windows Firewall: Public: Inbound connections' is set to 'Block (default)'

Fail

Description:

This setting determines the behavior for inbound connections that do not match an inbound firewall rule.

The recommended state for this setting is: `Block (default)`.

Rationale:

If the firewall allows all traffic to access the system then an attacker may be more easily able to remotely exploit a weakness in a network service.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Block (default)`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced
Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Inbound
connections
```

Impact:

None - this is the default behavior.

Assessment:

Ensure 'DefaultInboundAction' is 'Windows: Registry Value' to '1' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\PublicProfile:DefaultInboundAction does not exist

References:

- **CCE-IDv5:** CCE-33069-6 -- More

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

CIS Controls V6.1:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

Back to Summary

9.3.3 (L1) Ensure 'Windows Firewall: Public: Outbound connections' is set to 'Allow (default)'

Fail

Description:

This setting determines the behavior for outbound connections that do not match an outbound firewall rule.

The recommended state for this setting is: `Allow (default)`.

Note: If you set Outbound connections to Block and then deploy the firewall policy by using a GPO, computers that receive the GPO settings cannot receive subsequent Group Policy updates unless you create and deploy an outbound rule that enables Group Policy to work. Predefined rules for Core Networking include outbound rules that enable Group Policy to work. Ensure that these outbound rules are active, and thoroughly test firewall profiles before deploying.

Rationale:

Some people believe that it is prudent to block all outbound connections except those specifically approved by the user or administrator. Microsoft disagrees with this opinion, blocking outbound connections by default will force users to deal with a large number of dialog boxes prompting them to authorize or block applications such as their web browser or instant messaging software. Additionally, blocking outbound traffic has little value because if an attacker has compromised the system they can reconfigure the firewall anyway.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Allow (default)`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced
Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Outbound
connections
```

Impact:

None - this is the default behavior.

Assessment:

Ensure 'DefaultOutboundAction' is 'Windows: Registry Value' to '0' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\PublicProfile:DefaultOutboundAction          does not exist
```

References:

- **CCE-IDv5:** CCE-33070-4 -- More

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

CIS Controls V6.1:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

Back to Summary

9.3.4 (L1) Ensure 'Windows Firewall: Public: Settings: Display a notification' is set to 'No'

Fail

Description:

Select this option to have Windows Firewall with Advanced Security display notifications to the user when a program is blocked from receiving inbound connections.

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

Rationale:

Some organizations may prefer to avoid alarming users when firewall rules block certain types of network activity. However, notifications can be helpful when troubleshooting network issues involving the firewall.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced
Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Settings
Customize\Display a notification
```

Impact:

Windows Firewall will not display a notification when a program is blocked from receiving inbound connections.

Assessment:

Ensure 'DisableNotifications' is 'Windows: Registry Value' to '1' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\PublicProfile:DisableNotifications      does not exist
```

References:

- **CCE-IDv5:** CCE-33068-8 -- More

Back to Summary

9.3.5 (L1) Ensure 'Windows Firewall: Public: Settings: Apply local firewall rules' is set to 'No'

Fail

Description:

This setting controls whether local administrators are allowed to create local firewall rules that apply together with firewall rules configured by Group Policy.

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

Note: When the `Apply local firewall rules` setting is configured to `No`, it's recommended to also configure the `Display a notification` setting to `No`. Otherwise, users will continue to receive messages that ask if they want to unblock a restricted inbound connection, but the user's response will be ignored.

Rationale:

When in the Public profile, there should be no special local firewall exceptions per computer. These settings should be managed by a centralized policy.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced
Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Settings
Customize\Apply local firewall rules
```

Impact:

Administrators can still create firewall rules, but the rules will not be applied.

Assessment:

Ensure 'AllowLocalPolicyMerge' is 'Windows: Registry Value' to '0' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\PublicProfile:AllowLocalPolicyMerge      does not exist
```

References:

- **CCE-IDv5:** CCE-35537-0 -- More

CIS Controls V6.1:

- **Control 5: Controlled Use of Administrative Privileges:** -- More

Back to Summary

9.3.6 (L1) Ensure 'Windows Firewall: Public: Settings: Apply local connection security rules' is set to 'No'

Fail

Description:

This setting controls whether local administrators are allowed to create connection security rules that apply together with connection security rules configured by Group Policy.

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

Rationale:

Users with administrative privileges might create firewall rules that expose the system to remote attack.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced
Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Settings
Customize\Apply local connection security rules
```

Impact:

Administrators can still create local connection security rules, but the rules will not be applied.

Assessment:

Ensure 'AllowLocalIPsecPolicyMerge' is 'Windows: Registry Value' to '0' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\PublicProfile:AllowLocalIPsecPolicyMerge        does not exist
```

References:

- **CCE-IDv5:** CCE-33099-3 -- More

CIS Controls V6.1:

- **Control 5: Controlled Use of Administrative Privileges:** -- More

Back to Summary

9.3.7 (L1) Ensure 'Windows Firewall: Public: Logging: Name' is set to '%SYSTEMROOT%\System32\logfiles\firewall\publicfw.log'

Fail

Description:

Use this option to specify the path and name of the file in which Windows Firewall will write its log information.

The recommended state for this setting is: `%SYSTEMROOT%\System32\logfiles\firewall\publicfw.log`.

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `%SYSTEMROOT%\System32\logfiles\firewall\publicfw.log`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced
Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Logging
Customize\Name
```

Impact:

The log file will be stored in the specified file.

Assessment:

Ensure 'LogFilePath' is 'Windows: Registry Value' to '%SYSTEMROOT%\System32\logfiles\firewall\publicfw.log' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\PublicProfile\Logging:LogFilePath          does not exist
```

References:

- **CCE-IDv5:** CCE-35117-1 -- More

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More
- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More

CIS Controls V6.1:

- **Control 6: Maintenance, Monitoring, and Analysis of Audit Logs:** -- More

Back to Summary

9.3.8 (L1) Ensure 'Windows Firewall: Public: Logging: Size limit (KB)' is set to '16,384 KB or greater'

Fail

Description:

Use this option to specify the size limit of the file in which Windows Firewall will write its log information.

The recommended state for this setting is: `16,384 KB or greater`.

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `16,384 KB or greater`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced
Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Logging
Customize\Size limit (KB)
```

Impact:

The log file size will be limited to the specified size, old events will be overwritten by newer ones when the limit is reached.

Assessment:

Ensure 'LogFileSize' is 'Windows: Registry Value' to '16384' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\PublicProfile\Logging:LogFileSize          does not exist
```

References:

- **CCE-IDv5:** CCE-35421-7 -- More

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More

CIS Controls V6.1:

- **Control 6: Maintenance, Monitoring, and Analysis of Audit Logs:** -- More

Back to Summary

9.3.9 (L1) Ensure 'Windows Firewall: Public: Logging: Log dropped packets' is set to 'Yes'

Fail

Description:

Use this option to log when Windows Firewall with Advanced Security discards an inbound packet for any reason. The log records why and when the packet was dropped. Look for entries with the word `DROP` in the action column of the log.

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

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced
Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Logging
Customize\Log dropped packets
```

Impact:

Information about dropped packets will be recorded in the firewall log file.

Assessment:

Ensure 'LogDroppedPackets' is 'Windows: Registry Value' to '1' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\PublicProfile\Logging:LogDroppedPackets does not exist

References:

- **CCE-IDv5:** CCE-35116-3 -- More

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More
- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More

CIS Controls V6.1:

- **Control 6: Maintenance, Monitoring, and Analysis of Audit Logs:** -- More

Back to Summary

9.3.10 (L1) Ensure 'Windows Firewall: Public: Logging: Log successful connections' is set to 'Yes'

Fail

Description:

Use this option to log when Windows Firewall with Advanced Security allows an inbound connection. The log records why and when the connection was formed. Look for entries with the word `ALLOW` in the action column of the log.

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

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced
Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Logging
Customize\Log successful connections
```

Impact:

Information about successful connections will be recorded in the firewall log file.

Assessment:

Ensure 'LogSuccessfulConnections' is 'Windows: Registry Value' to '1' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\PublicProfile\Logging:LogSuccessfulConnections does not exist

References:

- **CCE-IDv5:** CCE-33734-5 -- More

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More
- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More

CIS Controls V6.1:

- **Control 6: Maintenance, Monitoring, and Analysis of Audit Logs:** -- More

Back to Summary

10 Network List Manager Policies

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

11 Wireless Network (IEEE 802.11) Policies

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

12 Public Key Policies

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

13 Software Restriction Policies

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

14 Network Access Protection NAP Client Configuration

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

15 Application Control Policies

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

16 IP Security Policies

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

17 Advanced Audit Policy Configuration

This section contains recommendations for configuring the Windows audit facilities.

17.1 Account Logon

This section contains recommendations for configuring the Account Logon audit policy.

17.1.1 (L1) Ensure 'Audit Credential Validation' is set to 'Success and Failure'

Fail

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.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Success and Failure`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Account Logon\Audit Credential Validation
```

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.

Assessment:

Ensure 'credential_validation' is 'Equals' to 'AUDIT_SUCCESS_FAILURE' -- Less

CIS-CAT Expected...	CIS-CAT Collected...
the Audit Sub-Category *credential_validation* to be set to **AUDIT_SUCCESS_FAILURE**	AUDIT_NONE

References:

- **CCE-IDv5:** CCE-35494-4 -- More

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More
- **Control 16: Account Monitoring and Control:** -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More
- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

17.2 Account Management

This section contains recommendations for configuring the Account Management audit policy.

17.2.1 (L1) Ensure 'Audit Application Group Management' is set to 'Success and

Fail

Failure'

Description:

This policy setting allows you to audit events generated by changes to application groups such as the following:

- Application group is created, changed, or deleted.
- Member is added or removed from an application group.

Application groups are utilized by Windows Authorization Manager, which is a flexible framework created by Microsoft for integrating role-based access control (RBAC) into applications. More information on Windows Authorization Manager is available at MSDN - Windows Authorization Manager.

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

Rationale:

Auditing events in this category may be useful when investigating an incident.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Success and Failure`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Account Management\Audit Application Group Management
```

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.

Assessment:

Ensure 'application_group_management' is 'Equals' to 'AUDIT_SUCCESS_FAILURE' -- Less

CIS-CAT Expected...	CIS-CAT Collected...
the Audit Sub-Category *application_group_management* to be set to **AUDIT_SUCCESS_FAILURE**	AUDIT_NONE

References:

- **CCE-IDv5:** CCE-32932-6 -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

17.2.2 (L1) Ensure 'Audit Computer Account Management' is set to 'Success and Failure'

Fail

Description:

This subcategory reports each event of computer account management, such as when a computer account is created, changed, deleted, renamed, disabled, or enabled. Events for this subcategory include:

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

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

Rationale:

Auditing events in this category may be useful when investigating an incident.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Success and Failure`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Account Management\Audit Computer Account Management
```

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.

Assessment:

Ensure 'computer_account_management' is 'Equals' to 'AUDIT_SUCCESS_FAILURE' -- Less

CIS-CAT Expected...	CIS-CAT Collected...
the Audit Sub-Category *computer_account_management* to be set to **AUDIT_SUCCESS_FAILURE**	AUDIT_NONE

References:

- **CCE-IDv5:** CCE-33410-2 -- More

CIS Controls V6.1:

- **Control 1: Inventory of Authorized and Unauthorized Devices:** -- More

Back to Summary

17.2.3 (L1) Ensure 'Audit Security Group Management' is set to include 'Success'

Pass

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.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Account Management\Audit Security Group Management
```

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.

Assessment:

Any of the following tests or sub-groups may pass:

Ensure 'security_group_management' is 'Equals' to 'AUDIT_SUCCESS_FAILURE' -- Less

CIS-CAT Expected...	CIS-CAT Collected...
the Audit Sub-Category *security_group_management* to be set to **AUDIT_SUCCESS_FAILURE**	AUDIT_SUCCESS

Ensure 'security_group_management' is 'Equals' to 'AUDIT_SUCCESS' -- More

References:

- **CCE-IDv5:** CCE-35498-5 -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

17.2.4 (L1) Ensure 'Audit User Account Management' is set to 'Success and Failure'

Fail

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.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Success and Failure`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Account Management\Audit User Account Management
```

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.

Assessment:

Ensure 'user_account_management' is 'Equals' to 'AUDIT_SUCCESS_FAILURE' -- Less

CIS-CAT Expected...	CIS-CAT Collected...
the Audit Sub-Category *user_account_management* to be set to **AUDIT_SUCCESS_FAILURE**	AUDIT_SUCCESS

References:

- **CCE-IDv5:** CCE-35499-3 -- More

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

17.3 Detailed Tracking

This section contains recommendations for configuring the Detailed Tracking audit policy.

17.3.1 (L1) Ensure 'Audit PNP Activity' is set to include 'Success'

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Detailed Tracking\Audit PNP Activity
```

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.

Assessment:

Any of the following tests or sub-groups may pass:

Ensure 'pnp_activity' is 'Equals' to 'AUDIT_SUCCESS' -- Less

CIS-CAT Expected...	CIS-CAT Collected...
the Audit Sub-Category *pnp_activity* to be set to **AUDIT_SUCCESS**	AUDIT_NONE

Ensure 'pnp_activity' is 'Equals' to 'AUDIT_SUCCESS_FAILURE' -- Less

CIS-CAT Expected...	CIS-CAT Collected...
the Audit Sub-Category *pnp_activity* to be set to **AUDIT_SUCCESS_FAILURE**	AUDIT_NONE

References:

CIS Controls V7.0:

- **Control 8: Malware Defenses:** -- More
- **Control 8: Malware Defenses:** -- More

CIS Controls V6.1:

- **Control 8: Malware Defenses:** -- More

Back to Summary

17.3.2 (L1) Ensure 'Audit Process Creation' is set to include 'Success'

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Detailed Tracking\Audit Process Creation
```

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.

Assessment:

Any of the following tests or sub-groups may pass:

Ensure 'process_creation' is 'Equals' to 'AUDIT_SUCCESS' -- Less

CIS-CAT Expected...	CIS-CAT Collected...
the Audit Sub-Category *process_creation* to be set to **AUDIT_SUCCESS**	AUDIT_NONE

Ensure 'process_creation' is 'Equals' to 'AUDIT_SUCCESS_FAILURE' -- Less

CIS-CAT Expected...	CIS-CAT Collected...
the Audit Sub-Category *process_creation* to be set to **AUDIT_SUCCESS_FAILURE**	AUDIT_NONE

References:

- **CCE-IDv5:** CCE-33040-7 -- More

Back to Summary

17.4 DS Access

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

17.5 Logon/Logoff

This section contains recommendations for configuring the Logon/Logoff audit policy.

17.5.1 (L1) Ensure 'Audit Account Lockout' is set to include 'Failure'

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Logon/Logoff\Audit Account Lockout
```

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.

Assessment:

Any of the following tests or sub-groups may pass:

Ensure 'account_lockout' is 'Equals' to 'AUDIT_FAILURE' -- Less

CIS-CAT Expected...	CIS-CAT Collected...
the Audit Sub-Category *account_lockout* to be set to **AUDIT_FAILURE**	AUDIT_SUCCESS

Ensure 'account_lockout' is 'Equals' to 'AUDIT_SUCCESS_FAILURE' -- Less

CIS-CAT Expected...	CIS-CAT Collected...
the Audit Sub-Category *account_lockout* to be set to **AUDIT_SUCCESS_FAILURE**	AUDIT_SUCCESS

References:

- **CCE-IDv5:** CCE-35504-0 -- More

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

17.5.2 (L1) Ensure 'Audit Group Membership' is set to include 'Success'

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Logon/Logoff\Audit Group Membership
```

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.

Assessment:

Any of the following tests or sub-groups may pass:

Ensure 'group_membership' is 'Equals' to 'AUDIT_SUCCESS' -- Less

CIS-CAT Expected...	CIS-CAT Collected...
the Audit Sub-Category *group_membership* to be set to **AUDIT_SUCCESS**	AUDIT_NONE

Ensure 'group_membership' is 'Equals' to 'AUDIT_SUCCESS_FAILURE' -- Less

CIS-CAT Expected...	CIS-CAT Collected...
the Audit Sub-Category *group_membership* to be set to **AUDIT_SUCCESS_FAILURE**	AUDIT_NONE

References:

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

17.5.3 (L1) Ensure 'Audit Logoff' is set to include 'Success'

Pass

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.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Logon/Logoff\Audit Logoff
```

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.

Assessment:

Any of the following tests or sub-groups may pass:

Ensure 'logoff' is 'Equals' to 'AUDIT_SUCCESS' -- More

Ensure 'logoff' is 'Equals' to 'AUDIT_SUCCESS_FAILURE' -- Less

CIS-CAT Expected...	CIS-CAT Collected...
the Audit Sub-Category *logoff* to be set to **AUDIT_SUCCESS_FAILURE**	AUDIT_SUCCESS

References:

- **CCE-IDv5:** CCE-35507-3 -- More

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

17.5.4 (L1) Ensure 'Audit Logon' is set to 'Success and Failure'

Fail

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.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Success and Failure`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Logon/Logoff\Audit Logon
```

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.

Assessment:

Ensure 'logon' is 'Equals' to 'AUDIT_SUCCESS_FAILURE' -- Less

CIS-CAT Expected...	CIS-CAT Collected...
the Audit Sub-Category *logon* to be set to **AUDIT_SUCCESS_FAILURE**	AUDIT_SUCCESS

References:

- **CCE-IDv5:** CCE-35508-1 -- More

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

17.5.5 (L1) Ensure 'Audit Other Logon/Logoff Events' is set to 'Success and Failure'

Fail

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.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Success and Failure`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Logon/Logoff\Audit Other Logon/Logoff Events
```

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.

Assessment:

Ensure 'other_logon_logoff_events' is 'Equals' to 'AUDIT_SUCCESS_FAILURE' -- Less

CIS-CAT Expected...	CIS-CAT Collected...
the Audit Sub-Category *other_logon_logoff_events* to be set to **AUDIT_SUCCESS_FAILURE**	AUDIT_NONE

References:

- **CCE-IDv5:** CCE-35510-7 -- More

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

17.5.6 (L1) Ensure 'Audit Special Logon' is set to include 'Success'

Pass

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.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Logon/Logoff\Audit Special Logon
```

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.

Assessment:

Any of the following tests or sub-groups may pass:

Ensure 'special_logon' is 'Equals' to 'AUDIT_SUCCESS' -- More

Ensure 'special_logon' is 'Equals' to 'AUDIT_SUCCESS_FAILURE' -- Less

CIS-CAT Expected...	CIS-CAT Collected...
the Audit Sub-Category *special_logon* to be set to **AUDIT_SUCCESS_FAILURE**	AUDIT_SUCCESS

References:

- **CCE-IDv5:** CCE-35511-5 -- More

CIS Controls V7.0:

- **Control 4: Controlled Use of Administrative Privileges:** -- More

CIS Controls V6.1:

- **Control 5: Controlled Use of Administrative Privileges:** -- More

Back to Summary

17.6 Object Access

This section contains recommendations for configuring the Object Access audit policy.

17.6.1 (L1) Ensure 'Audit Detailed File Share' is set to include 'Failure'

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Object Access\Audit Detailed File Share
```

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.

Assessment:

Any of the following tests or sub-groups may pass:

Ensure 'detailed_file_share' is 'Equals' to 'AUDIT_FAILURE' -- Less

CIS-CAT Expected...	CIS-CAT Collected...
the Audit Sub-Category *detailed_file_share* to be set to **AUDIT_FAILURE**	AUDIT_NONE

Ensure 'detailed_file_share' is 'Equals' to 'AUDIT_SUCCESS_FAILURE' -- Less

CIS-CAT Expected...	CIS-CAT Collected...
the Audit Sub-Category *detailed_file_share* to be set to **AUDIT_SUCCESS_FAILURE**	AUDIT_NONE

References:

- **CCE-IDv5:** CCE-35471-2 -- More

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More

Back to Summary

17.6.2 (L1) Ensure 'Audit File Share' is set to 'Success and Failure'

Fail

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.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Success and Failure`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Object Access\Audit File Share
```

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.

Assessment:

Ensure 'file_share' is 'Equals' to 'AUDIT_SUCCESS_FAILURE' -- Less

CIS-CAT Expected...	CIS-CAT Collected...
the Audit Sub-Category *file_share* to be set to **AUDIT_SUCCESS_FAILURE**	AUDIT_NONE

References:

- **CCE-IDv5:** CCE-35399-5 -- More

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More

CIS Controls V6.1:

- **Control 14: Controlled Access Based on the Need to Know:** -- More

Back to Summary

17.6.3 (L1) Ensure 'Audit Other Object Access Events' is set to 'Success and Failure'

Fail

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.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Success and Failure`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Object Access\Audit Other Object Access Events
```

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.

Assessment:

Ensure 'other_object_access_events' is 'Equals' to 'AUDIT_SUCCESS_FAILURE' -- Less

CIS-CAT Expected...	CIS-CAT Collected...
the Audit Sub-Category *other_object_access_events* to be set to **AUDIT_SUCCESS_FAILURE**	AUDIT_NONE

References:

- **CCE-IDv5:** CCE-35518-0 -- More

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More
- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More

CIS Controls V6.1:

- **Control 6: Maintenance, Monitoring, and Analysis of Audit Logs:** -- More

Back to Summary

17.6.4 (L1) Ensure 'Audit Removable Storage' is set to 'Success and Failure'

Fail

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.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Success and Failure`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Object Access\Audit Removable Storage
```

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.

Assessment:

Ensure 'removable_storage' is 'Equals' to 'AUDIT_SUCCESS_FAILURE' -- Less

CIS-CAT Expected...	CIS-CAT Collected...
the Audit Sub-Category *removable_storage* to be set to **AUDIT_SUCCESS_FAILURE**	AUDIT_NONE

References:

- **CCE-IDv5:** CCE-35520-6 -- More

CIS Controls V7.0:

- **Control 8: Malware Defenses:** -- More
- **Control 8: Malware Defenses:** -- More

CIS Controls V6.1:

- **Control 8: Malware Defenses:** -- More

Back to Summary

17.7 Policy Change

This section contains recommendations for configuring the Policy Change audit policy.

17.7.1 (L1) Ensure 'Audit Audit Policy Change' is set to include 'Success'

Pass

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.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Policy Change\Audit Audit Policy Change
```

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.

Assessment:

Any of the following tests or sub-groups may pass:

Ensure 'audit_policy_change' is 'Equals' to 'AUDIT_SUCCESS' -- More

Ensure 'audit_policy_change' is 'Equals' to 'AUDIT_SUCCESS_FAILURE' -- Less

CIS-CAT Expected...	CIS-CAT Collected...
the Audit Sub-Category *audit_policy_change* to be set to **AUDIT_SUCCESS_FAILURE**	AUDIT_SUCCESS

References:

- **CCE-IDv5:** CCE-35521-4 -- More

CIS Controls V7.0:

- **Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers:** -- More
- **Control 14: Controlled Access Based on the Need to Know:** -- More

CIS Controls V6.1:

- **Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers:** -- More

Back to Summary

17.7.2 (L1) Ensure 'Audit Authentication Policy Change' is set to include 'Success'

Pass

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.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Policy Change\Audit Authentication Policy Change
```

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.

Assessment:

Any of the following tests or sub-groups may pass:

Ensure 'authentication_policy_change' is 'Equals' to 'AUDIT_SUCCESS' -- More

Ensure 'authentication_policy_change' is 'Equals' to 'AUDIT_SUCCESS_FAILURE' -- Less

CIS-CAT Expected...	CIS-CAT Collected...
the Audit Sub-Category *authentication_policy_change* to be set to **AUDIT_SUCCESS_FAILURE**	AUDIT_SUCCESS

References:

- **CCE-IDv5:** CCE-33091-0 -- More

CIS Controls V7.0:

- **Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers:** -- More
- **Control 14: Controlled Access Based on the Need to Know:** -- More

CIS Controls V6.1:

- **Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers:** -- More

Back to Summary

17.7.3 (L1) Ensure 'Audit Authorization Policy Change' is set to include 'Success'

Fail

Description:

This subcategory reports changes in authorization policy. Events for this subcategory include:

- 4704: A user right was assigned.
- 4705: A user right was removed.
- 4706: A new trust was created to a domain.
- 4707: A trust to a domain was removed.
- 4714: Encrypted data recovery policy was changed.

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

Rationale:

Auditing these events may be useful when investigating a security incident.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Policy Change\Audit Authorization Policy Change
```

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.

Assessment:

Any of the following tests or sub-groups may pass:

Ensure 'authorization_policy_change' is 'Equal' to 'AUDIT_SUCCESS' -- Less

CIS-CAT Expected...	CIS-CAT Collected...
the Audit Sub-Category *authorization_policy_change* to be set to **AUDIT_SUCCESS**	AUDIT_NONE

Ensure 'authorization_policy_change' is 'Equal' to 'AUDIT_SUCCESS_FAILURE' -- Less

CIS-CAT Expected...	CIS-CAT Collected...
the Audit Sub-Category *authorization_policy_change* to be set to **AUDIT_SUCCESS_FAILURE**	AUDIT_NONE

References:

- **CCE-IDv5:** CCE-33042-3 -- More

CIS Controls V7.0:

- **Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers:** -- More
- **Control 14: Controlled Access Based on the Need to Know:** -- More

CIS Controls V6.1:

- **Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers:** -- More

Back to Summary

17.7.4 (L1) Ensure 'Audit MPSSVC Rule-Level Policy Change' is set to 'Success and Failure'

Fail

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.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Success and Failure`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Policy Change\Audit MPSSVC Rule-Level Policy Change
```

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.

Assessment:

Ensure 'mpssvc_rule_level_policy_change' is 'Equals' to 'AUDIT_SUCCESS_FAILURE' -- Less

CIS-CAT Expected...	CIS-CAT Collected...
the Audit Sub-Category *mpssvc_rule_level_policy_change* to be set to **AUDIT_SUCCESS_FAILURE**	AUDIT_NONE

References:

- **CCE-IDv5:** CCE-35532-1 -- More

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More

Back to Summary

17.7.5 (L1) Ensure 'Audit Other Policy Change Events' is set to include 'Failure'

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Policy Change\Audit Other Policy Change Events
```

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.

Assessment:

Any of the following tests or sub-groups may pass:

Ensure 'other_policy_change_events' is 'Equals' to 'AUDIT_FAILURE' -- Less

CIS-CAT Expected...	CIS-CAT Collected...
the Audit Sub-Category *other_policy_change_events* to be set to **AUDIT_FAILURE**	AUDIT_NONE

Ensure 'other_policy_change_events' is 'Equals' to 'AUDIT_SUCCESS_FAILURE' -- Less

CIS-CAT Expected...	CIS-CAT Collected...
the Audit Sub-Category *other_policy_change_events* to be set to **AUDIT_SUCCESS_FAILURE**	AUDIT_NONE

References:

- **CCE-IDv5:** CCE-35698-0 -- More

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More

Back to Summary

17.8 Privilege Use

This section contains recommendations for configuring the Privilege Use audit policy.

17.8.1 (L1) Ensure 'Audit Sensitive Privilege Use' is set to 'Success and Failure'

Fail

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.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Success and Failure`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\Privilege Use\Audit Sensitive Privilege Use
```

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.

Assessment:

Ensure 'sensitive_privilege_use' is 'Equals' to 'AUDIT_SUCCESS_FAILURE' -- Less

CIS-CAT Expected...	CIS-CAT Collected...
the Audit Sub-Category *sensitive_privilege_use* to be set to **AUDIT_SUCCESS_FAILURE**	AUDIT_NONE

References:

- **CCE-IDv5:** CCE-35524-8 -- More

CIS Controls V6.1:

- **Control 5: Controlled Use of Administrative Privileges:** -- More

Back to Summary

17.9 System

This section contains recommendations for configuring the System audit policy.

17.9.1 (L1) Ensure 'Audit IPsec Driver' is set to 'Success and Failure'

Fail

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.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Success and Failure`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\System\Audit IPsec Driver
```

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.

Assessment:

Ensure 'ipsec_driver' is 'Equals' to 'AUDIT_SUCCESS_FAILURE' -- Less

CIS-CAT Expected...	CIS-CAT Collected...
the Audit Sub-Category *ipsec_driver* to be set to **AUDIT_SUCCESS_FAILURE**	AUDIT_NONE

References:

- **CCE-IDv5:** CCE-35525-5 -- More

CIS Controls V6.1:

- **Control 13: Data Protection:** -- More

Back to Summary

17.9.2 (L1) Ensure 'Audit Other System Events' is set to 'Success and Failure'

Pass

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.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Success and Failure`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\System\Audit Other System Events
```

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.

Assessment:

Ensure 'other_system_events' is 'Equals' to 'AUDIT_SUCCESS_FAILURE' -- More

References:

- **CCE-IDv5:** CCE-32936-7 -- More

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

CIS Controls V6.1:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

Back to Summary

17.9.3 (L1) Ensure 'Audit Security State Change' is set to include 'Success'

Pass

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.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\System\Audit Security State Change
```

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.

Assessment:

Any of the following tests or sub-groups may pass:

Ensure 'security_state_change' is 'Equals' to 'AUDIT_SUCCESS_FAILURE' -- Less

CIS-CAT Expected...	CIS-CAT Collected...
the Audit Sub-Category *security_state_change* to be set to **AUDIT_SUCCESS_FAILURE**	AUDIT_SUCCESS

Ensure 'security_state_change' is 'Equals' to 'AUDIT_SUCCESS' -- More

References:

- **CCE-IDv5:** CCE-33043-1 -- More

Back to Summary

17.9.4 (L1) Ensure 'Audit Security System Extension' is set to include 'Success'

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\System\Audit Security System Extension
```

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.

Assessment:

Any of the following tests or sub-groups may pass:

Ensure 'security_system_extension' is 'Equals' to 'AUDIT_SUCCESS' -- Less

CIS-CAT Expected...	CIS-CAT Collected...
the Audit Sub-Category *security_system_extension* to be set to **AUDIT_SUCCESS**	AUDIT_NONE

Ensure 'security_system_extension' is 'Equals' to 'AUDIT_SUCCESS_FAILURE' -- Less

CIS-CAT Expected...	CIS-CAT Collected...
the Audit Sub-Category *security_system_extension* to be set to **AUDIT_SUCCESS_FAILURE**	AUDIT_NONE

References:

- **CCE-IDv5:** CCE-35526-3 -- More

CIS Controls V6.1:

- **Control 6: Maintenance, Monitoring, and Analysis of Audit Logs:** -- More

Back to Summary

17.9.5 (L1) Ensure 'Audit System Integrity' is set to 'Success and Failure'

Pass

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.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Success and Failure`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy
Configuration\Audit Policies\System\Audit System Integrity
```

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.

Assessment:

Ensure 'system_integrity' is 'Equals' to 'AUDIT_SUCCESS_FAILURE' -- More

References:

- **CCE-IDv5:** CCE-35527-1 -- More

CIS Controls V6.1:

- **Control 6: Maintenance, Monitoring, and Analysis of Audit Logs:** -- More

Back to Summary

18 Administrative Templates (Computer)

This section contains computer-based recommendations from Group Policy Administrative Templates (ADMX).

18.1 Control Panel

This section contains recommendations for Control Panel settings.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.1.1 Personalization

This section contains recommendations for Control Panel personalization settings.

This Group Policy section is provided by the Group Policy template `ControlPanelDisplay.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.1.1.1 (L1) Ensure 'Prevent enabling lock screen camera' is set to 'Enabled'

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Control Panel\Personalization\Prevent enabling
lock screen camera
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `ControlPanelDisplay.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

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.

Assessment:

Ensure 'NoLockScreenCamera' is 'Windows: Registry Value' to '1' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Personalization:NoLockScreenCamera          does not exist
```

References:

- **CCE-IDv5:** CCE-35799-6 -- More

Back to Summary

18.1.1.2 (L1) Ensure 'Prevent enabling lock screen slide show' is set to 'Enabled'

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Control Panel\Personalization\Prevent enabling
lock screen slide show
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `ControlPanelDisplay.admx/adml` that is included with the Microsoft Windows 8.1 & 2012 R2 Administrative Templates (or newer).

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.

Assessment:

Ensure 'NoLockScreenSlideshow' is 'Windows: Registry Value' to '1' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Personalization:NoLockScreenSlideshow does not exist

References:

- **CCE-IDv5:** CCE-35800-2 -- More

Back to Summary

18.1.2 Regional and Language Options

This section contains recommendation settings for Regional and Language Options.

This Group Policy section is provided by the Group Policy template `Globalization.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.1.2.1 Handwriting personalization

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

This Group Policy section is provided by the Group Policy template `Globalization.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.1.2.2 (L1) Ensure 'Allow input personalization' is set to 'Disabled'

Fail

Description:

This policy enables the automatic learning component of input personalization that includes speech, inking, and typing. Automatic learning enables the collection of speech and handwriting patterns, typing history, contacts, and recent calendar information. It is required for the use of Cortana. Some of this collected information may be stored on the user's OneDrive, in the case of inking and typing; some of the information will be uploaded to Microsoft to personalize speech.

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

Rationale:

If this setting is Enabled sensitive information could be stored in the cloud or sent to Microsoft.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Control Panel\Regional and Language
Options\Allow input personalization
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `Globalization.admx/adml` that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

Impact:

Automatic learning of speech, inking, and typing stops and users cannot change its value via PC Settings.

Assessment:

Ensure 'AllowInputPersonalization' is 'Windows: Registry Value' to '0' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\InputPersonalization:AllowInputPersonalization          does not exist
```

References:

- **CCE-IDv5:** CCE-41387-2 -- More

CIS Controls V6.1:

- **Control 13: Data Protection:** -- More

Back to Summary

18.2 LAPS

This section contains recommendations for configuring Microsoft Local Administrator Password Solution (LAPS).

This Group Policy section is provided by the Group Policy template `AdmPwd.admx/adml` that is included with LAPS.

18.2.1 (L1) Ensure LAPS AdmPwd GPO Extension / CSE is installed

Fail

Description:

In May 2015, Microsoft released the Local Administrator Password Solution (LAPS) tool, which is free and supported software that allows an organization to automatically set randomized and unique local Administrator account passwords on domain-attached workstations and Member Servers. The passwords are stored in a confidential attribute of the domain computer account and can be retrieved from Active Directory by approved Sysadmins when needed.

The LAPS tool requires a small Active Directory Schema update in order to implement, as well as installation of a Group Policy Client Side Extension (CSE) on targeted computers. Please see the LAPS documentation for details.

LAPS supports Windows Vista or newer workstation OSes, and Server 2003 or newer server OSes. LAPS does not support standalone computers - they must be joined to a domain.

Note: Organizations that utilize 3rd-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations.

Note #2: LAPS is only designed to manage *local* Administrator passwords, and is therefore not recommended (or supported) for use directly on Domain Controllers, which do not have a traditional local Administrator account. We strongly encourage you to only deploy the LAPS CSE and LAPS GPO settings to member servers and workstations.

Rationale:

Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or Member Servers when deploying them. This creates a serious attack surface security risk because if an attacker manages to compromise one system and learn the password to its local Administrator account, then they can leverage that account to instantly gain access to all other computers that also use that password for their local Administrator account.

Remediation:

In order to utilize LAPS, a minor Active Directory Schema update is required, and a Group Policy Client Side Extension (CSE) must be installed on each managed computer. When LAPS is installed, the file `AdmPwd.dll` must be present in the following location and registered in Windows (the LAPS AdmPwd GPO Extension / CSE installation does this for you):

```
C:\Program Files\LAPS\CSE\AdmPwd.dll
```

Impact:

No impact. When installed and registered properly, `AdmPwd.dll` takes no action unless given appropriate GPO commands during Group Policy refresh. It is not a memory-resident agent or service.

In a disaster recovery scenario where Active Directory is not available, the local Administrator password will not be retrievable and a local password reset using a tool (such as Microsoft's Disaster and Recovery Toolset (DaRT) Recovery Image) may be necessary.

Assessment:

Any of the following tests or sub-groups may pass:

Ensure 'DllName' is 'Windows: Registry Value' to 'C:\Program Files\LAPS\CSE\AdmPwd.dll' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions \{D76B9641-3288-4f75-942D-087DE603E3EA}:DllName	does not exist

Ensure 'DllName' is 'Windows: Registry Value' to 'C:\Program Files\LAPS\CSE\AdmPwd.dll' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions \{D76B9641-3288-4f75-942D-087DE603E3EA}:DllName	does not exist

References:

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

18.2.2 (L1) Ensure 'Do not allow password expiration time longer than required by policy' is set to 'Enabled'

Fail

Description:

In May 2015, Microsoft released the Local Administrator Password Solution (LAPS) tool, which is free and supported software that allows an organization to automatically set randomized and unique local Administrator account passwords on domain-attached workstations and Member Servers. The passwords are stored in a confidential attribute of the domain computer account and can be retrieved from Active Directory by approved Sysadmins when needed.

The LAPS tool requires a small Active Directory Schema update in order to implement, as well as installation of a Group Policy Client Side Extension (CSE) on targeted computers. Please see the LAPS documentation for details.

LAPS supports Windows Vista or newer workstation OSes, and Server 2003 or newer server OSes. LAPS does not support standalone computers - they must be joined to a domain.

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

Note: Organizations that utilize 3rd-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations.

Note #2: LAPS is only designed to manage *local* Administrator passwords, and is therefore not recommended (or supported) for use directly on Domain Controllers, which do not have a traditional local Administrator account. We strongly encourage you to only deploy the LAPS CSE and LAPS GPO settings to member servers and workstations.

Rationale:

Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or Member Servers when deploying them. This creates a serious attack surface security risk because if an attacker manages to compromise one system and learn the password to its local Administrator account, then they can leverage that account to instantly gain access to all other computers that also use that password for their local Administrator account.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\LAPS\Do not allow password expiration time
longer than required by policy
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`AdmPwd.admx/adml`) is required - it is included with Microsoft Local Administrator Password Solution (LAPS).

Impact:

Planned password expiration longer than password age dictated by "Password Settings" policy is NOT allowed.

Assessment:

Ensure 'PwdExpirationProtectionEnabled' is 'Windows: Registry Value' to '1' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft Services\AdmPwd:PwdExpirationProtectionEnabled        does not exist
```

References:

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

18.2.3 (L1) Ensure 'Enable Local Admin Password Management' is set to 'Enabled'

Fail

Description:

In May 2015, Microsoft released the Local Administrator Password Solution (LAPS) tool, which is free and supported software that allows an organization to automatically set randomized and unique local Administrator account passwords on domain-attached workstations and Member Servers. The passwords are stored in a confidential attribute of the domain computer account and can be retrieved from Active Directory by approved Sysadmins when needed.

The LAPS tool requires a small Active Directory Schema update in order to implement, as well as installation of a

Group Policy Client Side Extension (CSE) on targeted computers. Please see the LAPS documentation for details.

LAPS supports Windows Vista or newer workstation OSes, and Server 2003 or newer server OSes. LAPS does not support standalone computers - they must be joined to a domain.

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

Note: Organizations that utilize 3rd-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations.

Note #2: LAPS is only designed to manage *local* Administrator passwords, and is therefore not recommended (or supported) for use directly on Domain Controllers, which do not have a traditional local Administrator account. We strongly encourage you to only deploy the LAPS CSE and LAPS GPO settings to member servers and workstations.

Rationale:

Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or Member Servers when deploying them. This creates a serious attack surface security risk because if an attacker manages to compromise one system and learn the password to its local Administrator account, then they can leverage that account to instantly gain access to all other computers that also use that password for their local Administrator account.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\LAPS\Enable Local Admin Password Management
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`AdmPwd.admx/adml`) is required - it is included with Microsoft Local Administrator Password Solution (LAPS).

Impact:

The local administrator password is managed (provided that the LAPS AdmPwd GPO Extension / CSE is installed on the target computer (see Rule 18.2.1), the Active Directory domain schema and account permissions have been properly configured on the domain).

In a disaster recovery scenario where Active Directory is not available, the local Administrator password will not be retrievable and a local password reset using a tool (such as Microsoft's Disaster and Recovery Toolset (DaRT) Recovery Image) may be necessary.

Assessment:

Ensure 'AdmPwdEnabled' is 'Windows: Registry Value' to '1' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft Services\AdmPwd:AdmPwdEnabled                does not exist
```

References:

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

18.2.4 (L1) Ensure 'Password Settings: Password Complexity' is set to 'Enabled: Large letters + small letters + numbers + special characters'

Fail

Description:

In May 2015, Microsoft released the Local Administrator Password Solution (LAPS) tool, which is free and supported software that allows an organization to automatically set randomized and unique local Administrator account passwords on domain-attached workstations and Member Servers. The passwords are stored in a confidential attribute of the domain computer account and can be retrieved from Active Directory by approved Sysadmins when needed.

The LAPS tool requires a small Active Directory Schema update in order to implement, as well as installation of a Group Policy Client Side Extension (CSE) on targeted computers. Please see the LAPS documentation for details.

LAPS supports Windows Vista or newer workstation OSes, and Server 2003 or newer server OSes. LAPS does not support standalone computers - they must be joined to a domain.

The recommended state for this setting is: `Enabled: Large letters + small letters + numbers + special characters`.

Note: Organizations that utilize 3rd-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations.

Note #2: LAPS is only designed to manage *local* Administrator passwords, and is therefore not recommended (or supported) for use directly on Domain Controllers, which do not have a traditional local Administrator account. We strongly encourage you to only deploy the LAPS CSE and LAPS GPO settings to member servers and workstations.

Rationale:

Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or Member Servers when deploying them. This creates a serious attack surface security risk because if an attacker manages to compromise one system and learn the password to its local Administrator account, then they can leverage that account to instantly gain access to all other computers that also use that password for their local Administrator account.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`, and configure the `Password Complexity` option to `Large letters + small letters + numbers + special characters`:

```
Computer Configuration\Policies\Administrative Templates\LAPS\Password Settings
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`AdmPwd.admx/adml`) is required - it is included with Microsoft Local Administrator Password Solution (LAPS).

Impact:

LAPS-generated passwords will be required to contain large letters + small letters + numbers + special characters.

Assessment:

Ensure 'PasswordComplexity' is 'Windows: Registry Value' to '4' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft Services\AdmPwd:PasswordComplexity          does not exist
```

References:

CIS Controls V6.1:

- Control 5: Controlled Use of Administrative Privileges: -- More

Back to Summary

18.2.5 (L1) Ensure 'Password Settings: Password Length' is set to 'Enabled: 15 or more'

Fail

Description:

In May 2015, Microsoft released the Local Administrator Password Solution (LAPS) tool, which is free and supported software that allows an organization to automatically set randomized and unique local Administrator account passwords on domain-attached workstations and Member Servers. The passwords are stored in a confidential attribute of the domain computer account and can be retrieved from Active Directory by approved Sysadmins when needed.

The LAPS tool requires a small Active Directory Schema update in order to implement, as well as installation of a Group Policy Client Side Extension (CSE) on targeted computers. Please see the LAPS documentation for details.

LAPS supports Windows Vista or newer workstation OSes, and Server 2003 or newer server OSes. LAPS does not support standalone computers - they must be joined to a domain.

The recommended state for this setting is: `Enabled: 15 or more`.

Note: Organizations that utilize 3rd-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations.

Note #2: LAPS is only designed to manage *local* Administrator passwords, and is therefore not recommended (or supported) for use directly on Domain Controllers, which do not have a traditional local Administrator account. We strongly encourage you to only deploy the LAPS CSE and LAPS GPO settings to member servers and workstations.

Rationale:

Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or Member Servers when deploying them. This creates a serious attack surface security risk because if an attacker manages to compromise one system and learn the password to its local Administrator account, then they can leverage that account to instantly gain access to all other computers that also use that password for their local Administrator account.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`, and configure the `Password Length` option to `15 or more`:

```
Computer Configuration\Policies\Administrative Templates\LAPS\Password Settings
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`AdmPwd.admx/adml`) is required - it is included with Microsoft Local Administrator Password Solution (LAPS).

Impact:

LAPS-generated passwords will be required to have a length of 15 characters (or more, if selected).

Assessment:

Ensure 'PasswordLength' is 'Windows: Registry Value' to '15' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft Services\AdmPwd:PasswordLength          does not exist
```

References:

CIS Controls V6.1:

- **Control 5: Controlled Use of Administrative Privileges:** -- More

Back to Summary

18.2.6 (L1) Ensure 'Password Settings: Password Age (Days)' is set to 'Enabled: 30 or fewer'

Fail

Description:

In May 2015, Microsoft released the Local Administrator Password Solution (LAPS) tool, which is free and supported software that allows an organization to automatically set randomized and unique local Administrator account passwords on domain-attached workstations and Member Servers. The passwords are stored in a confidential attribute of the domain computer account and can be retrieved from Active Directory by approved Sysadmins when needed.

The LAPS tool requires a small Active Directory Schema update in order to implement, as well as installation of a Group Policy Client Side Extension (CSE) on targeted computers. Please see the LAPS documentation for details.

LAPS supports Windows Vista or newer workstation OSes, and Server 2003 or newer server OSes. LAPS does not support standalone computers - they must be joined to a domain.

The recommended state for this setting is: `Enabled: 30 or fewer`.

Note: Organizations that utilize 3rd-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations.

Note #2: LAPS is only designed to manage *local* Administrator passwords, and is therefore not recommended (or supported) for use directly on Domain Controllers, which do not have a traditional local Administrator account. We strongly encourage you to only deploy the LAPS CSE and LAPS GPO settings to member servers and workstations.

Rationale:

Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or Member Servers when deploying them. This creates a serious attack surface security risk because if an attacker manages to compromise one system and learn the password to its local Administrator account, then they can leverage that account to instantly gain access to all other computers that also use that password for their local Administrator account.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`, and configure the `Password Age (Days)` option to `30 or fewer`:

```
Computer Configuration\Policies\Administrative Templates\LAPS\Password Settings
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`AdmPwd.admx/adml`) is required - it is included with Microsoft Local Administrator Password Solution (LAPS).

Impact:

LAPS-generated passwords will be required to have a maximum age of 30 days (or fewer, if selected).

Assessment:

Ensure 'PasswordAgeDays' is 'Windows: Registry Value' to '30' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft Services\AdmPwd:PasswordAgeDays does not exist

References:

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

18.3 MS Security Guide

This section contains settings for configuring additional settings from the MS Security Guide.

This Group Policy section is provided by the Group Policy template `SecGuide.admx/adml` that is available from Microsoft at this link.

18.3.1 (L1) Ensure 'Apply UAC restrictions to local accounts on network logons' is set to 'Enabled'

Fail

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.

Remediation:

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

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

Note: This Group Policy path does not exist by default. An additional Group Policy template (`SecGuide.admx/adml`) is required - it is available from Microsoft at this link.

Impact:

None - this is the default behavior.

Assessment:

Ensure 'LocalAccountTokenFilterPolicy' is 'Windows: Registry Value' to '0' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System:LocalAccountTokenFilterPolicy does not exist

References:

- **CCE-IDv5:** CCE-35486-0 -- More

CIS Controls V7.0:

- **Control 4: Controlled Use of Administrative Privileges:** -- More

CIS Controls V6.1:

- **Control 5: Controlled Use of Administrative Privileges:** -- More

Back to Summary

18.3.2 (L1) Ensure 'Configure SMB v1 client driver' is set to 'Enabled: Disable driver'

Fail

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`.

Note: Do not, *under any circumstances*, configure this overall setting as `Disabled`, as doing so will delete the underlying registry entry altogether, which will cause serious problems.

Rationale:

Since September 2016, Microsoft has strongly encouraged that SMBv1 be disabled and no longer used on modern networks, as it is a 30 year old design that is much more vulnerable to attacks then much newer designs such as SMBv2 and SMBv3.

More information on this can be found at the following links:

Stop using SMB1 | Storage at Microsoft

Disable SMB v1 in Managed Environments with Group Policy – "Stay Safe" Cyber Security Blog

Disabling SMBv1 through Group Policy – Microsoft Security Guidance blog

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\MS Security Guide\Configure SMB v1 client
driver
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`SecGuide.admx/adml`) is required - it is available from Microsoft at this link.

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

Assessment:

Ensure 'Start' is 'Windows: Registry Value' to '4' -- Less

Check:	All Must Pass
Registry Key:	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\mrxsmb10
Registry Value:	Start

CIS-CAT Expected...	CIS-CAT Collected...
the registry key's *type* to be set to **reg_dword**	reg_dword
the registry key's *value* to be set to **4**	2

References:

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

CIS Controls V6.1:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

Back to Summary

18.3.3 (L1) Ensure 'Configure SMB v1 server' is set to 'Disabled'

Fail

Description:

This setting configures the server-side processing of the Server Message Block version 1 (SMBv1) protocol.

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

Rationale:

Since September 2016, Microsoft has strongly encouraged that SMBv1 be disabled and no longer used on modern networks, as it is a 30 year old design that is much more vulnerable to attacks then much newer designs such as SMBv2 and SMBv3.

More information on this can be found at the following links:

Stop using SMB1 | Storage at Microsoft

Disable SMB v1 in Managed Environments with Group Policy – "Stay Safe" Cyber Security Blog

Disabling SMBv1 through Group Policy – Microsoft Security Guidance blog

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\MS Security Guide\Configure SMB v1 server
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`SecGuide.admx/adml`) is required - it is available from Microsoft at this link.

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

Assessment:

Ensure 'SMB1' is 'Windows: Registry Value' to '0' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters:SMB1          does not exist
```

References:

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

CIS Controls V6.1:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

Back to Summary

18.3.4 (L1) Ensure 'Enable Structured Exception Handling Overwrite Protection (SEHOP)' is set to 'Enabled'

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\MS Security Guide\Enable Structured Exception
Handling Overwrite Protection (SEHOP)
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`SecGuide.admx/adml`) is required - it is available from Microsoft at this link.

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

Impact:

After you enable SEHOP, existing versions of Cygwin, Skype, and Armadillo-protected applications may not work correctly.

Assessment:

Ensure 'DisableExceptionChainValidation' is 'Windows: Registry Value' to '0' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\kernel:DisableExceptionChainValidation          does not exist
```

References:

CIS Controls V7.0:

- **Control 8: Malware Defenses:** -- More

CIS Controls V6.1:

- **Control 8: Malware Defenses:** -- More

Back to Summary

18.3.5 (L1) Ensure 'Turn on Windows Defender protection against Potentially Unwanted Applications' is set to 'Enabled'

Fail

Description:

Enabling this Windows Defender feature will protect against Potentially Unwanted Applications (PUA), which are sneaky unwanted application bundlers or their bundled applications to deliver adware or malware.

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

For more information, see this link: Block Potentially Unwanted Applications with Windows Defender AV | Microsoft Docs

Rationale:

This opt-in feature is free and could prevent malicious software from being installed.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\MS Security Guide\Turn on Windows Defender
protection against Potentially Unwanted Applications
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`SecGuide.admx/adml`) is required - it is available from Microsoft at this link.

Impact:

Applications that are identified by Microsoft as PUA will be blocked at download and install time.

Assessment:

Ensure 'MpEnablePus' is 'Windows: Registry Value' to '1' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\MpEngine:MpEnablePus          does not exist
```

References:

CIS Controls V7.0:

- **Control 8: Malware Defenses:** -- More

CIS Controls V6.1:

- **Control 8: Malware Defenses:** -- More

Back to Summary

18.3.6 (L1) Ensure 'WDigest Authentication' is set to 'Disabled'

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\MS Security Guide\WDigest Authentication
(disabling may require KB2871997)
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`SecGuide.admx/adml`) is required - it is available from Microsoft at this link.

Impact:

None - this is also the default configuration for Windows 8.1 and newer.

Assessment:

Ensure 'UseLogonCredential' is 'Windows: Registry Value' to '0' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest:UseLogonCredential          does not exist
```

References:

- **CCE-IDv5:** CCE-35815-0 -- More

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

18.4 MSS (Legacy)

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

This Group Policy section is provided by the Group Policy template `MSS-legacy.admx/adml` that is available from this TechNet blog post: The MSS settings – Microsoft Security Guidance blog

18.4.1 (L1) Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled'

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (AutoAdminLogon) Enable
Automatic Logon (not recommended)
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`MSS-legacy.admx/adml`) is required - it is available from this TechNet blog post: The MSS settings – Microsoft Security Guidance blog

Impact:

None - this is the default behavior.

Assessment:

All of the following tests or sub-groups must pass:

Ensure 'DefaultPassword' does not exist -- More

Ensure 'AutoAdminLogon' is 'Windows: Registry Value' to '0' -- Less

Check:	All Must Pass
Registry Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
Registry Value:	AutoAdminLogon

CIS-CAT Expected...	CIS-CAT Collected...
the registry key's *type* to be set to **reg_sz**	reg_sz
the registry key's *value* to be set to **0**	1

References:

- **CCE-IDv5:** CCE-35438-1 -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

18.4.2 (L1) Ensure 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled'

Fail

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.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Highest protection, source routing is completely disabled`:

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

Note: This Group Policy path does not exist by default. An additional Group Policy template (`MSS-legacy.admx/adml`) is required - it is available from this TechNet blog post: The MSS settings – Microsoft Security Guidance blog

Impact:

All incoming source routed packets will be dropped.

Assessment:

Ensure 'DisableIPSourceRouting' is 'Windows: Registry Value' to '2' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip6\Parameters:DisableIPSourceRouting          does not exist
```

References:

- **CCE-IDv5:** CCE-33790-7 -- More

CIS Controls V6.1:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

Back to Summary

18.4.3 (L1) Ensure 'MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled'

Fail

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.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Highest protection, source routing is completely disabled`:

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

Note: This Group Policy path does not exist by default. An additional Group Policy template (`MSS-legacy.admx/adml`) is required - it is available from this TechNet blog post: The MSS settings – Microsoft Security Guidance blog

Impact:

All incoming source routed packets will be dropped.

Assessment:

Ensure 'DisableIPSourceRouting' is 'Windows: Registry Value' to '2' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters:DisableIPSourceRouting          does not exist
```

References:

- **CCE-IDv5:** CCE-33816-0 -- More

CIS Controls V6.1:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

Back to Summary

18.4.5 (L1) Ensure 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' is set to 'Disabled'

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (EnableICMPRedirect) Allow
ICMP redirects to override OSPF generated routes
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`MSS-legacy.admx/adml`) is required - it is available from this TechNet blog post: The MSS settings – Microsoft Security Guidance blog

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.

Assessment:

Ensure 'EnableICMPRedirect' is 'Windows: Registry Value' to '0' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters:EnableICMPRedirect does not exist

References:

- **CCE-IDv5:** CCE-34597-5 -- More

CIS Controls V6.1:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

Back to Summary

18.4.7 (L1) Ensure 'MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers' is set to 'Enabled'

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (NoNameReleaseOnDemand) Allow
the computer to ignore NetBIOS name release requests except from WINS servers
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`MSS-legacy.admx/adml`) is required - it is available from this TechNet blog post: The MSS settings – Microsoft Security Guidance blog

Impact:

None - this is the default behavior.

Assessment:

Ensure 'nonamereleaseondemand' is 'Windows: Registry Value' to '1' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NetBT\Parameters:nonamereleaseondemand          does not exist
```

References:

- **CCE-IDv5:** CCE-35405-0 -- More

CIS Controls V6.1:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

Back to Summary

18.4.9 (L1) Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' is set to 'Enabled'

Fail

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`.

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.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (SafeDllSearchMode) Enable
Safe DLL search mode (recommended)
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`MSS-legacy.admx/adml`) is required - it is available from this TechNet blog post: The MSS settings – Microsoft Security Guidance blog

Impact:

None - this is the default behavior.

Assessment:

Ensure 'SafeDllSearchMode' is 'Windows: Registry Value' to '1' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager:SafeDllSearchMode          does not exist
```

References:

- **CCE-IDv5:** CCE-34022-4 -- More

CIS Controls V6.1:

- **Control 8: Malware Defenses:** -- More

Back to Summary

18.4.10 (L1) Ensure 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)' is set to 'Enabled: 5 or fewer seconds'

Fail

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.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: 5 or fewer seconds`:

```
Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (ScreenSaverGracePeriod) The
time in seconds before the screen saver grace period expires (0 recommended)
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`MSS-legacy.admx/adml`) is required - it is available from this TechNet blog post: The MSS settings – Microsoft Security Guidance blog

Impact:

Users will have to enter their passwords to resume their console sessions as soon as the grace period ends after screen saver activation.

Assessment:

Ensure 'ScreenSaverGracePeriod' is 'Windows: Registry Value' to '5' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon:ScreenSaverGracePeriod          does not exist
```

References:

- **CCE-IDv5:** CCE-34619-7 -- More

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

18.4.13 (L1) Ensure 'MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning' is set to 'Enabled: 90% or less'

Fail

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.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: 90% or less`:

```
Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (WarningLevel) Percentage
threshold for the security event log at which the system will generate a warning
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`MSS-legacy.admx/adml`) is required - it is available from this TechNet blog post: The MSS settings – Microsoft Security Guidance blog

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.

Assessment:

Ensure 'WarningLevel' is 'Windows: Registry Value' to '90' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Security:WarningLevel            does not exist
```

References:

- **CCE-IDv5:** CCE-35406-8 -- More

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More

CIS Controls V6.1:

- **Control 6: Maintenance, Monitoring, and Analysis of Audit Logs:** -- More

Back to Summary

18.5 Network

This section contains recommendations for network settings.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.5.1 Background Intelligent Transfer Service (BITS)

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

This Group Policy section is provided by the Group Policy template `Bits.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.5.2 BranchCache

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

This Group Policy section is provided by the Group Policy template `PeerToPeerCaching.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.5.3 DirectAccess Client Experience Settings

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

This Group Policy section is provided by the Group Policy template `nca.admx/adml` that is included with the Microsoft 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.5.4 DNS Client

This section contains recommendations related to DNS Client.

This Group Policy section is provided by the Group Policy template `DnsClient.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.5.4.1 (L1) Set 'NetBIOS node type' to 'P-node' (Ensure NetBT Parameter 'NodeType' is set to '0x2 (2)')

Fail

Description:

This parameter determines which method NetBIOS over TCP/IP (NetBT) will use to register and resolve names.

- A B-node (broadcast) system only uses broadcasts.
- A P-node (point-to-point) system uses only name queries to a name server (WINS).
- An M-node (mixed) system broadcasts first, then queries the name server (WINS).
- An H-node (hybrid) system queries the name server (WINS) first, then broadcasts.

The recommended state for this setting is: `NodeType - 0x2 (2)` (P-node / point-to-point).

Rationale:

In order to help mitigate the risk of NetBIOS Name Service (NBT-NS) poisoning attacks, setting the node type to P-node will prevent the system from sending out NetBIOS broadcasts.

Remediation:

To establish the recommended configuration, set the following Registry value to `0x2 (2) (DWORD)`:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NetBT\Parameters:NodeType
```

Note: This change does not take effect until the computer has been restarted.

Note #2: Although Microsoft does not provide an ADMX template to configure this registry value, a custom .ADM template (`Set-NetBIOS-node-type-KB160177.adm`) is provided in the CIS Benchmark Remediation Kit to facilitate its configuration. Be aware though that simply turning off the group policy setting in the .ADM template will not "undo" the change once applied. Instead, the opposite setting must be applied to change the registry value to the opposite state.

Impact:

NetBIOS name resolution queries will require a defined and available WINS server for external NetBIOS name resolution. If a WINS server is not defined or not reachable, and the desired hostname is not defined in the local cache, local LMHOSTS or HOSTS files, NetBIOS name resolution will fail.

Assessment:

Ensure 'NodeType' is 'Windows: Registry Value' to '2' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Netbt\Parameters:NodeType does not exist

References:

CIS Controls V6.1:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

Back to Summary

18.5.4.2 (L1) Ensure 'Turn off multicast name resolution' is set to 'Enabled'

Pass

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.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Network\DNS Client\Turn off multicast name
resolution
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `DnsClient.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Impact:

In the event DNS is unavailable a system will be unable to request it from other systems on the same subnet.

Assessment:

Ensure 'EnableMulticast' is 'Windows: Registry Value' to '0' -- More

References:

- **CCE-IDv5:** CCE-34055-4 -- More

CIS Controls V6.1:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

Back to Summary

18.5.5 Fonts

This section contains recommendations related to Fonts.

This Group Policy section is provided by the Group Policy template `GroupPolicy.admx/adml` that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

18.5.6 Hotspot Authentication

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

This Group Policy section is provided by the Group Policy template `hotspotauth.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.5.7 Lanman Server

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

This Group Policy section is provided by the Group Policy template `LanmanServer.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.5.8 Lanman Workstation

This section contains recommendations related to Lanman Workstation.

This Group Policy section is provided by the Group Policy template `LanmanWorkstation.admx/adml` that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

18.5.8.1 (L1) Ensure 'Enable insecure guest logons' is set to 'Disabled'

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Network\Lanman Workstation\Enable insecure
guest logons
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `LanmanWorkstation.admx/adml` that is included with the Microsoft Windows 10 Release 1511 Administrative Templates (or newer).

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]

Assessment:

Ensure 'AllowInsecureGuestAuth' is 'Windows: Registry Value' to '0' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\LanmanWorkstation:AllowInsecureGuestAuth          does not exist
```

References:

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

CIS Controls V6.1:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

Back to Summary

18.5.9 Link-Layer Topology Discovery

This section contains recommendations for Link-Layer Topology Discovery settings.

This Group Policy section is provided by the Group Policy template `LinkLayerTopologyDiscovery.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.5.10 Microsoft Peer-to-Peer Networking Services

This section contains recommendations for Microsoft Peer-to-Peer Networking Services settings.

This Group Policy section is provided by the Group Policy template `P2P-pnrp.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.5.10.1 Peer Name Resolution Protocol

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

This Group Policy section is provided by the Group Policy template `P2P-pnrp.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.5.11 Network Connections

This section contains recommendations for Network Connections settings.

This Group Policy section is provided by the Group Policy template `NetworkConnections.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.5.11.1 Windows Defender Firewall (formerly Windows Firewall)

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

This Group Policy section is provided by the Group Policy template `WindowsFirewall.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note: This section was initially named *Windows Firewall* but was renamed by Microsoft to *Windows Defender Firewall* starting with the Microsoft Windows 10 Release 1709 Administrative Templates.

18.5.11.2 (L1) Ensure 'Prohibit installation and configuration of Network Bridge on your DNS domain network' is set to 'Enabled'

Fail

Description:

You can use this procedure to controls 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.

Remediation:

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

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

Note: This Group Policy path is provided by the Group Policy template `NetworkConnections.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Impact:

Users cannot create or configure a Network Bridge.

Assessment:

Ensure 'NC_AllowNetBridge_NLA' is equal to '0' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Network Connections:NC_AllowNetBridge_NLA          does not exist
```

References:

- **CCE-IDv5:** CCE-33107-4 -- More

CIS Controls V6.1:

- **Control 5: Controlled Use of Administrative Privileges:** -- More

Back to Summary

18.5.11.3 (L1) Ensure 'Prohibit use of Internet Connection Sharing on your DNS domain network' is set to 'Enabled'

Fail

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.

Remediation:

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

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

Note: This Group Policy path is provided by the Group Policy template `NetworkConnections.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Impact:

Mobile Hotspot cannot be enabled or configured by Administrators and non-Administrators alike.

Assessment:

Ensure 'NC_ShowSharedAccessUI' is 'Windows: Registry Value' to '0' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Network Connections:NC_ShowSharedAccessUI does not exist

References:

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

CIS Controls V6.1:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

Back to Summary

18.5.11.4 (L1) Ensure 'Require domain users to elevate when setting a network's location' is set to 'Enabled'

Fail

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.

Remediation:

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

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

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `NetworkConnections.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Impact:

Domain users must elevate when setting a network's location.

Assessment:

Ensure 'NC_StdDomainUserSetLocation' is 'Windows: Registry Value' to '1' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Network Connections:NC_StdDomainUserSetLocation does not exist

References:

- **CCE-IDv5:** CCE-35554-5 -- More

CIS Controls V6.1:

- **Control 5: Controlled Use of Administrative Privileges:** -- More

Back to Summary

18.5.12 Network Connectivity Status Indicator

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

This Group Policy section is provided by the Group Policy template `NCSI.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.5.13 Network Isolation

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

This Group Policy section is provided by the Group Policy template `NetworkIsolation.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.5.14 Network Provider

This section contains recommendations for Network Provider settings.

This Group Policy section is provided by the Group Policy template `NetworkProvider.admx/adml` that is included with the MS15-011 / MSKB 3000483 security update and the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

18.5.14.1 (L1) Ensure 'Hardened UNC Paths' is set to 'Enabled, with "Require Mutual Authentication" and "Require Integrity" set for all NETLOGON and SYSVOL shares'

Fail

Description:

This policy setting configures secure access to UNC paths.

The recommended state for this setting is: `Enabled, with "Require Mutual Authentication" and "Require Integrity" set for all NETLOGON and SYSVOL shares.`

Note: If the environment exclusively contains Windows 8.0 / Server 2012 (non-R2) or newer systems, then the "`Privacy`" setting may (optionally) also be set to enable SMB encryption. However, using SMB encryption will render the targeted share paths completely inaccessible by older OSes, so only use this additional option with caution and thorough testing.

Rationale:

In February 2015, Microsoft released a new control mechanism to mitigate a security risk in Group Policy as part of the MS15-011 / MSKB 3000483 security update. This mechanism requires both the installation of the new security update and also the deployment of specific group policy settings to all computers on the domain from Windows Vista / Server 2008 (non-R2) or newer (the associated security patch to enable this feature was not released for Server 2003). A new group policy template (`NetworkProvider.admx/adml`) was also provided with the security update.

Once the new GPO template is in place, the following are the minimum requirements to remediate the Group Policy security risk:

```
\\*\NETLOGON RequireMutualAuthentication=1, RequireIntegrity=1
```

```
\\*\SYSVOL RequireMutualAuthentication=1, RequireIntegrity=1
```

Note: A reboot may be required after the setting is applied to a client machine to access the above paths.

Additional guidance on the deployment of this security setting is available from the Microsoft Premier Field Engineering (PFE) Platforms TechNet Blog here: Guidance on Deployment of MS15-011 and MS15-014.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled` with the following paths configured, at a minimum:

```
\\*\NETLOGON RequireMutualAuthentication=1, RequireIntegrity=1 \\*\SYSVOL
RequireMutualAuthentication=1, RequireIntegrity=1
```

```
Computer Configuration\Policies\Administrative Templates\Network\Network Provider\Hardened UNC Paths
```

Note: This Group Policy path does not exist by default. An additional Group Policy template (`NetworkProvider.admx/adml`) is required - it is included with the MS15-011 / MSKB 3000483 security update or with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

Impact:

Windows only allows access to the specified UNC paths after fulfilling additional security requirements.

Assessment:

All of the following tests or sub-groups must pass:

Ensure '\\*\NETLOGON' is 'Windows: Registry Value' to '[Rr]equire([Mm]utual[Aa]uthentication|[Ii]ntegrity)=1.*[Rr]equire([Mm]utual[Aa]uthentication|[Ii]ntegrity)=1' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths:\\*\NETLOGON does not exist

Ensure '\\*\SYSVOL' is 'Windows: Registry Value' to '[Rr]equire([Mm]utual[Aa]uthentication|[Ii]ntegrity)=1.*[Rr]equire([Mm]utual[Aa]uthentication|[Ii]ntegrity)=1' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths:\\*\SYSVOL does not exist

References:

CIS Controls V6.1:

- **Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers:** -- More

Back to Summary

18.5.15 Offline Files

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

This Group Policy section is provided by the Group Policy template `OfflineFiles.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.5.16 QoS Packet Scheduler

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

This Group Policy section is provided by the Group Policy template `QOS.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.5.17 SNMP

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

This Group Policy section is provided by the Group Policy template `Snmp.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.5.18 SSL Configuration Settings

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

This Group Policy section is provided by the Group Policy template `CipherSuiteOrder.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.5.19 TCPIP Settings

This section contains TCP/IP configuration settings.

This Group Policy section is provided by the Group Policy template `tcpip.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.5.19.1 IPv6 Transition Technologies

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

This Group Policy section is provided by the Group Policy template `tcpip.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.5.19.2 Parameters

This section contains TCP/IP parameter configuration settings.

This Group Policy section is provided by the Group Policy template `tcpip.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.5.20 Windows Connect Now

This section contains recommendations for Windows Connect Now settings.

This Group Policy section is provided by the Group Policy template `WindowsConnectNow.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.5.21 Windows Connection Manager

This section contains recommendations for Windows Connection Manager settings.

This Group Policy section is provided by the Group Policy template `WCM.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.5.21.1 (L1) Ensure 'Minimize the number of simultaneous connections to the Internet or a Windows Domain' is set to 'Enabled'

Fail

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`.

Rationale:

Blocking simultaneous connections can help prevent a user unknowingly allowing network traffic to flow between the Internet and the enterprise managed network.

Remediation:

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

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

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WCM.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Impact:

None - this is the default behavior.

Assessment:

Ensure 'fMinimizeConnections' is 'Windows: Registry Value' to '1' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WcmSvc\GroupPolicy:fMinimizeConnections     does not exist
```

References:

- **CCE-IDv5:** CCE-35242-7 -- More

CIS Controls V6.1:

- **Control 12: Boundary Defense:** -- More

Back to Summary

18.5.21.2 (L1) Ensure 'Prohibit connection to non-domain networks when connected to domain authenticated network' is set to 'Enabled'

Fail

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.

Remediation:

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

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

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WCM.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

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.

Assessment:

Ensure 'fBlockNonDomain' is 'Windows: Registry Value' to '1' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WcmSvc\GroupPolicy:fBlockNonDomain          does not exist
```

References:

- **CCE-IDv5:** CCE-35375-5 -- More

CIS Controls V6.1:

- **Control 12: Boundary Defense:** -- More

Back to Summary

18.5.22 Wireless Display

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

This Group Policy section is provided by the Group Policy template `wlansvc.admx/adml` that is included with the Microsoft Windows 10 Release 1511 Administrative Templates (or newer).

18.5.23 WLAN Service

This section contains recommendations for WLAN Service settings.

This Group Policy section is provided by the Group Policy template `wlansvc.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.5.23.1 WLAN Media Cost

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

This Group Policy section is provided by the Group Policy template `wlansvc.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.5.23.2 WLAN Settings

This setting contains recommendations for WLAN Settings.

This Group Policy section is provided by the Group Policy template `wlansvc.admx/adml` that is included with the Microsoft Windows 10 Release 1511 Administrative Templates (or newer).

18.5.23.2.1 (L1) Ensure 'Allow Windows to automatically connect to suggested open hotspots, to networks shared by contacts, and to hotspots offering paid services' is set to 'Disabled'

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Network\WLAN Service\WLAN Settings\Allow
Windows to automatically connect to suggested open hotspots, to networks shared by contacts, and to
hotspots offering paid services
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `wlansvc.admx/adml` that is included with the Microsoft Windows 10 Release 1511 Administrative Templates (or newer).

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.

Assessment:

Ensure 'AutoConnectAllowedOEM' is 'Windows: Registry Value' to '0' -- Less

CIS-CAT expected every collected registry item to exist on the target system, and found 0 items.

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WcmSvc\wifinetworkmanager\config:AutoConnectAllowedOEM does not exist

References:

- **CCE-IDv5:** CCE-41378-1 -- More

CIS Controls V7.0:

- **Control 15: Wireless Access Control:** -- More
- **Control 15: Wireless Access Control:** -- More

CIS Controls V6.1:

- **Control 15: Wireless Access Control:** -- More

Back to Summary

18.6 Printers

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

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.7 Start Menu and Taskbar

This section contains recommendations for Start Menu and Taskbar.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.7.1 Notifications

This section contains recommendations for Start Menu and Taskbar Notifications.

This Group Policy section is provided by the Group Policy template `WPN.admx/adml` that is included with the Microsoft 10 Release 1803 Administrative Templates (or newer).

18.8 System

This section contains recommendations for System settings.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.1 Access-Denied Assistance

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

This Group Policy section is provided by the Group Policy template `srm-fci.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.8.2 App-V

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

This Group Policy section is provided by the Group Policy template `appv.admx/adml` that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

18.8.3 Audit Process Creation

This section contains settings related to auditing of process creation events.

This Group Policy section is provided by the Group Policy template `AuditSettings.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.8.3.1 (L1) Ensure 'Include command line in process creation events' is set to 'Disabled'

Fail

Description:

This policy setting determines what information is logged in security audit events when a new process has been created.

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

Rationale:

When this policy setting is enabled, any user who has read access to the security events can read the command-line arguments for any successfully created process. Command-line arguments may contain sensitive or private information such as passwords or user data.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\System\Audit Process Creation\Include command
line in process creation events
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `AuditSettings.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Impact:

None - this is the default behavior.

Assessment:

Ensure 'ProcessCreationIncludeCmdLine_Enabled' is 'Windows: Registry Value' to '0' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
\Audit:ProcessCreationIncludeCmdLine_Enabled                                          does not exist
```

References:

- **CCE-IDv5:** CCE-35802-8 -- More

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

18.8.4 Credentials Delegation

This section contains settings related to Credential Delegation.

This Group Policy section is provided by the Group Policy template `CredSsp.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.4.1 (L1) Ensure 'Encryption Oracle Remediation' is set to 'Enabled: Force Updated Clients'

Fail

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).

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\System\Credentials Delegation\Encryption Oracle
Remediation
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `CredSsp.admx/adml` that is included with the Microsoft Windows 10 Release 1803 Administrative Templates (or newer).

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.

Assessment:

Ensure 'AllowEncryptionOracle' is 'Windows: Registry Value' to '0' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\CredSSP\Parameters:AllowEncryptionOracle does not exist

References:

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control: --** More

Back to Summary

18.8.4.2 (L1) Ensure 'Remote host allows delegation of non-exportable credentials' is set to 'Enabled'

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\System\Credentials Delegation\Remote host
allows delegation of non-exportable credentials
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `CredSsp.admx/adml` that is included with the Microsoft Windows 10 Release 1703 Administrative Templates (or newer).

Impact:

The host will support the *Restricted Admin Mode* and *Windows Defender Remote Credential Guard* features.

Assessment:

Ensure 'AllowProtectedCreds' is 'Windows: Registry Value' to '1' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CredentialsDelegation:AllowProtectedCreds          does not exist
```

References:

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

18.8.5 Device Guard

This section contains Device Guard settings.

This Group Policy section is provided by the Group Policy template `DeviceGuard.admx/adml` that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

18.8.6 Device Health Attestation Service

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

This Group Policy section is provided by the Group Policy template `TPM.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

18.8.7 Device Installation

This section contains recommendations related to device installation.

This Group Policy section is provided by the Group Policy template `DeviceInstallation.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.7.1 Device Installation Restrictions

This section contains recommendations related to device installation restrictions.

This Group Policy section is provided by the Group Policy template `DeviceInstallation.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.8 Device Redirection

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

This Group Policy section is provided by the Group Policy template `DeviceRedirection.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.8.9 Disk NV Cache

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

This Group Policy section is provided by the Group Policy template `DiskNVCache.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.10 Disk Quotas

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

This Group Policy section is provided by the Group Policy template `DiskQuota.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.11 Display

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

This Group Policy section is provided by the Group Policy template `Display.admx/adml` that is included with the Microsoft Windows 10 Release 1703 Administrative Templates (or newer).

18.8.12 Distributed COM

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

This Group Policy section is provided by the Group Policy template `DCOM.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.13 Driver Installation

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

This Group Policy section is provided by the Group Policy template `DeviceInstallation.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.14 Early Launch Antimalware

This section contains recommendations for configuring boot-start driver initialization settings.

This Group Policy section is provided by the Group Policy template `EarlyLaunchAM.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.8.14.1 (L1) Ensure 'Boot-Start Driver Initialization Policy' is set to 'Enabled: Good, unknown and bad but critical'

Fail

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.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Good, unknown and bad but critical`:

```
Computer Configuration\Policies\Administrative Templates\System\Early Launch Antimalware\Boot-Start
Driver Initialization Policy
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `EarlyLaunchAM.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Impact:

None - this is the default behavior.

Assessment:

Ensure 'DriverLoadPolicy' is 'Windows: Registry Value' to '3' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Policies\EarlyLaunch:DriverLoadPolicy          does not exist
```

References:

- **CCE-IDv5:** CCE-33231-2 -- More

CIS Controls V6.1:

- **Control 8: Malware Defenses:** -- More

Back to Summary

18.8.15 Enhanced Storage Access

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

This Group Policy section is provided by the Group Policy template `EnhancedStorage.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.8.16 File Classification Infrastructure

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

This Group Policy section is provided by the Group Policy template `srm-fci.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.8.17 File Share Shadow Copy Agent

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

This Group Policy section is provided by the Group Policy template `FileServerVSSAgent.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.8.18 File Share Shadow Copy Provider

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

This Group Policy section is provided by the Group Policy templates `FileServerVSSProvider.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.8.19 Filesystem (formerly NTFS Filesystem)

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

This Group Policy section is provided by the Group Policy template `FileSys.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note: This section was initially named *NTFS Filesystem* but was renamed by Microsoft to *Filesystem* starting with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates.

18.8.20 Folder Redirection

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

This Group Policy section is provided by the Group Policy template `FolderRedirection.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.21 Group Policy

This section contains recommendations for configuring group policy-related settings.

This Group Policy section is provided by the Group Policy template `GroupPolicy.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.21.1 Logging and tracing

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

This Group Policy section is provided by the Group Policy template `GroupPolicyPreferences.admx/adml` that is included with the Microsoft Windows Server 2008 (non-R2) Administrative Templates (or newer).

18.8.21.2 (L1) Ensure 'Configure registry policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE'

Fail

Description:

The "Do not apply during periodic background processing" option prevents the system from updating affected policies in the background while the computer is in use. When background updates are disabled, policy changes will not take effect until the next user logon or system restart.

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

Rationale:

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

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`, then set the `Do not apply during periodic background processing` option to `FALSE` (unchecked):

```
Computer Configuration\Policies\Administrative Templates\System\Group Policy\Configure registry policy
processing
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `GroupPolicy.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Impact:

Group Policies will be reapplied every time they are refreshed, which could have a slight impact on performance.

Assessment:

Ensure 'NoBackgroundPolicy' is 'Windows: Registry Value' to '0' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Group Policy\{35378EAC-683F-11D2-
A89A-00C04FBBCFA2}:NoBackgroundPolicy                                          does not exist
```

References:

- **CCE-IDv5:** CCE-35384-7 -- More

CIS Controls V7.0:

- **Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers:** -- More
- **Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers:** -- More

CIS Controls V6.1:

- **Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers:** -- More

Back to Summary

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

Fail

Description:

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

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

Rationale:

Setting this option to true (checked) will ensure unauthorized changes that might have been configured locally are forced to match the domain-based Group Policy settings again.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`, then set the `Process even if the Group Policy objects have not changed` option to `TRUE` (checked):

```
Computer Configuration\Policies\Administrative Templates\System\Group Policy\Configure registry policy
processing
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `GroupPolicy.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Impact:

Group Policies will be reapplied even if they have not been changed, which could have a slight impact on performance.

Assessment:

Ensure 'NoGPOListChanges' is 'Windows: Registry Value' to '0' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Group Policy\{35378EAC-683F-11D2-A89A-00C04FBBCFA2}:NoGPOListChanges does not exist

References:

- **CCE-IDv5:** CCE-35384-7 -- More

CIS Controls V7.0:

- **Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers:** -- More
- **Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers:** -- More

CIS Controls V6.1:

- **Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers:** -- More

Back to Summary

18.8.21.4 (L1) Ensure 'Continue experiences on this device' is set to 'Disabled'

Fail

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.

Remediation:

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

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

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template

`GroupPolicy.admx/adml` that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

Impact:

The Windows device will not be discoverable by other devices, and cannot participate in cross-device experiences.

Assessment:

Ensure 'EnableCdp' is 'Windows: Registry Value' to '0' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System:EnableCdp          does not exist
```

References:

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

CIS Controls V6.1:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

Back to Summary

18.8.21.5 (L1) Ensure 'Turn off background refresh of Group Policy' is set to 'Disabled'

Pass

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.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\System\Group Policy\Turn off background refresh
of Group Policy
```

Note: This Group Policy path is provided by the Group Policy template `GroupPolicy.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Impact:

None - this is the default behavior.

Assessment:

Ensure 'DisableBkGndGroupPolicy' is 'Existence Test' to 'none_exist' -- More

References:

- **CCE-IDv5:** CCE-35776-4 -- More

CIS Controls V7.0:

- **Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers:** -- More
- **Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers:** -- More

CIS Controls V6.1:

- **Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers:** -- More

Back to Summary

18.8.22 Internet Communication Management

This section contains recommendations related to Internet Communication Management.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.22.1 Internet Communication settings

This section contains recommendations related to Internet Communication settings.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.22.1.6 (L1) Ensure 'Turn off Internet download for Web publishing and online ordering wizards' is set to 'Enabled'

Fail

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.

Remediation:

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

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

Note: This Group Policy path is provided by the Group Policy template `ICM.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Impact:

Windows is prevented from downloading providers; only the service providers cached in the local registry are displayed.

Assessment:

Ensure 'NoWebServices' is 'Windows: Registry Value' to '1' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer:NoWebServices        does not exist
```

References:

- **CCE-IDv5:** CCE-33143-9 -- More

CIS Controls V6.1:

- **Control 7: Email and Web Browser Protections:** -- More

Back to Summary

18.8.22.1.7 (L1) Ensure 'Turn off printing over HTTP' is set to 'Enabled'

Fail

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`.

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.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\System\Internet Communication
Management\Internet Communication settings\Turn off printing over HTTP
```

Note: This Group Policy path is provided by the Group Policy template `ICM.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Impact:

The client computer will not be able to print to Internet printers over HTTP.

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.

Assessment:

Ensure 'DisableHTTPPrinting' is 'Windows: Registry Value' to '1' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\Printers:DisableHTTPPrinting          does not exist
```

References:

- **CCE-IDv5:** CCE-33783-2 -- More

CIS Controls V6.1:

- **Control 13: Data Protection:** -- More

Back to Summary

18.8.23 iSCSI

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

This Group Policy section is provided by the Group Policy template `iSCSI.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.24 KDC

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

This Group Policy section is provided by the Group Policy template `KDC.admx/adml` that is included with the Microsoft Windows Server 2008 (non-R2) Administrative Templates (or newer).

18.8.25 Kerberos

This section contains recommendations for Kerberos settings.

This Group Policy section is provided by the Group Policy template `Kerberos.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.26 Locale Services

This section contains recommendations for Locale Services settings.

This Group Policy section is provided by the Group Policy template `Globalization.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.27 Logon

This section contains recommendations related to the logon process and lock screen.

This Group Policy section is provided by the Group Policy template `Logon.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.27.1 (L1) Ensure 'Block user from showing account details on sign-in' is set to 'Enabled'

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\System\Logon\Block user from showing account
details on sign-in
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `Logon.admx/adml` that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative

Templates (or newer).

Impact:

Users cannot choose to show account details on the sign-in screen.

Assessment:

Ensure 'BlockUserFromShowingAccountDetailsOnSignin' is 'Windows: Registry Value' to '1' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System:BlockUserFromShowingAccountDetailsOnSignin        does not exist
```

References:

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control: --** More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control: --** More

Back to Summary

18.8.27.2 (L1) Ensure 'Do not display network selection UI' is set to 'Enabled'

Pass

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.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\System\Logon\Do not display network selection
UI
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `Logon.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Impact:

The PC's network connectivity state cannot be changed without signing into Windows.

Assessment:

Ensure 'DontDisplayNetworkSelectionUI' is 'Windows: Registry Value' to '1' -- More

References:

- **CCE-IDv5:** CCE-33822-8 -- More

CIS Controls V6.1:

- **Control 5: Controlled Use of Administrative Privileges:** -- More

Back to Summary

18.8.27.3 (L1) Ensure 'Do not enumerate connected users on domain-joined computers' is set to 'Enabled'

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\System\Logon\Do not enumerate connected users
on domain-joined computers
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `Logon.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Impact:

The Logon UI will not enumerate any connected users on domain-joined computers.

Assessment:

Ensure 'DontEnumerateConnectedUsers' is 'Windows: Registry Value' to '1' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\System:DontEnumerateConnectedUsers     does not exist
```

References:

- **CCE-IDv5:** CCE-35207-0 -- More

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

18.8.27.4 (L1) Ensure 'Enumerate local users on domain-joined computers' is set to 'Disabled'

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\System\Logon\Enumerate local users on domain-joined computers
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `Logon.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Impact:

None - this is the default behavior.

Assessment:

Ensure 'EnumerateLocalUsers' is 'Windows: Registry Value' to '0' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\System:EnumerateLocalUsers        does not exist
```

References:

- **CCE-IDv5:** CCE-34838-3 -- More

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

18.8.27.5 (L1) Ensure 'Turn off app notifications on the lock screen' is set to 'Enabled'

Fail

Description:

This policy setting allows you to prevent app notifications from appearing on the lock screen.

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

Rationale:

App notifications might display sensitive business or personal data.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\System\Logon\Turn off app notifications on the
lock screen
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `Logon.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Impact:

No app notifications are displayed on the lock screen.

Assessment:

Ensure 'DisableLockScreenAppNotifications' is 'Windows: Registry Value' to '1' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\System:DisableLockScreenAppNotifications does not exist

References:

- **CCE-IDv5:** CCE-34837-5 -- More

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

18.8.27.6 (L1) Ensure 'Turn off picture password sign-in' is set to 'Enabled'

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\System\Logon\Turn off picture password sign-in
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `CredentialProviders.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Impact:

Users will not be able to set up or sign in with a picture password.

Assessment:

Ensure 'BlockDomainPicturePassword' is 'Windows: Registry Value' to '1' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\System:BlockDomainPicturePassword          does not exist
```

References:

- **CCE-IDv5:** CCE-35291-4 -- More

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

18.8.27.7 (L1) Ensure 'Turn on convenience PIN sign-in' is set to 'Disabled'

Fail

Description:

This policy setting allows you to control whether a domain user can sign in using a convenience PIN. In Windows 10, convenience PIN was replaced with Passport, which has stronger security properties. To configure Passport for domain users, use the policies under Computer Configuration\Administrative Templates\Windows Components\Microsoft Passport for Work.

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

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

Rationale:

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

Remediation:

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

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

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template

`CredentialProviders.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Turn on PIN sign-in*, but it was renamed starting with the Windows 10 Release 1511 Administrative Templates.

Impact:

None - this is the default behavior.

Assessment:

Ensure 'AllowDomainPINLogon' is 'Windows: Registry Value' to '0' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\System:AllowDomainPINLogon        does not exist
```

References:

- **CCE-IDv5:** CCE-35095-9 -- More

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

18.8.28 Mitigation Options

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

This Group Policy section is provided by the Group Policy template `GroupPolicy.admx/adml` that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

18.8.29 Net Logon

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

This Group Policy section is provided by the Group Policy template `Netlogon.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.30 OS Policies

This section contains recommendations related to OS Policies.

This Group Policy section is provided by the Group Policy template `OSPolicy.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

18.8.31 Performance Control Panel

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

This Group Policy section is provided by the Group Policy template `PerfCenterCPL.admx/adml` that is only included with the Microsoft Windows Vista through the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

18.8.32 PIN Complexity

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

This Group Policy section is provided by the Group Policy template `Passport.admx/adml` that is included with the Microsoft Windows 10 Release 1703 Administrative Templates (or newer).

18.8.33 Power Management

This section contains recommendations for Power Management settings.

This Group Policy section is provided by the Group Policy template `Power.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.33.1 Button Settings

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

This Group Policy section is provided by the Group Policy template `Power.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.33.2 Energy Saver Settings

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

This Group Policy section is provided by the Group Policy template `Power.admx/adml` that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

18.8.33.3 Hard Disk Settings

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

This Group Policy section is provided by the Group Policy template `Power.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.33.4 Notification Settings

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

This Group Policy section is provided by the Group Policy template `Power.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.33.5 Power Throttling Settings

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

This Group Policy section is provided by the Group Policy template `Power.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

18.8.33.6 Sleep Settings

This section contains recommendations related to Power Management Sleep mode.

This Group Policy section is provided by the Group Policy template `Power.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.33.6.1 (L1) Ensure 'Allow network connectivity during connected-standby (on battery)' is set to 'Disabled'

Fail

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.

Remediation:

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

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

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `Power.admx/adml` that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

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).

Assessment:

Ensure 'DCSettingIndex' is 'Windows: Registry Value' to '0' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Power\PowerSettings\f15576e8-98b7-4186-b944-eafa664402d9:DCSettingIndex does not exist

References:

CIS Controls V6.1:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

Back to Summary

18.8.33.6.2 (L1) Ensure 'Allow network connectivity during connected-standby (plugged in)' is set to 'Disabled'

Fail

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.

Remediation:

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

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

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `Power.admx/adml` that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

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).

Assessment:

Ensure 'ACSettingIndex' is 'Windows: Registry Value' to '0' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Power\PowerSettings\f15576e8-98b7-4186-b944-eafa664402d9:ACSettingIndex does not exist

References:

CIS Controls V6.1:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

Back to Summary

18.8.33.6.5 (L1) Ensure 'Require a password when a computer wakes (on battery)' is set to 'Enabled'

Fail

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.

Remediation:

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

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

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `Power.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Impact:

None - this is the default behavior.

Assessment:

Ensure 'DCSettingIndex' is 'Windows: Registry Value' to '1' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Power\PowerSettings\0e796bdb-100d-47d6-a2d5-f7d2daa51f51:DCSettingIndex does not exist

References:

- **CCE-IDv5:** CCE-33782-4 -- More

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

18.8.33.6.6 (L1) Ensure 'Require a password when a computer wakes (plugged in)' is set to 'Enabled'

Fail

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.

Remediation:

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

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

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `Power.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Impact:

None - this is the default behavior.

Assessment:

Ensure 'ACSettingIndex' is 'Windows: Registry Value' to '1' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Power\PowerSettings\0e796bdb-100d-47d6-a2d5-f7d2daa51f51:ACSettingIndex does not exist

References:

- **CCE-IDv5:** CCE-35462-1 -- More

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

18.8.34 Recovery

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

This Group Policy section is provided by the Group Policy template `ReAgent.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.8.35 Remote Assistance

This section contains recommendations related to Remote Assistance.

This Group Policy section is provided by the Group Policy template `RemoteAssistance.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.35.1 (L1) Ensure 'Configure Offer Remote Assistance' is set to 'Disabled'

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\System\Remote Assistance\Configure Offer Remote
Assistance
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `RemoteAssistance.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Impact:

None - this is the default behavior.

Assessment:

Ensure 'fAllowUnsolicited' is 'Windows: Registry Value' to '0' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\Software\policies\Microsoft\Windows NT\Terminal Services:fAllowUnsolicited        does not exist
```

References:

- **CCE-IDv5:** CCE-33801-2 -- More

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

CIS Controls V6.1:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

Back to Summary

18.8.35.2 (L1) Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled'

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\System\Remote Assistance\Configure Solicited
Remote Assistance
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `RemoteAssistance.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

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.

Assessment:

Ensure 'fAllowToGetHelp' is 'Windows: Registry Value' to '0' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\Software\policies\Microsoft\Windows NT\Terminal Services:fAllowToGetHelp          does not exist
```

References:

- **CCE-IDv5:** CCE-35331-8 -- More

CIS Controls V6.1:

- **Control 5: Controlled Use of Administrative Privileges:** -- More

Back to Summary

18.8.36 Remote Procedure Call

This section contains recommendations related to Remote Procedure Call.

This Group Policy section is provided by the Group Policy template `RPC.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.36.1 (L1) Ensure 'Enable RPC Endpoint Mapper Client Authentication' is set to 'Enabled'

Fail

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 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.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\System\Remote Procedure Call\Enable RPC
Endpoint Mapper Client Authentication
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `RPC.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

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.

Assessment:

Ensure 'EnableAuthEpResolution' is 'Windows: Registry Value' to '1' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\Rpc:EnableAuthEpResolution          does not exist
```

References:

- **CCE-IDv5:** CCE-35392-0 -- More

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

CIS Controls V6.1:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

Back to Summary

18.8.36.2 (L1) Ensure 'Restrict Unauthenticated RPC clients' is set to 'Enabled: Authenticated'

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\System\Remote Procedure Call\Restrict
Unauthenticated RPC clients
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `RPC.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Impact:

None - this is the default behavior.

Assessment:

Ensure 'RestrictRemoteClients' is 'Windows: Registry Value' to '1' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\Rpc:RestrictRemoteClients does not exist

References:

- **CCE-IDv5:** CCE-35391-2 -- More

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

CIS Controls V6.1:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

Back to Summary

18.8.37 Removable Storage Access

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

This Group Policy section is provided by the Group Policy template `RemovableStorage.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.38 Scripts

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

This Group Policy section is provided by the Group Policy template `Scripts.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.39 Server Manager

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

This Group Policy section is provided by the Group Policy template `ServerManager.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.40 Shutdown

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

This Group Policy section is provided by the Group Policy template `WinInit.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.8.41 Shutdown Options

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

This Group Policy section is provided by the Group Policy template `Winsrv.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.42 Storage Health

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

This Group Policy section is provided by the Group Policy template `StorageHealth.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

18.8.43 System Restore

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

This Group Policy section is provided by the Group Policy template `SystemRestore.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.44 Troubleshooting and Diagnostics

This section contains recommendations related to Troubleshooting and Diagnostics.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.44.1 Application Compatibility Diagnostics

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

This Group Policy section is provided by the Group Policy template `pca.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.44.2 Corrupted File Recovery

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

This Group Policy section is provided by the Group Policy template `FileRecovery.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.44.3 Disk Diagnostic

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

This Group Policy section is provided by the Group Policy template `DiskDiagnostic.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.44.4 Fault Tolerant Heap

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

This Group Policy section is provided by the Group Policy template `fthsvc.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.8.44.5 Microsoft Support Diagnostic Tool

This section contains recommendations related to the Microsoft Support Diagnostic Tool.

This Group Policy section is provided by the Group Policy template `MSDT.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.44.6 MSI Corrupted File Recovery

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

This Group Policy section is provided by the Group Policy template `Msi-FileRecovery.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.8.44.7 Scheduled Maintenance

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

This Group Policy section is provided by the Group Policy template `sdiagschd.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.8.44.8 Scripted Diagnostics

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

This Group Policy section is provided by the Group Policy template `sdiageng.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.8.44.9 Windows Boot Performance Diagnostics

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

This Group Policy section is provided by the Group Policy template `PerformanceDiagnostics.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.44.10 Windows Memory Leak Diagnosis

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

This Group Policy section is provided by the Group Policy template `LeakDiagnostic.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.44.11 Windows Performance PerfTrack

This section contains recommendations related to Windows Performance PerfTrack.

This Group Policy section is provided by the Group Policy template `PerformancePerftrack.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.8.45 Trusted Platform Module Services

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

This Group Policy section is provided by the Group Policy template `TPM.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.46 User Profiles

This section contains recommendations related to User Profiles.

This Group Policy section is provided by the Group Policy template `UserProfiles.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.47 Windows File Protection

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

This Group Policy section is provided by the Group Policy template `WindowsFileProtection.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.48 Windows HotStart

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

This Group Policy section is provided by the Group Policy template `HotStart.admx/adml` that is only included with the Microsoft Windows Vista through the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

18.8.49 Windows Time Service

This section contains recommendations related to the Windows Time Service.

This Group Policy section is provided by the Group Policy template `W32Time.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.8.49.1 Time Providers

This section contains recommendations related to Time Providers.

This Group Policy section is provided by the Group Policy template `W32Time.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9 Windows Components

This section contains recommendations for Windows Component settings.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.1 Active Directory Federation Services

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

This Group Policy section is provided by the Group Policy template `adfs.admx/adml` that is only included with the Microsoft Windows Vista through the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

18.9.2 ActiveX Installer Service

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

This Group Policy section is provided by the Group Policy template `ActiveXInstallService.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.3 Add features to Windows 8 / 8.1 / 10 (formerly Windows Anytime Upgrade)

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

This Group Policy section is provided by the Group Policy template `WindowsAnytimeUpgrade.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Note: This section was initially named *Windows Anytime Upgrade* but was renamed by Microsoft to *Add features to Windows x* starting with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

18.9.4 App Package Deployment

This section contains recommendations for App Package Deployment settings.

This Group Policy section is provided by the Group Policy template `AppxPackageManager.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.9.5 App Privacy

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

This Group Policy section is provided by the Group Policy template `AppPrivacy.admx/adml` that is included with the Microsoft Windows 10 Release 1511 Administrative Templates (or newer).

18.9.6 App runtime

This section contains recommendations for App runtime settings.

This Group Policy section is provided by the Group Policy template `AppXRuntime.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.9.6.1 (L1) Ensure 'Allow Microsoft accounts to be optional' is set to 'Enabled'

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\App runtime\Allow Microsoft
accounts to be optional
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `AppXRuntime.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Impact:

Windows Store apps that typically require a Microsoft account to sign in will allow users to sign in with an enterprise account instead.

Assessment:

Ensure 'MSAOptional' is 'Windows: Registry Value' to '1' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System:MSAOptional          does not exist
```

References:

- **CCE-IDv5:** CCE-35803-6 -- More

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

18.9.7 Application Compatibility

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

This Group Policy section is provided by the Group Policy template `AppCompat.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.8 AutoPlay Policies

This section contains recommendations for AutoPlay policies.

This Group Policy section is provided by the Group Policy template `AutoPlay.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.8.1 (L1) Ensure 'Disallow Autoplay for non-volume devices' is set to 'Enabled'

Description:

Fail

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.

Remediation:

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

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

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `AutoPlay.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Impact:

AutoPlay will not be allowed for MTP devices like cameras or phones.

Assessment:

Ensure 'NoAutoplayfornonVolume' is 'Windows: Registry Value' to '1' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Explorer:NoAutoplayfornonVolume        does not exist
```

References:

- **CCE-IDv5:** CCE-35289-8 -- More

CIS Controls V7.0:

- **Control 8: Malware Defenses:** -- More
- **Control 8: Malware Defenses:** -- More

CIS Controls V6.1:

- **Control 8: Malware Defenses:** -- More

Back to Summary

18.9.8.2 (L1) Ensure 'Set the default behavior for AutoRun' is set to 'Enabled: Do not execute any autorun commands'

Fail

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.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Do not execute any autorun commands`:

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

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `AutoPlay.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Impact:

AutoRun commands will be completely disabled.

Assessment:

Ensure 'NoAutorun' is 'Windows: Registry Value' to '1' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer:NoAutorun          does not exist
```

References:

- **CCE-IDv5:** CCE-34771-6 -- More

CIS Controls V7.0:

- **Control 8: Malware Defenses:** -- More
- **Control 8: Malware Defenses:** -- More

CIS Controls V6.1:

- **Control 8: Malware Defenses:** -- More

Back to Summary

18.9.8.3 (L1) Ensure 'Turn off Autoplay' is set to 'Enabled: All drives'

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\AutoPlay Policies\Turn off
Autoplay
```

Note: This Group Policy path is provided by the Group Policy template `AutoPlay.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Impact:

Autoplay will be disabled - users will have to manually launch setup or installation programs that are provided on removable media.

Assessment:

Ensure 'NoDriveTypeAutoRun' is 'Windows: Registry Value' to '255' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer:NoDriveTypeAutoRun          does not exist
```

References:

- **CCE-IDv5:** CCE-33791-5 -- More

CIS Controls V7.0:

- **Control 8: Malware Defenses:** -- More
- **Control 8: Malware Defenses:** -- More

CIS Controls V6.1:

- **Control 8: Malware Defenses:** -- More

Back to Summary

18.9.9 Backup

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

This Group Policy section is provided by the Group Policy template `UserDataBackup.admx/adml` that is only included with the Microsoft Windows Vista through the Windows 10 Release 1511 Administrative Templates (except for the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates).

18.9.10 Biometrics

This section contains recommendations related to Biometrics.

This Group Policy section is provided by the Group Policy template `Biometrics.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.9.10.1 Facial Features

This section contains recommendations related to Facial Feature Biometrics.

This Group Policy section is provided by the Group Policy template `Biometrics.admx/adml` that is included with the Microsoft Windows 10 Release 1511 Administrative Templates (or newer).

18.9.10.1.1 (L1) Ensure 'Configure enhanced anti-spoofing' is set to 'Enabled'

Fail

Description:

This policy setting determines whether enhanced anti-spoofing is configured for devices which support it.

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

Rationale:

Enterprise managed environments are now supporting a wider range of mobile devices, increasing the security on these devices will help protect against unauthorized access on your network.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Biometrics\Facial
Features\Configure enhanced anti-spoofing
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `Biometrics.admx/adml` that is included with the Microsoft Windows 10 Release 1511 Administrative Templates (or newer).

Note #2: In the Windows 10 Release 1511 and Windows 10 Release 1607 & Server 2016 Administrative Templates, this setting was named *Use enhanced anti-spoofing when available*. It was renamed to *Configure enhanced anti-spoofing* starting with the Windows 10 Release 1703 Administrative Templates.

Impact:

Windows will require all users on the device to use anti-spoofing for facial features, on devices which support it.

Assessment:

Ensure 'EnhancedAntiSpoofing' is 'Windows: Registry Value' to '1' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Biometrics\FacialFeatures:EnhancedAntiSpoofing          does not exist
```

References:

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

18.9.11 BitLocker Drive Encryption

This section contains recommendations for configuring BitLocker.

This Group Policy section is provided by the Group Policy template `VolumeEncryption.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.11.1 Fixed Data Drives

This section contains recommendations for configuring Fixed Data Drives in BitLocker.

This Group Policy section is provided by the Group Policy template `VolumeEncryption.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.9.11.2 Operating System Drives

This section contains recommendations for configuring Operating System Drives in BitLocker.

This Group Policy section is provided by the Group Policy template `VolumeEncryption.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.9.11.3 Removable Data Drives

This section contains recommendations for configuring Removable Data Drives in BitLocker.

This Group Policy section is provided by the Group Policy template `VolumeEncryption.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.9.12 Camera

This section contains recommendations related to Camera.

This Group Policy section is provided by the Group Policy template `Camera.admx/adml` that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

18.9.13 Cloud Content

This section contains recommendations related to Cloud Content.

This Group Policy section is provided by the Group Policy template `CloudContent.admx/adml` that is included with the Microsoft Windows 10 Release 1511 Administrative Templates (or newer).

18.9.13.1 (L1) Ensure 'Turn off Microsoft consumer experiences' is set to 'Enabled'

Fail

Description:

This policy setting turns off experiences that help consumers make the most of their devices and Microsoft account.

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

Note: Per Microsoft TechNet, this policy setting only applies to Windows 10 Enterprise and Windows 10 Education editions.

Rationale:

Having apps silently install in an enterprise managed environment is not good security practice - especially if the apps send data back to a 3rd party.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Cloud Content\Turn off
Microsoft consumer experiences
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `CloudContent.admx/adml` that is included with the Microsoft Windows 10 Release 1511 Administrative Templates (or newer).

Impact:

Users will no longer see personalized recommendations from Microsoft and notifications about their Microsoft account.

Assessment:

Ensure 'DisableWindowsConsumerFeatures' is 'Windows: Registry Value' to '1' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CloudContent:DisableWindowsConsumerFeatures          does not exist
```

References:

CIS Controls V6.1:

- **Control 13: Data Protection:** -- More

Back to Summary

18.9.14 Connect

This section contains recommendations related to Connect.

This Group Policy section is provided by the Group Policy template `WirelessDisplay.admx/adml` that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

18.9.14.1 (L1) Ensure 'Require pin for pairing' is set to 'Enabled'

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Connect\Require pin for
pairing
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WirelessDisplay.admx/adml` that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

Impact:

The pairing ceremony for connecting to new wireless display devices will always require a PIN.

Assessment:

Ensure 'AllowProjectionToPC' is 'Windows: Registry Value' to '1' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Connect:RequirePinForPairing          does not exist
```

References:

CIS Controls V7.0:

- **Control 15: Wireless Access Control:** -- More

CIS Controls V6.1:

- **Control 15: Wireless Access Control:** -- More

Back to Summary

18.9.15 Credential User Interface

This section contains recommendations related to the Credential User Interface.

This Group Policy section is provided by the Group Policy template `CredUI.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.15.1 (L1) Ensure 'Do not display the password reveal button' is set to 'Enabled'

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Credential User Interface\Do
not display the password reveal button
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `CredUI.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Impact:

The password reveal button will not be displayed after a user types a password in the password entry text box.

Assessment:

Ensure 'DisablePasswordReveal' is 'Windows: Registry Value' to '1' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CredUI:DisablePasswordReveal          does not exist
```

References:

- **CCE-IDv5:** CCE-32965-6 -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

18.9.15.2 (L1) Ensure 'Enumerate administrator accounts on elevation' is set to 'Disabled'

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Credential User
Interface\Enumerate administrator accounts on elevation
```

Note: This Group Policy path is provided by the Group Policy template `CredUI.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Impact:

None - this is the default behavior.

Assessment:

Ensure 'EnumerateAdministrators' is 'Windows: Registry Value' to '0' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\CredUI:EnumerateAdministrators          does not exist
```

References:

- **CCE-IDv5:** CCE-35194-0 -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

18.9.16 Data Collection and Preview Builds

This section contains settings for Data Collection and Preview Builds.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with the

Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

18.9.16.1 (L1) Ensure 'Allow Telemetry' is set to 'Enabled: 0 - Security [Enterprise Only]' or 'Enabled: 1 - Basic'

Fail

Description:

This policy setting determines the amount of diagnostic and usage data reported to Microsoft:

- A value of `0 - Security [Enterprise Only]` will send minimal data to Microsoft. This data includes Malicious Software Removal Tool (MSRT) & Windows Defender data, if enabled, and telemetry client settings. Setting a value of 0 applies to enterprise, EDU, IoT and server devices only. Setting a value of 0 for other devices is equivalent to choosing a value of 1.
- A value of `1 - Basic` sends only a basic amount of diagnostic and usage data. Note that setting values of 0 or 1 will degrade certain experiences on the device.
- A value of `2 - Enhanced` sends enhanced diagnostic and usage data.
- A value of `3 - Full` sends the same data as a value of 2, plus additional diagnostics data, including the files and content that may have caused the problem.

Windows 10 telemetry settings apply to the Windows operating system and some first party apps. This setting does not apply to third party apps running on Windows 10.

The recommended state for this setting is: `Enabled: 0 - Security [Enterprise Only]` or `Enabled: 1 - Basic`.

Note: If the *Allow Telemetry* setting is configured to `0 - Security [Enterprise Only]`, then the options in Windows Update to defer upgrades and updates will have no effect.

Note #2: In the Microsoft Windows 10 RTM (Release 1507) Administrative Templates, the zero value was named `0 - Off [Enterprise Only]`, but it was renamed to `0 - Security [Enterprise Only]` starting with the Windows 10 Release 1511 Administrative Templates.

Rationale:

Sending any data to a 3rd party vendor is a security concern and should only be done on an as needed basis.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: 0 - Security [Enterprise Only]` or `Enabled: 1 - Basic`:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Data Collection and Preview Builds\Allow Telemetry
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `DataCollection.admx/adml` that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

Impact:

Note that setting values of 0 or 1 will degrade certain experiences on the device.

Assessment:

Any of the following tests or sub-groups may pass:

Ensure 'AllowTelemetry' is 'Windows: Registry Value' to '1' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\DataCollection:AllowTelemetry does not exist

Ensure 'AllowTelemetry' is 'Windows: Registry Value' to '0' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\DataCollection:AllowTelemetry does not exist

References:

- **CCE-IDv5:** CCE-41400-3 -- More

CIS Controls V6.1:

- **Control 13: Data Protection:** -- More

Back to Summary

18.9.16.3 (L1) Ensure 'Do not show feedback notifications' is set to 'Enabled'

Fail

Description:

This policy setting allows an organization to prevent its devices from showing feedback questions from Microsoft.

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

Rationale:

Users should not be sending any feedback to 3rd party vendors in an enterprise managed environment.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Data Collection and Preview
Builds\Do not show feedback notifications
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `FeedbackNotifications.admx/adml` that is included with the Microsoft Windows 10 Release 1511 Administrative Templates (or newer).

Impact:

Users will no longer see feedback notifications through the Windows Feedback app.

Assessment:

Ensure 'DoNotShowFeedbackNotifications' is 'Windows: Registry Value' to '1' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DataCollection:DoNotShowFeedbackNotifications          does not exist
```

References:

CIS Controls V6.1:

- **Control 13: Data Protection:** -- More

Back to Summary

18.9.16.4 (L1) Ensure 'Toggle user control over Insider builds' is set to 'Disabled'

Fail

Description:

This policy setting determines whether users can access the Insider build controls in the Advanced Options for Windows Update. These controls are located under "Get Insider builds," and enable users to make their devices available for downloading and installing Windows preview software.

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

Note: This policy setting applies only to devices running Windows 10 Pro or Windows 10 Enterprise, up until Release 1703. For Release 1709 or newer, Microsoft encourages using the `Manage preview builds` setting (Rule 18.9.101.1.1). We have kept this setting in the benchmark to ensure that any older builds of Windows 10 in the environment are still enforced.

Rationale:

It can be risky for experimental features to be allowed in an enterprise managed environment because this can introduce bugs and security holes into systems, making it easier for an attacker to gain access. It is generally preferred to only use production-ready builds.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Data Collection and Preview
Builds\Toggle user control over Insider builds
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `AllowBuildPreview.admx/adml` that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

Impact:

The item "Get Insider builds" will be unavailable.

Assessment:

Ensure 'AllowBuildPreview' is 'Windows: Registry Value' to '0' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\PreviewBuilds:AllowBuildPreview          does not exist
```

References:

- **CCE-IDv5:** CCE-41380-7 -- More

CIS Controls V6.1:

- **Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers:** -- More

Back to Summary

18.9.17 Delivery Optimization

This section contains settings for Delivery Optimization.

This Group Policy section is provided by the Group Policy template `DeliveryOptimization.admx/adml` that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

18.9.17.1 (L1) Ensure 'Download Mode' is NOT set to 'Enabled: Internet'

Pass

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` (i.e. 3).

Note: The default on all SKUs other than Enterprise, Enterprise LTSB or Education is `Enabled: Internet`, 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.

Remediation:

To establish the recommended configuration via GP, set the following UI path to any value *other than* `Enabled: Internet`:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Delivery
Optimization\Download Mode
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `DeliveryOptimization.admx/adml` that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

Impact:

Machines will not be able to download updates from peers on the Internet. If set to `Enabled: HTTP only`, `Enabled: Simple`, or `Enabled: Bypass`, machines will not be able to download updates from other machines on the same LAN.

Assessment:

Ensure 'DODownloadMode' is 'Windows: Registry Value' not set to '3' -- More

References:

CIS Controls V7.0:

- **Control 3: Continuous Vulnerability Management:** -- More
- **Control 3: Continuous Vulnerability Management:** -- More

CIS Controls V6.1:

- **Control 4: Continuous Vulnerability Assessment and Remedia:** -- More

Back to Summary

18.9.18 Desktop Gadgets

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

This Group Policy section is provided by the Group Policy template `Sidebar.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.9.19 Desktop Window Manager

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

This Group Policy section is provided by the Group Policy template `DWM.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.20 Device and Driver Compatibility

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

This Group Policy section is provided by the Group Policy template `DeviceCompat.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.9.21 Device Registration (formerly Workplace Join)

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

This Group Policy section is provided by the Group Policy template `WorkplaceJoin.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Note: This section was initially named *Workplace Join* but was renamed by Microsoft to *Device Registration* starting with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates.

18.9.22 Digital Locker

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

This Group Policy section is provided by the Group Policy template `DigitalLocker.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.23 Edge UI

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

This Group Policy section is provided by the Group Policy template `EdgeUI.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.9.24 EMET

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

This Group Policy section is provided by the Group Policy template `EMET.admx/adml` that is included with Microsoft EMET.

EMET is free and supported security software developed by Microsoft that allows an enterprise to apply exploit mitigations to applications that run on Windows. Many of these mitigations were later coded directly into Windows 10 and Server 2016.

Note: Although EMET is quite effective at enhancing exploit protection on Windows workstation OSes prior to Windows 10, it is highly recommended that compatibility testing is done on typical workstation configurations (including all CIS-recommended EMET settings) before widespread deployment to your environment.

Note #2: EMET has been reported to be very problematic on 32-bit OSes - we only recommend using it with 64-bit OSes.

Note #3: Microsoft has announced that EMET will be End-Of-Life (EOL) on July 31, 2018. This does not mean the software will stop working, only that Microsoft will not update it any further past that date, nor troubleshoot new problems with it. They are instead recommending that workstations be upgraded to Windows 10.

18.9.25 Event Forwarding

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

This Group Policy section is provided by the Group Policy template `EventForwarding.admx/adml` that is included with the Microsoft Windows Server 2008 (non-R2) Administrative Templates (or newer).

18.9.26 Event Log Service

This section contains recommendations for configuring the Event Log Service.

This Group Policy section is provided by the Group Policy template `EventLog.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.26.1 Application

This section contains recommendations for configuring the Application Event Log.

This Group Policy section is provided by the Group Policy template `EventLog.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.26.1.1 (L1) Ensure 'Application: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'

Fail

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.

Remediation:

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

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

Note: This Group Policy path is provided by the Group Policy template `EventLog.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Retain old events*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

Impact:

None - this is the default behavior.

Assessment:

Ensure 'Retention' is 'Windows: Registry Value' to '0' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\EventLog\Application:Retention          does not exist
```

References:

- **CCE-IDv5:** CCE-34169-3 -- More

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More

CIS Controls V6.1:

- **Control 6: Maintenance, Monitoring, and Analysis of Audit Logs:** -- More

Back to Summary

18.9.26.1.2 (L1) Ensure 'Application: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'

Fail

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.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: 32,768 or greater`:

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

Note: This Group Policy path is provided by the Group Policy template `EventLog.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Maximum Log Size (KB)*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

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.

Assessment:

Ensure 'MaxSize' is 'Windows: Registry Value' to '32768' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\EventLog\Application:MaxSize does not exist

References:

- **CCE-IDv5:** CCE-33975-4 -- More

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More

CIS Controls V6.1:

- **Control 6: Maintenance, Monitoring, and Analysis of Audit Logs:** -- More

Back to Summary

18.9.26.2 Security

This section contains recommendations for configuring the Security Event Log.

This Group Policy section is provided by the Group Policy template `EventLog.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.26.2.1 (L1) Ensure 'Security: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'

Fail

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.

Remediation:

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

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

Note: This Group Policy path is provided by the Group Policy template `EventLog.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Retain old events*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

Impact:

None - this is the default behavior.

Assessment:

Ensure 'Retention' is 'Windows: Registry Value' to '0' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\EventLog\Security:Retention        does not exist
```

References:

- **CCE-IDv5:** CCE-35090-0 -- More

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More

CIS Controls V6.1:

- **Control 6: Maintenance, Monitoring, and Analysis of Audit Logs:** -- More

Back to Summary

18.9.26.2.2 (L1) Ensure 'Security: Specify the maximum log file size (KB)' is set to 'Enabled: 196,608 or greater'

Fail

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.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: 196,608 or greater`:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Security
\Specify the maximum log file size (KB)
```

Note: This Group Policy path is provided by the Group Policy template `EventLog.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Maximum Log Size (KB)*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

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.

Assessment:

Ensure 'MaxSize' is 'Windows: Registry Value' to '196608' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\EventLog\Security:MaxSize          does not exist
```

References:

- **CCE-IDv5:** CCE-33428-4 -- More

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More

CIS Controls V6.1:

- **Control 6: Maintenance, Monitoring, and Analysis of Audit Logs:** -- More

Back to Summary

18.9.26.3 Setup

This section contains recommendations for configuring the Setup Event Log.

This Group Policy section is provided by the Group Policy template `EventLog.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.26.3.1 (L1) Ensure 'Setup: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'

Fail

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.

Remediation:

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

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

Note: This Group Policy path is provided by the Group Policy template `EventLog.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Retain old events*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

Impact:

None - this is the default behavior.

Assessment:

Ensure 'Retention' is 'Windows: Registry Value' to '0' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\EventLog\Setup:Retention                    does not exist
```

References:

- **CCE-IDv5:** CCE-34170-1 -- More

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More

CIS Controls V6.1:

- **Control 6: Maintenance, Monitoring, and Analysis of Audit Logs:** -- More

Back to Summary

18.9.26.3.2 (L1) Ensure 'Setup: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'

Fail

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

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: 32,768 or greater`:

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

Note: This Group Policy path is provided by the Group Policy template `EventLog.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Maximum Log Size (KB)*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

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.

Assessment:

Ensure 'MaxSize' is 'Windows: Registry Value' to '32768' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\EventLog\Setup:MaxSize          does not exist
```

References:

- **CCE-IDv5:** CCE-35091-8 -- More

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More

CIS Controls V6.1:

- **Control 6: Maintenance, Monitoring, and Analysis of Audit Logs:** -- More

Back to Summary

18.9.26.4 System

This section contains recommendations for configuring the System Event Log.

This Group Policy section is provided by the Group Policy template `EventLog.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.26.4.1 (L1) Ensure 'System: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'

Fail

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.

Remediation:

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

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

Note: This Group Policy path is provided by the Group Policy template `EventLog.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Retain old events*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

Impact:

None - this is the default behavior.

Assessment:

Ensure 'Retention' is 'Windows: Registry Value' to '0' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\EventLog\System:Retention          does not exist
```

References:

- **CCE-IDv5:** CCE-33729-5 -- More

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More

CIS Controls V6.1:

- **Control 6: Maintenance, Monitoring, and Analysis of Audit Logs:** -- More

Back to Summary

18.9.26.4.2 (L1) Ensure 'System: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'

Fail

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

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: 32,768 or greater`:

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

Note: This Group Policy path is provided by the Group Policy template `EventLog.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Maximum Log Size (KB)*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

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.

Assessment:

Ensure 'MaxSize' is 'Windows: Registry Value' to '32768' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\EventLog\System:MaxSize                     does not exist
```

References:

- **CCE-IDv5:** CCE-35288-0 -- More

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More

CIS Controls V6.1:

- **Control 6: Maintenance, Monitoring, and Analysis of Audit Logs:** -- More

Back to Summary

18.9.27 Event Logging

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

This Group Policy section is provided by the Group Policy template `EventLogging.admx/adml` that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

18.9.28 Event Viewer

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

This Group Policy section is provided by the Group Policy template `EventViewer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.29 Family Safety (formerly Parental Controls)

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

This Group Policy section is provided by the Group Policy template `ParentalControls.admx/adml` that is only included with the Microsoft Windows Vista through the Windows 10 RTM (Release 1507) Administrative Templates.

Note: This section was initially named *Parental Controls* but was renamed by Microsoft to *Family Safety* starting with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

18.9.30 File Explorer (formerly Windows Explorer)

This section contains recommendations to control the availability of options such as menu items and tabs in dialog boxes.

This Group Policy section is provided by the Group Policy template `WindowsExplorer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note: This section was initially named *Windows Explorer* but was renamed by Microsoft to *File Explorer* starting with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

18.9.30.1 Previous Versions

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

This Group Policy section is provided by the Group Policy template `PreviousVersions.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.30.2 (L1) Ensure 'Turn off Data Execution Prevention for Explorer' is set to 'Disabled'

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\File Explorer\Turn off Data
Execution Prevention for Explorer
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `Explorer.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Impact:

None - this is the default behavior.

Assessment:

Ensure 'NoDataExecutionPrevention' is 'Windows: Registry Value' to '0' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Explorer:NoDataExecutionPrevention        does not exist
```

References:

- **CCE-IDv5:** CCE-33608-1 -- More

CIS Controls V7.0:

- **Control 8: Malware Defenses:** -- More

CIS Controls V6.1:

- **Control 8: Malware Defenses:** -- More

Back to Summary

18.9.30.3 (L1) Ensure 'Turn off heap termination on corruption' is set to 'Disabled'

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\File Explorer\Turn off heap termination on corruption
```

Note: This Group Policy path is provided by the Group Policy template `Explorer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Impact:

None - this is the default behavior.

Assessment:

Ensure 'NoHeapTerminationOnCorruption' is 'Windows: Registry Value' to '0' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Explorer:NoHeapTerminationOnCorruption          does not exist
```

References:

- **CCE-IDv5:** CCE-33745-1 -- More

CIS Controls V7.0:

- **Control 8: Malware Defenses:** -- More

CIS Controls V6.1:

- **Control 8: Malware Defenses:** -- More

Back to Summary

18.9.30.4 (L1) Ensure 'Turn off shell protocol protected mode' is set to 'Disabled'

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\File Explorer\Turn off shell
protocol protected mode
```

Note: This Group Policy path is provided by the Group Policy template `WindowsExplorer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Impact:

None - this is the default behavior.

Assessment:

Ensure 'PreXPSP2ShellProtocolBehavior' is 'Windows: Registry Value' to '0' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer:PreXPSP2ShellProtocolBehavior        does not exist
```

References:

- **CCE-IDv5:** CCE-33764-2 -- More

CIS Controls V7.0:

- **Control 8: Malware Defenses:** -- More

CIS Controls V6.1:

- **Control 8: Malware Defenses:** -- More

Back to Summary

18.9.31 File History

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

This Group Policy section is provided by the Group Policy template `FileHistory.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.9.32 Find My Device

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

This Group Policy section is provided by the Group Policy template `FindMy.admx/adml` that is included with the Microsoft Windows 10 Release 1703 Administrative Templates (or newer).

18.9.33 Game Explorer

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

This Group Policy section is provided by the Group Policy template `GameExplorer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.34 Handwriting

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

This Group Policy section is provided by the Group Policy template `Handwriting.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

18.9.35 HomeGroup

This section contains recommendations related to the HomeGroup feature, which is available in all workstations of Windows from Windows 7 through Windows 10 Release 1709. Microsoft removed it from Windows starting with Windows 10 Release 1803.

This Group Policy section is provided by the Group Policy template `Sharing.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.9.35.1 (L1) Ensure 'Prevent the computer from joining a homegroup' is set to 'Enabled'

Fail

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. This recommendation will be removed from future CIS Windows 10 benchmarks that are released after April 14, 2020 (i.e. end of Microsoft support for Windows 10 Release 1709, the last version to support HomeGroup).

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.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\HomeGroup\Prevent the
computer from joining a homegroup
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `Sharing.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

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.

Assessment:

Ensure 'DisableHomeGroup' is 'Windows: Registry Value' to '1' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\HomeGroup:DisableHomeGroup          does not exist
```

References:

- **CCE-IDv5:** CCE-34776-5 -- More

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More
- **Control 14: Controlled Access Based on the Need to Know:** -- More

CIS Controls V6.1:

- **Control 14: Controlled Access Based on the Need to Know:** -- More

Back to Summary

18.9.36 Import Video

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

This Group Policy section is provided by the Group Policy template `CaptureWizard.admx/adml` that is only included with the Microsoft Windows Vista and Windows Server 2008 (non-R2) Administrative Templates.

18.9.37 Internet Explorer

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

This Group Policy section is provided by the Group Policy template `InetRes.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.38 Internet Information Services

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

This Group Policy section is provided by the Group Policy template `IIS.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.39 Location and Sensors

This section contains settings for Locations and Sensors.

This Group Policy section is provided by the Group Policy template `Sensors.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.9.39.1 Windows Location Provider

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

This Group Policy section is provided by the Group Policy template `LocationProviderAdm.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.9.40 Maintenance Scheduler

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

This Group Policy section is provided by the Group Policy template `msched.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.9.41 Maps

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

This Group Policy section is provided by the Group Policy template `WinMaps.admx/adml` that is included with the Microsoft Windows 10 Release 1511 Administrative Templates (or newer).

18.9.42 MDM

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

This Group Policy section is provided by the Group Policy template `MDM.admx/adml` that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

18.9.43 Messaging

This section contains messaging settings.

This Group Policy section is provided by the Group Policy template `Messaging.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

18.9.44 Microsoft account

This section contains recommendations related to Microsoft Accounts.

This Group Policy section is provided by the Group Policy template `MSAPolicy.admx/adml` that is included with the Microsoft Windows 10 Release 1703 Administrative Templates (or newer).

18.9.44.1 (L1) Ensure 'Block all consumer Microsoft account user authentication' is set to 'Enabled'

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft accounts\Block all
consumer Microsoft account user authentication
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MSAPolicy.admx/adml` that is included with the Microsoft Windows 10 Release 1703 Administrative Templates (or newer).

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.

Assessment:

Ensure 'DisableUserAuth' is 'Windows: Registry Value' to '1' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\MicrosoftAccount:DisableUserAuth        does not exist
```

References:

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

18.9.45 Microsoft Edge

This section contains recommendations related to the Microsoft Edge web browser, which is available in Windows 10.

This Group Policy section is provided by the Group Policy template MicrosoftEdge.admx/adml that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

18.9.45.4 (L1) Ensure 'Configure cookies' is set to 'Enabled: Block only 3rd-party cookies' or higher

Fail

Description:

This setting lets you configure how your company deals with cookies.

The recommended state for this setting is: Enabled: Block only 3rd-party cookies. Configuring this setting to Enabled: Block all cookies also conforms to the benchmark.

Rationale:

Cookies can pose a serious privacy concern, although many websites depend on them for operation. It is recommended when possible to block 3rd party cookies in order to reduce tracking.

Remediation:

To establish the recommended configuration via GP, set the following UI path to Enabled: Block only 3rd-party cookies (or, if applicable for your environment, Enabled: Block all cookies):

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Edge\Configure
cookies
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template MicrosoftEdge.admx/adml that is included with the Microsoft Windows 10 Release 1507 Administrative Templates (or newer).

Note #2: In the Microsoft Windows 10 Release 1507 Administrative Templates, this setting was named *Configure how Microsoft Edge treats cookies*, but it was renamed starting with the Windows 10 Release 1511 Administrative Templates.

Impact:

If you select "Block only 3rd-party cookies", cookies from 3rd-party websites will be blocked, but 1st-party website cookies will still be permitted. If you select "Block all cookies", cookies from all websites will be blocked.

Note: Blocking all cookies may interfere with functionality on some websites that depend on them for session tracking and/or login credentials.

Assessment:

Ensure 'Cookies' is 'Windows: Registry Value' to '1' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\MicrosoftEdge\Main:Cookies                          does not exist
```

References:

CIS Controls V6.1:

- **Control 13: Data Protection:** -- More

Back to Summary

18.9.45.5 (L1) Ensure 'Configure Password Manager' is set to 'Disabled'

Fail

Description:

This setting lets you decide whether employees can save their passwords locally, using Password Manager.

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

Rationale:

Using Password Manager can potentially makes it easier for an unauthorized user who gains access to the user’s desktop (including a coworker who sits down at a user’s desk soon after the user walks away and forgets to lock their workstation), to log in to sites as the user, without needing to know or enter the password.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Edge\Configure
Password Manager
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MicrosoftEdge.admx/adml` that is included with the Microsoft Windows 10 Release 1507 Administrative Templates (or newer).

Note #2: In the Microsoft Windows 10 Release 1507 Administrative Templates, this setting was named *Allows you to configure password manager*. In the Microsoft Windows 10 Release 1511 Administrative Templates, this setting was renamed to *Turn off Password Manager*, but it was finally renamed to *Configure Password Manager* starting with the Windows 10 Release 1607 & Server 2016 Administrative Templates.

Impact:

Employees will not be able to use Password Manager.

Assessment:

Ensure 'FormSuggest Passwords' is 'Windows: Registry Value' to 'no' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\MicrosoftEdge\Main:FormSuggest Passwords          does not exist
```

References:

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

18.9.45.8 (L1) Ensure 'Configure the Adobe Flash Click-to-Run setting' is set to 'Enabled'

Fail

Description:

This setting controls whether Adobe Flash (within the Microsoft Edge web browser) will require the user to click on the Flash element before the browser will display the Flash content.

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

Note: This setting will not manage Adobe Flash usage from other web browsers, so we recommend that each organization make a determining decision on how to manage (or whether to uninstall) Adobe Flash for other browsers on their systems.

Rationale:

Adobe Flash is a very insecure product and has been a frequent attack vector on the web. However, disabling it completely may not be a practical option for many organizations, as it is still used frequently on many websites. This feature at least makes Adobe Flash content "opt-in", so the user has to choose to click on each specific piece of Flash content before it will run.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Edge\Configure the
Adobe Flash Click-to-Run setting
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MicrosoftEdge.admx/adml` that is included with the Microsoft Windows 10 Release 1703 Administrative Templates (or newer).

Impact:

None - this is the default behavior.

Assessment:

Ensure 'FlashClickToRunMode' is 'Windows: Registry Value' to '1' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\MicrosoftEdge\Security:FlashClickToRunMode          does not exist
```

References:

CIS Controls V7.0:

- **Control 7: Email and Web Browser Protections:** -- More

CIS Controls V6.1:

- **Control 7: Email and Web Browser Protections:** -- More

Back to Summary

18.9.46 Microsoft FIDO Authentication

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

This Group Policy section is provided by the Group Policy template `FidoAuth.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

18.9.47 Microsoft Secondary Authentication Factor

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

This Group Policy section is provided by the Group Policy template `DeviceCredential.admx/adml` that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

18.9.48 Microsoft User Experience Virtualization

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

This Group Policy section is provided by the Group Policy template `UserExperienceVirtualization.admx/adml` that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

18.9.49 NetMeeting

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

This Group Policy section is provided by the Group Policy template `Conf.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.50 Network Access Protection

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

This Group Policy section is provided by the Group Policy template `NAPXPQec.admx/adml` that is only included with the Microsoft Windows Server 2008 (non-R2) through the Windows 8.1 Update & Server 2012 R2 Update Administrative Templates.

18.9.51 Network Projector

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

This Group Policy section is provided by the Group Policy template `NetworkProjection.admx/adml` that is only included with the Microsoft Windows Vista through the Windows 8.1 Update & Server 2012 R2 Update Administrative Templates.

18.9.52 OneDrive (formerly SkyDrive)

This section contains recommendations related to OneDrive.

The Group Policy settings contained within this section are provided by the Group Policy template `SkyDrive.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Note: This section was initially named *SkyDrive* but was renamed by Microsoft to *OneDrive* starting with the Microsoft

Windows 10 RTM (Release 1507) Administrative Templates.

18.9.52.1 (L1) Ensure 'Prevent the usage of OneDrive for file storage' is set to 'Enabled'

Pass

Description:

This policy setting lets you prevent apps and features from working with files on OneDrive using the Next Generation Sync Client.

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

Rationale:

Enabling this setting prevents users from accidentally (or intentionally) uploading confidential or sensitive corporate information to the OneDrive cloud service using the Next Generation Sync Client.

Note: This security concern applies to *any* cloud-based file storage application installed on a workstation, not just the one supplied with Windows.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\OneDrive\Prevent the usage
of OneDrive for file storage
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `SkyDrive.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer). However, we strongly recommend you only use the version included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer). Older versions of the templates had conflicting settings in different template files for both OneDrive & SkyDrive, until it was cleaned up properly in the above version.

Note #2: In older Microsoft Windows Administrative Templates, this setting was named *Prevent the usage of SkyDrive for file storage*, but it was renamed starting with the Windows 10 RTM (Release 1507) Administrative Templates.

Impact:

Users can't access OneDrive from the OneDrive app and file picker. Windows Store apps can't access OneDrive using the `WinRT` API. OneDrive doesn't appear in the navigation pane in File Explorer. OneDrive files aren't kept in sync with the cloud. Users can't automatically upload photos and videos from the camera roll folder.

Note: If your organization uses Office 365, be aware that this setting will prevent users from saving files to OneDrive/SkyDrive.

Note #2: If your organization has decided to implement **OneDrive for Business** and therefore needs to except itself from this recommendation, we highly suggest that you also obtain and utilize the `OneDrive.admx/adml` template that is bundled with the latest OneDrive client, as noted at this link (this template is not included with the Windows Administrative Templates). Two alternative OneDrive settings in particular from that template are worth your consideration:

- *Allow syncing OneDrive accounts for only specific organizations* - a computer-based setting that restricts OneDrive client connections to only **approved** tenant IDs.
- *Prevent users from synchronizing personal OneDrive accounts* - a user-based setting that prevents use of consumer OneDrive (i.e. non-business).

Assessment:

Ensure 'DisableFileSyncNGSC' is 'Windows: Registry Value' to '1' -- More

References:

- **CCE-IDv5:** CCE-33826-9 -- More

CIS Controls V6.1:

- **Control 13: Data Protection:** -- More

Back to Summary

18.9.53 Online Assistance

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

This Group Policy section is provided by the Group Policy template `HelpAndSupport.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.54 Password Synchronization

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

This Group Policy section is provided by the Group Policy template `PswdSync.admx/adml` that is only included with the Microsoft Windows Vista through the Windows 8.1 Update & Server 2012 R2 Update Administrative Templates.

18.9.55 Portable Operating System

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

This Group Policy section is provided by the Group Policy template `ExternalBoot.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.9.56 Presentation Settings

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

This Group Policy section is provided by the Group Policy template `MobilePCPresentationSettings.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.57 Push To Install

This section contains recommendations related to the Push To Install service.

This Group Policy section is provided by the Group Policy template `PushToInstall.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

18.9.58 Remote Desktop Services (formerly Terminal Services)

This section contains recommendations related to Remote Desktop Services.

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note: This section was initially named *Terminal Services* but was renamed by Microsoft to *Remote Desktop Services* starting with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates.

18.9.58.1 RD Licensing (formerly TS Licensing)

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

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note: This section was initially named *TS Licensing* but was renamed by Microsoft to *RD Licensing* starting with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates.

18.9.58.2 Remote Desktop Connection Client

This section contains recommendations for the Remote Desktop Connection Client.

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.58.2.1 RemoteFX USB Device Redirection

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

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.9.58.2.2 (L1) Ensure 'Do not allow passwords to be saved' is set to 'Enabled'

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop
Services\Remote Desktop Connection Client\Do not allow passwords to be saved
```

Note: This Group Policy path is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Impact:

The password saving checkbox will be disabled for Remote Desktop clients and users will not be able to save passwords.

Assessment:

Ensure 'DisablePasswordSaving' is 'Windows: Registry Value' to '1' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services:DisablePasswordSaving          does not exist
```

References:

- **CCE-IDv5:** CCE-34506-6 -- More

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

18.9.58.3 Remote Desktop Session Host (formerly Terminal Server)

This section contains recommendations for the Remote Desktop Session Host.

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note: This section was initially named *Terminal Server* but was renamed by Microsoft to *Remote Desktop Session Host* starting with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates.

18.9.58.3.1 Application Compatibility

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

This Group Policy section is provided by the Group Policy template `TerminalServer-Server.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.9.58.3.2 Connections

This section contains recommendations for Connections to the Remote Desktop Session Host.

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.58.3.3 Device and Resource Redirection

This section contains recommendations related to Remote Desktop Session Host Device and Resource Redirection.

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.58.3.3.2 (L1) Ensure 'Do not allow drive redirection' is set to 'Enabled'

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop
Services\Remote Desktop Session Host\Device and Resource Redirection\Do not allow drive redirection
```

Note: This Group Policy path is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

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.

Assessment:

Ensure 'fDisableCdm' is 'Windows: Registry Value' to '1' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services:fDisableCdm          does not exist
```

References:

- **CCE-IDv5:** CCE-34697-3 -- More

CIS Controls V6.1:

- **Control 13: Data Protection:** -- More

Back to Summary

18.9.58.3.4 Licensing

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

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.58.3.5 Printer Redirection

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

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.58.3.6 Profiles

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

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.58.3.7 RD Connection Broker (formerly TS Connection Broker)

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

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note: This section was initially named *TS Connection Broker* but was renamed by Microsoft to *RD Connection Broker* starting with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates.

18.9.58.3.8 Remote Session Environment

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

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.58.3.9 Security

This section contains recommendations related to Remote Desktop Session Host Security.

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.58.3.9.1 (L1) Ensure 'Always prompt for password upon connection' is set to 'Enabled'

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop
Services\Remote Desktop Session Host\Security\Always prompt for password upon connection
```

Note: This Group Policy path is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In the Microsoft Windows Vista Administrative Templates, this setting was named *Always prompt client for password upon connection*, but it was renamed starting with the Windows Server 2008 (non-R2) Administrative Templates.

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.

Assessment:

Ensure 'fPromptForPassword' is 'Windows: Registry Value' to '1' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services:fPromptForPassword     does not exist
```

References:

- **CCE-IDv5:** CCE-33960-6 -- More

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

18.9.58.3.9.2 (L1) Ensure 'Require secure RPC communication' is set to 'Enabled'

Fail

Description:

This policy setting allows you to specify whether Remote Desktop Services requires secure Remote Procedure Call (RPC) communication with all clients or allows unsecured communication.

You can use this policy setting to strengthen the security of RPC communication with clients by allowing only authenticated and encrypted requests.

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

Rationale:

Allowing unsecure RPC communication can exposes the server to man in the middle attacks and data disclosure attacks.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop
Services\Remote Desktop Session Host\Security\Require secure RPC communication
```

Note: This Group Policy path is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Impact:

Remote Desktop Services accepts requests from RPC clients that support secure requests, and does not allow unsecured communication with untrusted clients.

Assessment:

Ensure 'fEncryptRPCTraffic' is 'Windows: Registry Value' to '1' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\Terminal Services:fEncryptRPCTraffic          does not exist
```

References:

- **CCE-IDv5:** CCE-35723-6 -- More

CIS Controls V7.0:

- **Control 4: Controlled Use of Administrative Privileges:** -- More

CIS Controls V6.1:

- **Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers:** -- More

Back to Summary

18.9.58.3.9.3 (L1) Ensure 'Require use of specific security layer for remote (RDP) connections' is set to 'Enabled: SSL'

Fail

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 labelled *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.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop
Services\Remote Desktop Session Host\Security\Require use of specific security layer for remote (RDP)
connections
```

Note: This Group Policy path is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Impact:

TLS 1.0 will be required to authenticate to the RD Session Host server. If TLS is not supported, the connection fails.

Assessment:

Ensure 'SecurityLayer' is 'Windows: Registry Value' to '2' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services:SecurityLayer does not exist

References:

- **CCE-IDv5:** CCE-33025-8 -- More

CIS Controls V7.0:

- **Control 3: Continuous Vulnerability Management:** -- More

Back to Summary

18.9.58.3.9.4 (L1) Ensure 'Require user authentication for remote connections by using Network Level Authentication' is set to 'Enabled'

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop
Services\Remote Desktop Session Host\Security\Require user authentication for remote connections by
using Network Level Authentication
```

Note: This Group Policy path is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In the Microsoft Windows Vista Administrative Templates, this setting was initially named *Require user authentication using RDP 6.0 for remote connections*, but it was renamed starting with the Windows Server 2008 (non-R2) Administrative Templates.

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, and once successfully authenticated, pass the credential along to the 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.

Assessment:

Ensure 'UserAuthentication' is 'Windows: Registry Value' to '1' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services:UserAuthentication          does not exist
```

References:

- **CCE-IDv5:** CCE-35724-4 -- More

CIS Controls V7.0:

- **Control 3: Continuous Vulnerability Management:** -- More

Back to Summary

18.9.58.3.9.5 (L1) Ensure 'Set client connection encryption level' is set to 'Enabled: High Level'

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop
Services\Remote Desktop Session Host\Security\Set client connection encryption level
```

Note: This Group Policy path is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Impact:

None - this is the default behavior.

Assessment:

Ensure 'MinEncryptionLevel' is 'Windows: Registry Value' to '3' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services:MinEncryptionLevel        does not exist
```

References:

- **CCE-IDv5:** CCE-35578-4 -- More

CIS Controls V7.0:

- **Control 4: Controlled Use of Administrative Privileges:** -- More

CIS Controls V6.1:

- **Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers:** -- More

Back to Summary

18.9.58.3.10 Session Time Limits

This section contains recommendations related to Remote Desktop Session Host Session Time Limits.

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.58.3.11 Temporary folders

This section contains recommendations related to Remote Desktop Session Host Session Temporary folders.

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.58.3.11.1 (L1) Ensure 'Do not delete temp folders upon exit' is set to 'Disabled'

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop
Services\Remote Desktop Session Host\Temporary Folders\Do not delete temp folders upon exit
```

Note: This Group Policy path is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In older Microsoft Windows Administrative Templates, this setting was named *Do not delete temp folder upon exit*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

Impact:

None - this is the default behavior.

Assessment:

Ensure 'DeleteTempDirsOnExit' is 'Windows: Registry Value' to '1' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services:DeleteTempDirsOnExit          does not exist
```

References:

- **CCE-IDv5:** CCE-34136-2 -- More

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More

CIS Controls V6.1:

- **Control 14: Controlled Access Based on the Need to Know:** -- More

Back to Summary

18.9.58.3.11.2 (L1) Ensure 'Do not use temporary folders per session' is set to 'Disabled'

Fail

Description:

By default, Remote Desktop Services creates a separate temporary folder on the RD Session Host server for each active session that a user maintains on the RD Session Host server. The temporary folder is created on the RD Session Host server in a Temp folder under the user's profile folder and is named with the `sessionid`. This temporary folder is used to store individual temporary files.

To reclaim disk space, the temporary folder is deleted when the user logs off from a session.

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

Rationale:

Disabling this setting keeps the cached data independent for each session, both reducing the chance of problems from shared cached data between sessions, and keeping possibly sensitive data separate to each user session.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop
Services\Remote Desktop Session Host\Temporary Folders\Do not use temporary folders per session
```

Note: This Group Policy path is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Impact:

None - this is the default behavior.

Assessment:

Ensure 'PerSessionTempDir' is 'Windows: Registry Value' to '1' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\Terminal Services:PerSessionTempDir          does not exist
```

References:

- **CCE-IDv5:** CCE-34531-4 -- More

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More

CIS Controls V6.1:

- **Control 14: Controlled Access Based on the Need to Know:** -- More

Back to Summary

18.9.59 RSS Feeds

This section contains recommendations related to RSS feeds.

This Group Policy section is provided by the Group Policy template `InetRes.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.59.1 (L1) Ensure 'Prevent downloading of enclosures' is set to 'Enabled'

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\RSS Feeds\Prevent
downloading of enclosures
```

Note: This Group Policy path is provided by the Group Policy template `InetRes.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In older Microsoft Windows Administrative Templates, this setting was named *Turn off downloading of enclosures*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

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.

Assessment:

Ensure 'DisableEnclosureDownload' is 'Windows: Registry Value' to '1' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Feeds:DisableEnclosureDownload        does not exist
```

References:

- **CCE-IDv5:** CCE-34822-7 -- More

CIS Controls V7.0:

- **Control 7: Email and Web Browser Protections:** -- More

CIS Controls V6.1:

- **Control 7: Email and Web Browser Protections:** -- More

Back to Summary

18.9.60 Search

This section contains recommendations for Search settings.

This Group Policy section is provided by the Group Policy template `Search.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.60.1 OCR

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

This Group Policy section is provided by the Group Policy template `SearchOCR.admx/adml` that is only included with the Microsoft Windows 7 & Server 2008 R2 through the Windows 10 Release 1511 Administrative Templates.

18.9.60.3 (L1) Ensure 'Allow Cortana' is set to 'Disabled'

Fail

Description:

This policy setting specifies whether Cortana is allowed on the device.

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

Rationale:

If Cortana is enabled, sensitive information could be contained in search history and sent out to Microsoft.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Search\Allow Cortana
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `Search.admx/adml` that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

Impact:

Cortana will be turned off. Users will still be able to use search to find things on the device and on the Internet.

Assessment:

Ensure 'AllowCortana' is 'Windows: Registry Value' to '0' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Windows Search:AllowCortana                    does not exist
```

References:

- **CCE-IDv5:** CCE-41421-9 -- More

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

CIS Controls V6.1:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

Back to Summary

18.9.60.4 (L1) Ensure 'Allow Cortana above lock screen' is set to 'Disabled'

Fail

Description:

This policy setting determines whether or not the user can interact with Cortana using speech while the system is locked.

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

Rationale:

Access to any computer resource should not be allowed when the device is locked.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Search\Allow Cortana above
lock screen
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `Search.admx/adml` that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

Impact:

The system will need to be unlocked for the user to interact with Cortana using speech.

Assessment:

Ensure 'AllowCortanaAboveLock' is 'Windows: Registry Value' to '0' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Windows Search:AllowCortanaAboveLock          does not exist
```

References:

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

18.9.60.5 (L1) Ensure 'Allow indexing of encrypted files' is set to 'Disabled'

Fail

Description:

This policy setting controls whether encrypted items are allowed to be indexed. When this setting is changed, the index is rebuilt completely. Full volume encryption (such as BitLocker Drive Encryption or a non-Microsoft solution) must be used for the location of the index to maintain security for encrypted files.

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

Rationale:

Indexing and allowing users to search encrypted files could potentially reveal confidential data stored within the encrypted files.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Search\Allow indexing of
encrypted files
```

Note: This Group Policy path is provided by the Group Policy template `Search.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Impact:

None - this is the default behavior.

Assessment:

Ensure 'AllowIndexingEncryptedStoresOrItems' is 'Windows: Registry Value' to '0' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Windows Search:AllowIndexingEncryptedStoresOrItems        does not exist
```

References:

- **CCE-IDv5:** CCE-35314-4 -- More

CIS Controls V6.1:

- **Control 13: Data Protection:** -- More

Back to Summary

18.9.60.6 (L1) Ensure 'Allow search and Cortana to use location' is set to 'Disabled'

Fail

Description:

This policy setting specifies whether search and Cortana can provide location aware search and Cortana results.

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

Rationale:

In an enterprise managed environment, allowing Cortana and Search to have access to location data is unnecessary. Organizations likely do not want this information shared out.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Search\Allow search and
Cortana to use location
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `Search.admx/adml` that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

Impact:

Search and Cortana will not have access to location information.

Assessment:

Ensure 'AllowSearchToUseLocation' is 'Windows: Registry Value' to '0' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Windows Search:AllowSearchToUseLocation        does not exist
```

References:

- **CCE-IDv5:** CCE-41372-4 -- More

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

CIS Controls V6.1:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

Back to Summary

18.9.61 Security Center

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

This Group Policy section is provided by the Group Policy template `SecurityCenter.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.62 Server for NIS

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

This Group Policy section is provided by the Group Policy template `Snis.admx/adml` that is only included with the Microsoft Windows Vista through the Windows 8.1 Update & Server 2012 R2 Update Administrative Templates.

18.9.63 Shutdown Options

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

This Group Policy section is provided by the Group Policy template `WinInit.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.64 Smart Card

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

This Group Policy section is provided by the Group Policy template `SmartCard.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.65 Software Protection Platform

This section contains recommendations related to the Software Protection Platform.

This Group Policy section is provided by the Group Policy template `AVSValidationGP.admx/adml` that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

18.9.66 Sound Recorder

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

This Group Policy section is provided by the Group Policy template `SoundRec.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.67 Speech

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

This Group Policy section is provided by the Group Policy template `Speech.admx/adml` that is included with the Microsoft Windows 10 Release 1703 Administrative Templates (or newer).

18.9.68 Store

This section contains recommendations related to the Microsoft Store.

This Group Policy section is provided by the Group Policy template `WinStoreUI.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates, or by the Group Policy template

`WindowsStore.admx/adml` that is included with the Microsoft Windows 10 Release 1511 Administrative Templates (or newer).

18.9.68.2 (L1) Ensure 'Only display the private store within the Microsoft Store' is set to 'Enabled'

Fail

Description:

This policy setting denies access to the retail catalog in the Microsoft Store, but displays the private store.

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

Rationale:

Allowing the private store will allow an organization to control the apps that users have access to add to a system. This will help ensure that unapproved malicious apps are not running on a system.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Store\Only display the
private store within the Microsoft Store
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WindowsStore.admx/adml` that is included with the Microsoft Windows 10 Release 1607 Administrative Templates (or newer).

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Only display the private store within the Windows Store app*, but it was renamed starting with the Windows 10 Release 1803 Administrative Templates.

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.

Assessment:

Ensure 'RequirePrivateStoreOnly' is 'Windows: Registry Value' to '1' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsStore:RequirePrivateStoreOnly          does not exist
```

References:

CIS Controls V7.0:

- **Control 3: Continuous Vulnerability Management:** -- More
- **Control 3: Continuous Vulnerability Management:** -- More

Back to Summary

18.9.68.3 (L1) Ensure 'Turn off Automatic Download and Install of updates' is set to 'Disabled'

Fail

Description:

This setting enables or disables the automatic download and installation of Microsoft Store app updates.

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

Rationale:

Keeping your system properly patched can help protect against 0 day vulnerabilities.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Store\Turn off Automatic
Download and Install of updates
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WinStoreUI.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates, or by the Group Policy template `WindowsStore.admx/adml` that is included with the Microsoft Windows 10 Release 1511 Administrative Templates (or newer).

Impact:

None - this is the default behavior.

Assessment:

Ensure 'AutoDownload' is 'Windows: Registry Value' to '4' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsStore:AutoDownload does not exist

References:

- **CCE-IDv5:** CCE-35807-7 -- More

CIS Controls V7.0:

- **Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers:** -- More
- **Control 3: Continuous Vulnerability Management:** -- More
- **Control 3: Continuous Vulnerability Management:** -- More

CIS Controls V6.1:

- **Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers:** -- More
- **Control 4: Continuous Vulnerability Assessment and Remedia:** -- More

Back to Summary

18.9.68.4 (L1) Ensure 'Turn off the offer to update to the latest version of Windows' is set to 'Enabled'

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Store\Turn off the offer to
update to the latest version of Windows
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WinStoreUI.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates, or by the Group Policy template `WindowsStore.admx/adml` that is included with the Microsoft Windows 10 Release 1511 Administrative Templates (or newer).

Impact:

The Microsoft Store application will not offer updates to the latest version of Windows.

Assessment:

Ensure 'DisableOSUpgrade' is 'Windows: Registry Value' to '1' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsStore:DisableOSUpgrade does not exist

References:

- **CCE-IDv5:** CCE-35809-3 -- More

CIS Controls V7.0:

- **Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers:** -- More
- **Control 3: Continuous Vulnerability Management:** -- More
- **Control 3: Continuous Vulnerability Management:** -- More

CIS Controls V6.1:

- **Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers:** -- More
- **Control 4: Continuous Vulnerability Assessment and Remedia:** -- More

Back to Summary

18.9.69 Sync your settings

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

This Group Policy section is provided by the Group Policy template `SettingSync.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.9.70 Tablet PC

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

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.71 Task Scheduler

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

This Group Policy section is provided by the Group Policy template `TaskScheduler.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.72 Text Input

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

This Group Policy section is provided by the Group Policy template `TextInput.admx/adml` that is only included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates and Microsoft Windows 10 Release 1511 Administrative Templates.

18.9.73 Windows Calendar

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

This Group Policy section is provided by the Group Policy template `WinCal.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.74 Windows Color System

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

This Group Policy section is provided by the Group Policy template `WindowsColorSystem.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.75 Windows Customer Experience Improvement Program

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

This Group Policy section is provided by the Group Policy template `CEIPEnable.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.76 Windows Defender Antivirus (formerly Windows Defender)

This section contains recommendations related to Windows Defender Antivirus.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note: This section was originally named *Windows Defender* but was renamed by Microsoft to *Windows Defender Antivirus* starting with the Microsoft Windows 10 Release 1703 Administrative Templates.

18.9.76.1 Client Interface

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

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.9.76.2 Exclusions

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

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.9.76.3 MAPS

This section contains recommendations related to Microsoft Active Protection Service (MAPS).

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.9.76.3.1 (L1) Ensure 'Configure local setting override for reporting to Microsoft MAPS' is set to 'Disabled'

Fail

Description:

This policy setting configures a local override for the configuration to join Microsoft Active Protection Service (MAPS), which Microsoft has now renamed to "Windows 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 / Windows 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.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender
Antivirus\MAPS\Configure local setting override for reporting to Microsoft MAPS
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Impact:

None - this is the default behavior.

Assessment:

Ensure 'LocalSettingOverrideSpynetReporting' is 'Windows: Registry Value' to '0' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet:LocalSettingOverrideSpynetReporting        does not exist
```

References:

- **CCE-IDv5:** CCE-33833-5 -- More

CIS Controls V6.1:

- **Control 8: Malware Defenses:** -- More

Back to Summary

18.9.76.4 MpEngine

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

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 10 Release 1703 Administrative Templates (or newer).

18.9.76.5 Network Inspection System

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

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.9.76.6 Quarantine

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

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.9.76.7 Real-time Protection

This section contains settings related to Real-time Protection.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.9.76.7.1 (L1) Ensure 'Turn on behavior monitoring' is set to 'Enabled'

Fail

Description:

This policy setting allows you to configure behavior monitoring for Windows Defender Antivirus.

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

Rationale:

When running an antivirus solution such as Windows Defender Antivirus, it is important to ensure that it is configured to heuristically monitor in real-time for suspicious and known malicious activity.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender
Antivirus\Real-Time Protection\Turn on behavior monitoring
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Impact:

None - this is the default configuration.

Assessment:

Ensure 'DisableBehaviorMonitoring' is 'Windows: Registry Value' to '0' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection:DisableBehaviorMonitoring — does not exist

References:

- **CCE-IDv5:** CCE-33865-7 -- More

CIS Controls V7.0:

- **Control 8: Malware Defenses:** -- More
- **Control 8: Malware Defenses:** -- More

CIS Controls V6.1:

- **Control 8: Malware Defenses:** -- More

Back to Summary

18.9.76.8 Remediation

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

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.9.76.9 Reporting

This section contains settings related to Windows Defender Reporting.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.9.76.10 Scan

This section contains settings related to Windows Defender scanning.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.9.76.10.1 (L1) Ensure 'Scan removable drives' is set to 'Enabled'

Fail

Description:

This policy setting allows you to manage whether or not to scan for malicious software and unwanted software in the contents of removable drives, such as USB flash drives, when running a full scan.

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

Rationale:

It is important to ensure that any present removable drives are always included in any type of scan, as removable drives are more likely to contain malicious software brought in to the enterprise managed environment from an external, unmanaged computer.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender
Antivirus\Scan\Scan removable drives
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Impact:

Removable drives will be scanned during any type of scan by Windows Defender Antivirus.

Assessment:

Ensure 'DisableRemovableDriveScanning' is 'Windows: Registry Value' to '0' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Scan:DisableRemovableDriveScanning        does not exist
```

References:

- **CCE-IDv5:** CCE-33888-9 -- More

CIS Controls V6.1:

- **Control 13: Data Protection:** -- More

Back to Summary

18.9.76.10.2 (L1) Ensure 'Turn on e-mail scanning' is set to 'Enabled'

Fail

Description:

This policy setting allows you to configure e-mail scanning. When e-mail scanning is enabled, the engine will parse the mailbox and mail files, according to their specific format, in order to analyze the mail bodies and attachments. Several e-mail formats are currently supported, for example: pst (Outlook), dbx, mbx, mime (Outlook Express), binhex (Mac).

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

Rationale:

Incoming e-mails should be scanned by an antivirus solution such as Windows Defender Antivirus, as email attachments are a commonly used attack vector to infiltrate computers with malicious software.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender
Antivirus\Scan\Turn on e-mail scanning
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Impact:

E-mail scanning by Windows Defender Antivirus will be enabled.

Assessment:

Ensure 'DisableEmailScanning' is 'Windows: Registry Value' to '0' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Scan:DisableEmailScanning      does not exist
```

References:

- **CCE-IDv5:** CCE-33906-9 -- More

CIS Controls V6.1:

- **Control 13: Data Protection:** -- More

Back to Summary

18.9.76.11 Signature Updates

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

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.9.76.12 Threats

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

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.9.76.13 Windows Defender Exploit Guard

This section contains Windows Defender Exploit Guard settings.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

18.9.76.13.1 Attack Surface Reduction

This section contains Attack Surface Reduction settings.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.9.76.13.1.1 (L1) Ensure 'Configure Attack Surface Reduction rules' is set to 'Enabled'

Fail

Description:

This policy setting controls the state for the Attack Surface Reduction (ASR) rules.

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

Rationale:

Attack surface reduction helps prevent actions and apps that are typically used by exploit-seeking malware to infect machines.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender
Antivirus\Windows Defender Exploit Guard\Attack Surface Reduction\Configure Attack Surface Reduction
rules
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

Impact:

When a rule is triggered, a notification will be displayed from the Action Center.

Assessment:

Ensure 'ExploitGuard_ASR_Rules' is 'Windows: Registry Value' to '1' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR:ExploitGuard_ASR_Rules does not exist

References:

CIS Controls V7.0:

- **Control 8: Malware Defenses:** -- More

CIS Controls V6.1:

- **Control 8: Malware Defenses:** -- More

Back to Summary

18.9.76.13.1.2 (L1) Ensure 'Configure Attack Surface Reduction rules: Set the state for each ASR rule' is 'configured'

Fail

Description:

This policy setting sets the Attack Surface Reduction rules.

The recommended state for this setting is:

`26190899-1602-49e8-8b27-eb1d0a1ce869 - 1` (Block Office communication application from creating child processes)

`3b576869-a4ec-4529-8536-b80a7769e899 - 1` (Block Office applications from creating executable content)

`5beb7efe-fd9a-4556-801d-275e5ffc04cc - 1` (Block execution of potentially obfuscated scripts)

`75668c1f-73b5-4cf0-bb93-3ecf5cb7cc84 - 1` (Block Office applications from injecting code into other processes)

`7674ba52-37eb-4a4f-a9a1-f0f9a1619a2c - 1` (Block Adobe Reader from creating child processes)

`92e97fa1-2edf-4476-bdd6-9dd0b4dddc7b - 1` (Block Win32 API calls from Office macro)

`9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2 - 1` (Block credential stealing from the Windows local security authority subsystem (lsass.exe))

`b2b3f03d-6a65-4f7b-a9c7-1c7ef74a9ba4 - 1` (Block untrusted and unsigned processes that run from USB)

`be9ba2d9-53ea-4cdc-84e5-9b1eeee46550 - 1` (Block executable content from email client and webmail)

`d3e037e1-3eb8-44c8-a917-57927947596d - 1` (Block JavaScript or VBScript from launching downloaded executable content)

`d4f940ab-401b-4efc-aadc-ad5f3c50688a - 1` (Block Office applications from creating child processes)

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.

Remediation:

To establish the recommended configuration via GP, set the following UI path so that `26190899-1602-49e8-8b27-eb1d0a1ce869`, `3b576869-a4ec-4529-8536-b80a7769e899`, `5beb7efe-fd9a-4556-801d-275e5ffc04cc`, `75668c1f-73b5-4cf0-bb93-3ecf5cb7cc84`, `7674ba52-37eb-4a4f-a9a1-f0f9a1619a2c`, `92e97fa1-2edf-4476-bdd6-9dd0b4dddc7b`, `9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2`, `b2b3f03d-6a65-4f7b-a9c7-1c7ef74a9ba4`, `be9ba2d9-53ea-4cdc-84e5-9b1eeee46550`, `d3e037e1-3eb8-44c8-a917-57927947596d` and `d4f940ab-401b-4efc-aadc-ad5f3c50688a` are each set to a value of `1`:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender
Antivirus\Windows Defender Exploit Guard\Attack Surface Reduction\Configure Attack Surface Reduction
rules: Set the state for each ASR rule
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

Impact:

When a rule is triggered, a notification will be displayed from the Action Center.

Assessment:

All of the following tests or sub-groups must pass:

Ensure '75668c1f-73b5-4cf0-bb93-3ecf5cb7cc84' is 'Windows: Registry Value' to '1' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR \Rules:75668c1f-73b5-4cf0-bb93-3ecf5cb7cc84 does not exist

Ensure '5beb7efe-fd9a-4556-801d-275e5ffc04cc' is 'Windows: Registry Value' to '1' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR \Rules:5beb7efe-fd9a-4556-801d-275e5ffc04cc does not exist

Ensure '3b576869-a4ec-4529-8536-b80a7769e899' is 'Windows: Registry Value' to '1' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR \Rules:3b576869-a4ec-4529-8536-b80a7769e899 does not exist

Ensure '26190899-1602-49e8-8b27-eb1d0a1ce869' is 'Windows: Registry Value' to '1' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR \Rules:26190899-1602-49e8-8b27-eb1d0a1ce869 does not exist

Ensure 'd4f940ab-401b-4efc-aadc-ad5f3c50688a' is 'Windows: Registry Value' to '1' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR \Rules:d4f940ab-401b-4efc-aadc-ad5f3c50688a does not exist

Ensure 'd3e037e1-3eb8-44c8-a917-57927947596d' is 'Windows: Registry Value' to '1' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR \Rules:d3e037e1-3eb8-44c8-a917-57927947596d does not exist

Ensure 'be9ba2d9-53ea-4cdc-84e5-9b1eeee46550' is 'Windows: Registry Value' to '1' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules:be9ba2d9-53ea-4cdc-84e5-9b1eeee46550 does not exist

Ensure 'b2b3f03d-6a65-4f7b-a9c7-1c7ef74a9ba4' is 'Windows: Registry Value' to '1' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules:b2b3f03d-6a65-4f7b-a9c7-1c7ef74a9ba4 does not exist

Ensure '9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2' is 'Windows: Registry Value' to '1' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules:9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2 does not exist

Ensure '92e97fa1-2edf-4476-bdd6-9dd0b4dddc7b' is 'Windows: Registry Value' to '1' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules:92e97fa1-2edf-4476-bdd6-9dd0b4dddc7b does not exist

Ensure '7674ba52-37eb-4a4f-a9a1-f0f9a1619a2c' is 'Windows: Registry Value' to '1' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules:7674ba52-37eb-4a4f-a9a1-f0f9a1619a2c does not exist

References:

CIS Controls V7.0:

- **Control 8: Malware Defenses:** -- More

CIS Controls V6.1:

- **Control 8: Malware Defenses:** -- More

Back to Summary

18.9.76.13.2 Controlled Folder Access

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

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.9.76.13.3 Network Protection

This section contains Windows Network Protection settings.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

18.9.76.13.3.1 (L1) Ensure 'Prevent users and apps from accessing dangerous websites' is set to 'Enabled: Block'

Fail

Description:

This policy setting controls Windows Defender Exploit Guard network protection.

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

Rationale:

This setting can help prevent employees from using any application to access dangerous domains that may host phishing scams, exploit-hosting sites, and other malicious content on the Internet.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender
Antivirus\Windows Defender Exploit Guard\Network Protection\Prevent users and apps from accessing
dangerous websites
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

Impact:

Users and applications will not be able to access dangerous domains.

Assessment:

Ensure 'EnableNetworkProtection' is 'Windows: Registry Value' to '1' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\Network Protection:EnableNetworkProtection does not exist

References:

CIS Controls V6.1:

- **Control 7: Email and Web Browser Protections: --** More

Back to Summary

18.9.76.14 (L1) Ensure 'Turn off Windows Defender AntiVirus' is set to 'Disabled'

Fail

Description:

This policy setting turns off Windows Defender Antivirus. If the setting is configured to Disabled, Windows 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 Windows Defender Antivirus.

Organizations that choose to purchase a reputable 3rd-party antivirus solution may choose to exempt themselves from this recommendation in lieu of the commercial alternative.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender
Antivirus\Turn off Windows Defender AntiVirus
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Turn off Windows Defender*, but it was renamed starting with the Windows 10 Release 1703 Administrative Templates.

Impact:

None - this is the default behavior.

Assessment:

Ensure 'DisableAntiSpyware' is 'Windows: Registry Value' to '0' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender:DisableAntiSpyware                      does not exist
```

References:

- **CCE-IDv5:** CCE-33478-9 -- More

CIS Controls V7.0:

- **Control 8: Malware Defenses:** -- More
- **Control 8: Malware Defenses:** -- More

CIS Controls V6.1:

- **Control 8: Malware Defenses:** -- More

Back to Summary

18.9.77 Windows Defender Application Guard

This section contains settings related to Windows Defender Application Guard.

This Group Policy section is provided by the Group Policy template `AppHVSI.admx/adml` that is included with the Microsoft Windows 10 Release 1703 Administrative Templates (or newer).

18.9.78 Windows Defender Exploit Guard

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

This Group Policy section is provided by the Group Policy template `ExploitGuard.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

18.9.79 Windows Defender Security Center

This section contains Windows Defender Security Center settings.

This Group Policy section is provided by the Group Policy template `WindowsDefenderSecurityCenter.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

18.9.79.1 Account protection

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

This Group Policy section is provided by the Group Policy template `WindowsDefenderSecurityCenter.admx/adml` that is included with the Microsoft Windows 10 Release 1803 Administrative Templates (or newer).

18.9.79.2 App and browser protection

This section contains App and browser protection settings.

This Group Policy section is provided by the Group Policy template `WindowsDefenderSecurityCenter.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

18.9.79.2.1 (L1) Ensure 'Prevent users from modifying settings' is set to 'Enabled'

Fail

Description:

This policy setting prevent users from making changes to the Exploit protection settings area in the Windows Defender Security Center.

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

Rationale:

Only authorized IT staff should be able to make changes to the exploit protection settings in order to ensure the organizations specific configuration is not modified.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender Security
Center\App and browser protection\Prevent users from modifying settings
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WindowsDefenderSecurityCenter.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

Impact:

Local users cannot make changes in the Exploit protection settings area.

Assessment:

Ensure 'DisallowExploitProtectionOverride' is 'Windows: Registry Value' to '1' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender Security Center\App and Browser protection:DisallowExploitProtectionOverride does not exist

References:

CIS Controls V7.0:

- **Control 8: Malware Defenses:** -- More

CIS Controls V6.1:

- **Control 8: Malware Defenses:** -- More

Back to Summary

18.9.80 Windows Defender SmartScreen

This section contains Windows Defender SmartScreen settings.

This Group Policy section is provided by the Group Policy template `SmartScreen.admx/adml` that is included with the Microsoft Windows 10 Release 1703 Administrative Templates (or newer).

18.9.80.1 Explorer

This section contains recommendations for Explorer-related Windows Defender SmartScreen settings.

The Group Policy settings contained within this section are provided by the Group Policy template `WindowsExplorer.admx/adml` that is included with the Microsoft Windows 10 Release 1703 Administrative Templates (or newer).

18.9.80.1.1 (L1) Ensure 'Configure Windows Defender SmartScreen' is set to 'Enabled: Warn and prevent bypass'

Fail

Description:

This policy setting allows you to manage the behavior of Windows SmartScreen. Windows SmartScreen helps keep PCs safer by warning users before running unrecognized programs downloaded from the Internet. Some information is sent to Microsoft about files and programs run on PCs with this feature enabled.

The recommended state for this setting is: `Enabled: Warn and prevent bypass`.

Rationale:

Windows SmartScreen helps keep PCs safer by warning users before running unrecognized programs downloaded from the Internet. However, due to the fact that some information is sent to Microsoft about files and programs run on PCs some organizations may prefer to disable it.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender
SmartScreen\Explorer\Configure Windows Defender SmartScreen
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WindowsExplorer.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Configure Windows SmartScreen*, but it was renamed starting with the Windows 10 Release 1703 Administrative Templates.

Impact:

Users will be warned before they are allowed to run unrecognized programs downloaded from the Internet.

Assessment:

All of the following tests or sub-groups must pass:

Ensure 'ShellSmartScreenLevel' is 'Windows: Registry Value' to 'Block' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System:ShellSmartScreenLevel does not exist

Ensure 'EnableSmartScreen' is 'Windows: Registry Value' to '1' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\System:EnableSmartScreen does not exist

References:

- **CCE-IDv5:** CCE-34026-5 -- More

CIS Controls V6.1:

- **Control 2: Inventory of Authorized and Unauthorized Software:** -- More

Back to Summary

18.9.80.2 Microsoft Edge

This section contains recommendations for Microsoft Edge-related Windows Defender SmartScreen settings.

The Group Policy settings contained within this section are provided by the Group Policy template `SmartScreen.admx/adml` that is included with the Microsoft Windows 10 Release 1703 Administrative Templates (or newer).

18.9.80.2.1 (L1) Ensure 'Configure Windows Defender SmartScreen' is set to 'Enabled'

Fail

Description:

This setting lets you decide whether to turn on SmartScreen Filter. SmartScreen Filter provides warning messages to help protect your employees from potential phishing scams and malicious software.

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

Rationale:

SmartScreen serves an important purpose as it helps to warn users of possible malicious sites and files. Allowing users to turn off this setting can make the browser become more vulnerable to compromise.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender
SmartScreen\Microsoft Edge\Configure Windows Defender SmartScreen
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template

`MicrosoftEdge.admx/adml` that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

Note #2: In the Microsoft Windows 10 RTM (Release 1507) Administrative Templates, this setting was named *Allows you to configure SmartScreen*. In the Microsoft Windows 10 Release 1511 Administrative Templates, it was renamed to *Turn off the SmartScreen Filter*. In the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates, it was renamed again to *Configure SmartScreen Filter*. Finally, it was given its current name of *Configure Windows Defender SmartScreen* in the Windows 10 Release 1703 Administrative Templates.

Impact:

None - this is the default behavior.

Assessment:

Ensure 'EnabledV9' is 'Windows: Registry Value' to '1' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\MicrosoftEdge\PhishingFilter:EnabledV9 does not exist

References:

CIS Controls V6.1:

- **Control 2: Inventory of Authorized and Unauthorized Software:** -- More

Back to Summary

18.9.80.2.2 (L1) Ensure 'Prevent bypassing Windows Defender SmartScreen prompts for files' is set to 'Enabled'

Fail

Description:

This setting lets you decide whether employees can override the SmartScreen Filter warnings about downloading unverified files.

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

Rationale:

SmartScreen will warn an employee if a file is potentially malicious. Enabling this setting prevents these warnings from being bypassed.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender
SmartScreen\Microsoft Edge\Prevent bypassing Windows Defender SmartScreen prompts for files
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MicrosoftEdge.admx/adml` that is included with the Microsoft Windows 10 Release 1511 Administrative Templates (or newer).

Note #2: In the Microsoft Windows 10 Release 1511 Administrative Templates, this setting was named *Don't allow SmartScreen Filter warning overrides for unverified files*. In the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates, this setting was renamed to *Prevent bypassing SmartScreen prompts for files*. Finally, it was given its current name of *Prevent bypassing Windows Defender SmartScreen prompts for files* in the Windows 10

Release 1703 Administrative Templates.

Impact:

Employees will not be able to ignore SmartScreen Filter warnings on files, and they will be blocked from downloading unverified files (that are potentially malicious) that SmartScreen detects.

Assessment:

Ensure 'PreventOverrideAppRepUnknown' is 'Windows: Registry Value' to '1' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\MicrosoftEdge\PhishingFilter:PreventOverrideAppRepUnknown        does not exist
```

References:

CIS Controls V6.1:

- **Control 7: Email and Web Browser Protections:** -- More

Back to Summary

18.9.80.2.3 (L1) Ensure 'Prevent bypassing Windows Defender SmartScreen prompts for sites' is set to 'Enabled'

Fail

Description:

This setting lets you decide whether employees can override the SmartScreen Filter warnings about potentially malicious websites.

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

Rationale:

SmartScreen will warn an employee if a website is potentially malicious. Enabling this setting prevents these warnings from being bypassed.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender
SmartScreen\Microsoft Edge\Prevent bypassing Windows Defender SmartScreen prompts for sites
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `MicrosoftEdge.admx/adml` that is included with the Microsoft Windows 10 Release 1511 Administrative Templates (or newer).

Note #2: In the Microsoft Windows 10 Release 1511 Administrative Templates, this setting was named *Don't allow SmartScreen Filter warning overrides*. In the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates, this setting was renamed to *Prevent bypassing SmartScreen prompts for sites*. Finally, it was given its current name of *Prevent bypassing Windows Defender SmartScreen prompts for sites* in the Windows 10 Release 1703 Administrative Templates.

Impact:

Employees will not be able to ignore SmartScreen Filter warnings, and they will be blocked from going to potentially malicious websites that SmartScreen detects.

Assessment:

Ensure 'PreventOverride' is 'Windows: Registry Value' to '1' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\MicrosoftEdge\PhishingFilter:PreventOverride          does not exist
```

References:

CIS Controls V6.1:

- **Control 7: Email and Web Browser Protections:** -- More

Back to Summary

18.9.81 Windows Error Reporting

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

This Group Policy section is provided by the Group Policy template `ErrorReporting.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.82 Windows Game Recording and Broadcasting

This section contains settings for Windows Game Recording and Broadcasting.

This Group Policy section is provided by the Group Policy template `GameDVR.admx/adml` that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

18.9.82.1 (L1) Ensure 'Enables or disables Windows Game Recording and Broadcasting' is set to 'Disabled'

Fail

Description:

This setting enables or disables the Windows Game Recording and Broadcasting features.

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

Rationale:

If this setting is allowed users could record and broadcast session info to external sites which is a privacy concern.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Game Recording and
Broadcasting\Enables or disables Windows Game Recording and Broadcasting
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `GameDVR.admx/adml` that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

Impact:

Windows Game Recording will not be allowed.

Assessment:

Ensure 'AllowGameDVR' is 'Windows: Registry Value' to '0' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\GameDVR:AllowGameDVR                    does not exist
```

References:

CIS Controls V6.1:

- **Control 13: Data Protection:** -- More

Back to Summary

18.9.83 Windows Hello for Business (formerly Microsoft Passport for Work)

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

This Group Policy section is provided by the Group Policy template `Passport.admx/adml` that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

Note: This section was initially named *Microsoft Passport for Work* but was renamed by Microsoft to *Windows Hello for Business* starting with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates.

18.9.84 Windows Ink Workspace

This section contains recommendations related to the Windows Ink Workspace.

This Group Policy section is provided by the Group Policy template `WindowsInkWorkspace.admx/adml` that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

18.9.84.2 (L1) Ensure 'Allow Windows Ink Workspace' is set to 'Enabled: On, but disallow access above lock' OR 'Disabled' but not 'Enabled: On'

Fail

Description:

This policy setting determines whether Windows Ink items are allowed above the lock screen.

The recommended state for this setting is: `Enabled: On, but disallow access above lock` OR `Disabled`.

Rationale:

Allowing any apps to be accessed while system is locked is not recommended. If this feature is permitted, it should only be accessible once a user authenticates with the proper credentials.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: On, but disallow access above lock` OR `Disabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Ink Workspace\Allow
Windows Ink Workspace
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WindowsInkWorkspace.admx/adml` that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

Impact:

Windows Ink Workspace will not be permitted above the lock screen.

Assessment:

Any of the following tests or sub-groups may pass:

Ensure 'AllowWindowsInkWorkspace' is 'Windows: Registry Value' to '1' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsInkWorkspace:AllowWindowsInkWorkspace        does not exist
```

Ensure 'AllowWindowsInkWorkspace' is 'Windows: Registry Value' to '0' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsInkWorkspace:AllowWindowsInkWorkspace        does not exist
```

References:

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

18.9.85 Windows Installer

This section contains recommendations related to Windows Installer.

This Group Policy section is provided by the Group Policy template `MSI.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.85.1 (L1) Ensure 'Allow user control over installs' is set to 'Disabled'

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Installer\Allow user
control over installs
```

Note: This Group Policy path is provided by the Group Policy template `MSI.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In older Microsoft Windows Administrative Templates, this setting was named *Enable user control over installs*, but it was renamed starting with the Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

Impact:

None - this is the default behavior.

Assessment:

Ensure 'EnableUserControl' is 'Windows: Registry Value' to '0' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Installer:EnableUserControl does not exist

References:

- **CCE-IDv5:** CCE-35431-6 -- More

CIS Controls V6.1:

- **Control 5: Controlled Use of Administrative Privileges:** -- More

Back to Summary

18.9.85.2 (L1) Ensure 'Always install with elevated privileges' is set to 'Disabled'

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Installer\Always
install with elevated privileges
```

Note: This Group Policy path is provided by the Group Policy template `MSI.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Impact:

None - this is the default behavior.

Assessment:

Ensure 'AlwaysInstallElevated' is 'Windows: Registry Value' to '0' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Installer:AlwaysInstallElevated          does not exist
```

References:

- **CCE-IDv5:** CCE-35400-1 -- More

CIS Controls V6.1:

- **Control 5: Controlled Use of Administrative Privileges:** -- More

Back to Summary

18.9.86 Windows Logon Options

This section contains recommendations related to Windows Logon Options.

This Group Policy section is provided by the Group Policy template `WinLogon.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.86.1 (L1) Ensure 'Sign-in last interactive user automatically after a system-initiated restart' is set to 'Disabled'

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Logon
Options\Sign-in last interactive user automatically after a system-initiated restart
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WinLogon.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

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.

Assessment:

Ensure 'DisableAutomaticRestartSignOn' is 'Windows: Registry Value' to '1' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System:DisableAutomaticRestartSignOn does not exist

References:

- **CCE-IDv5:** CCE-33891-3 -- More

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

18.9.87 Windows Mail

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

This Group Policy section is provided by the Group Policy template `WindowsMail.admx/adml` that is only included with the Microsoft Windows Vista through the Windows 10 Release 1703 Administrative Templates.

18.9.88 Windows Media Center

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

This Group Policy section is provided by the Group Policy template `MediaCenter.admx/adml` that is only included with the Microsoft Windows Vista through Windows 10 Release 1511 Administrative Templates.

18.9.89 Windows Media Digital Rights Management

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

This Group Policy section is provided by the Group Policy template `WindowsMediaDRM.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.90 Windows Media Player

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

This Group Policy section is provided by the Group Policy template `WindowsMediaPlayer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.91 Windows Meeting Space

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

This Group Policy section is provided by the Group Policy template `WindowsCollaboration.admx/adml` that is only included with the Microsoft Windows Vista and Server 2008 (non-R2) Administrative Templates.

18.9.92 Windows Messenger

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

This Group Policy section is provided by the Group Policy template `WindowsMessenger.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.93 Windows Mobility Center

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

This Group Policy section is provided by the Group Policy template `MobilePCMobilityCenter.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.94 Windows Movie Maker

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

This Group Policy section is provided by the Group Policy template `MovieMaker.admx/adml` that is only included with the Microsoft Windows Vista and Server 2008 (non-R2) Administrative Templates.

18.9.95 Windows PowerShell

This section contains recommendations related to Windows PowerShell.

This Group Policy section is provided by the Group Policy template `PowerShellExecutionPolicy.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.9.95.1 (L1) Ensure 'Turn on PowerShell Script Block Logging' is set to 'Disabled'

Fail

Description:

This policy setting enables logging of all PowerShell script input to the Microsoft-Windows-PowerShell/Operational event log.

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

Note: In Microsoft's own hardening guidance, they recommend the opposite value, `Enabled`, because having this data logged improves investigations of PowerShell attack incidents. However, the default ACL on the PowerShell Operational log allows Interactive User (i.e. *any* logged on user) to read it, and therefore possibly expose passwords or other sensitive information to unauthorized users. If Microsoft locks down the default ACL on that log in the future (e.g. to restrict it only to Administrators), then we will revisit this recommendation in a future release.

Rationale:

There are potential risks of capturing passwords in the PowerShell logs. This setting should only be needed for debugging purposes, and not in normal operation, it is important to ensure this is set to `Disabled`.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows PowerShell\Turn on
PowerShell Script Block Logging
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `PowerShellExecutionPolicy.admx/adml` that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

Impact:

Logging of PowerShell script input is disabled.

Assessment:

Ensure 'EnableScriptBlockLogging' is 'Windows: Registry Value' to '0' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\PowerShell                      does not exist
\ScriptBlockLogging:EnableScriptBlockLogging
```

References:

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

18.9.95.2 (L1) Ensure 'Turn on PowerShell Transcription' is set to 'Disabled'

Fail

Description:

This Policy setting lets you capture the input and output of Windows PowerShell commands into text-based transcripts.

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

Rationale:

If this setting is enabled there is a risk that passwords could get stored in plain text in the `PowerShell_transcript` output file.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows PowerShell\Turn on
PowerShell Transcription
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `PowerShellExecutionPolicy.admx/adml` that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

Impact:

None - this is the default behavior.

Assessment:

Ensure 'EnableTranscripting' is 'Windows: Registry Value' to '0' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\PowerShell\Transcription:EnableTranscripting    does not exist
```

References:

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

18.9.96 Windows Reliability Analysis

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

This Group Policy section is provided by the Group Policy template `RacWmiProv.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.9.97 Windows Remote Management (WinRM)

This section contains recommendations related to Windows Remote Management (WinRM).

This Group Policy section is provided by the Group Policy template `WindowsRemoteManagement.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.97.1 WinRM Client

This section contains recommendations related to the Windows Remote Management (WinRM) client.

This Group Policy section is provided by the Group Policy template `WindowsRemoteManagement.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.97.1.1 (L1) Ensure 'Allow Basic authentication' is set to 'Disabled'

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management
(WinRM)\WinRM Client\Allow Basic authentication
```

Note: This Group Policy path is provided by the Group Policy template `WindowsRemoteManagement.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Impact:

None - this is the default behavior.

Assessment:

Ensure 'AllowBasic' (Client) is 'Windows: Registry Value' to '0' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WinRM\Client:AllowBasic does not exist

References:

- **CCE-IDv5:** CCE-35258-3 -- More

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

18.9.97.1.2 (L1) Ensure 'Allow unencrypted traffic' is set to 'Disabled'

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management
(WinRM)\WinRM Client\Allow unencrypted traffic
```

Note: This Group Policy path is provided by the Group Policy template `WindowsRemoteManagement.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Impact:

None - this is the default behavior.

Assessment:

Ensure 'AllowUnencryptedTraffic' is 'Windows: Registry Value' to '0' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WinRM\Client:AllowUnencryptedTraffic does not exist

References:

- **CCE-IDv5:** CCE-34458-0 -- More

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

18.9.97.1.3 (L1) Ensure 'Disallow Digest authentication' is set to 'Enabled'

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management
(WinRM)\WinRM Client\Disallow Digest authentication
```

Note: This Group Policy path is provided by the Group Policy template `WindowsRemoteManagement.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Impact:

The WinRM client will not use Digest authentication.

Assessment:

Ensure 'AllowDigest' is 'Windows: Registry Value' to '0' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WinRM\Client:AllowDigest                    does not exist
```

References:

- **CCE-IDv5:** CCE-34778-1 -- More

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

18.9.97.2 WinRM Service

This section contains recommendations related to the Windows Remote Management (WinRM) service.

This Group Policy section is provided by the Group Policy template `WindowsRemoteManagement.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.97.2.1 (L1) Ensure 'Allow Basic authentication' is set to 'Disabled'

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management
(WinRM)\WinRM Service\Allow Basic authentication
```

Note: This Group Policy path is provided by the Group Policy template `WindowsRemoteManagement.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Impact:

None - this is the default behavior.

Assessment:

Ensure 'AllowBasic' (Service) is 'Windows: Registry Value' to '0' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WinRM\Service:AllowBasic          does not exist
```

References:

- **CCE-IDv5:** CCE-34779-9 -- More

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

18.9.97.2.3 (L1) Ensure 'Allow unencrypted traffic' is set to 'Disabled'

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management
(WinRM)\WinRM Service\Allow unencrypted traffic
```

Note: This Group Policy path is provided by the Group Policy template `WindowsRemoteManagement.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Impact:

None - this is the default behavior.

Assessment:

Ensure 'AllowUnencryptedTraffic' is 'Windows: Registry Value' to '0' -- Less

```
CIS-CAT expected every collected registry item to exist on the target system, and found 0 items.
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WinRM\Service:AllowUnencryptedTraffic        does not exist
```

References:

- **CCE-IDv5:** CCE-35054-6 -- More

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

18.9.97.2.4 (L1) Ensure 'Disallow WinRM from storing RunAs credentials' is set to 'Enabled'

Fail

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.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management
(WinRM)\WinRM Service\Disallow WinRM from storing RunAs credentials
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WindowsRemoteManagement.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

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.

Assessment:

Ensure 'DisableRunAs' is 'Windows: Registry Value' to '1' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WinRM\Service:DisableRunAs                    does not exist
```

References:

- **CCE-IDv5:** CCE-35416-7 -- More

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

18.9.98 Windows Remote Shell

This section contains settings related to Windows Remote Shell (WinRS).

This Group Policy section is provided by the Group Policy template `WindowsRemoteShell.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.99 Windows SideShow

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

This Group Policy section is provided by the Group Policy template `SideShow.admx/adml` that is only included with the Microsoft Windows Vista Administrative Templates through Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

18.9.100 Windows System Resource Manager

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

This Group Policy section is provided by the Group Policy template `SystemResourceManager.admx/adml` that is only included with the Microsoft Windows Vista through Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

18.9.101 Windows Update

This section contains recommendations related to Windows Update.

This Group Policy section is provided by the Group Policy template `WindowsUpdate.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.101.1 Windows Update for Business (formerly Defer Windows Updates)

This section contains recommendations related to Windows Update for Business.

This Group Policy section is provided by the Group Policy template `WindowsUpdate.admx/adml` that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

Note: This section was initially named *Defer Windows Updates* but was renamed by Microsoft to *Windows Update for Business* starting with the Microsoft Windows 10 Release 1709 Administrative Templates.

18.9.101.1.1 (L1) Ensure 'Manage preview builds' is set to 'Enabled: Disable preview builds'

Fail

Description:

This policy setting determines whether users can access the Windows Insider Program controls in Settings -> Update and Security. These controls enable users to make their devices available for downloading and installing preview (beta) builds of Windows software.

The recommended state for this setting is: `Enabled: Disable preview builds`.

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.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update\Windows
Update for Business\Manage preview builds
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WindowsUpdate.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

Impact:

Preview builds are prevented from installing on the device.

Assessment:

All of the following tests or sub-groups must pass:

Ensure 'ManagePreviewBuildsPolicyValue' is 'Windows: Registry Value' to '0' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate:ManagePreviewBuildsPolicyValue does not exist

Ensure 'ManagePreviewBuilds' is 'Windows: Registry Value' to '1' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate:ManagePreviewBuilds does not exist

References:

CIS Controls V7.0:

- **Control 3: Continuous Vulnerability Management:** -- More

CIS Controls V6.1:

- **Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers:** -- More

Back to Summary

18.9.101.1.2 (L1) Ensure 'Select when Preview Builds and Feature Updates are received' is set to 'Enabled: Semi-Annual Channel, 180 or more days'

Fail

Description:

This policy setting determines the level of Preview Build or Feature Updates to receive, and when.

The Windows readiness level for each new Windows 10 Feature Update is classified in one of 5 categories, depending on your organizations level of comfort with receiving them:

- **Preview Build - Fast:** Devices set to this level will be the first to receive new builds of Windows with features not yet available to the general public. Select Fast to participate in identifying and reporting issues to Microsoft, and provide suggestions on new functionality.
- **Preview Build - Slow:** Devices set to this level receive new builds of Windows before they are available to the general public, but at a slower cadence than those set to Fast, and with changes and fixes identified in earlier builds.
- **Release Preview:** Receive builds of Windows just before Microsoft releases them to the general public.
- **Semi-Annual Channel (Targeted):** Receive feature updates when they are released to the general public.
- **Semi-Annual Channel:** Feature updates will arrive when they are declared Semi-Annual Channel. This usually occurs about 4 months after Semi-Annual Channel (Targeted), indicating that Microsoft, Independent Software Vendors (ISVs), partners and customer believe that the release is ready for broad deployment.

The recommended state for this setting is: `Enabled: Semi-Annual Channel, 180 or more 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

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:

Forcing new features without prior testing in your environment could cause software incompatibilities as well as introducing new bugs into the operating system. In an enterprise managed environment, it is generally preferred to delay Feature Updates until thorough testing and a deployment plan is in place. This recommendation delays the *automatic* installation of new features as long as possible.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: Semi-Annual Channel, 180 or more days`:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update\Windows
Update for Business\Select when Preview Builds and Feature Updates are received
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WindowsUpdate.admx/adml` that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Select when Feature Updates are received*, but it was renamed to *Select when Preview Builds and Feature Updates are received* starting with the Windows 10 Release 1709 Administrative Templates.

Impact:

Feature Updates will be delayed until 180 or more days after they are declared to have a Windows readiness level of "Semi-Annual Channel".

Assessment:

All of the following tests or sub-groups must pass:

Ensure 'BranchReadinessLevel' is 'Windows: Registry Value' to '32' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate:BranchReadinessLevel        does not exist
```

Ensure 'DeferFeatureUpdates' is 'Windows: Registry Value' to '1' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate:DeferFeatureUpdates         does not exist
```

Ensure 'DeferFeatureUpdatesPeriodInDays' is 'Windows: Registry Value' to '180' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate:DeferFeatureUpdatesPeriodInDays          does not exist
```

References:

CIS Controls V6.1:

- **Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers:** -- More

Back to Summary

18.9.101.1.3 (L1) Ensure 'Select when Quality Updates are received' is set to 'Enabled: 0 days'

Fail

Description:

This settings 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.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled:0 days`:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update\Windows
Update for Business\Select when Quality Updates are received
```

Note: This Group Policy path does not exist by default. An updated Group Policy template (`WindowsUpdate.admx/adml`) is required - it is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

Impact:

None - this is the default behavior.

Assessment:

All of the following tests or sub-groups must pass:

Ensure 'DeferQualityUpdatesPeriodInDays' is 'Windows: Registry Value' to '0' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate:DeferQualityUpdatesPeriodInDays        does not exist
```

Ensure 'DeferQualityUpdates' is 'Windows: Registry Value' to '1' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate:DeferQualityUpdates        does not exist
```

References:

CIS Controls V7.0:

- **Control 3: Continuous Vulnerability Management:** -- More
- **Control 3: Continuous Vulnerability Management:** -- More

CIS Controls V6.1:

- **Control 4: Continuous Vulnerability Assessment and Remedia:** -- More

Back to Summary

18.9.101.2 (L1) Ensure 'Configure Automatic Updates' is set to 'Enabled'

Pass

Description:

This policy setting specifies whether computers in your environment will receive security updates from Windows Update or WSUS. If you configure this policy setting to Enabled, the operating system will recognize when a network connection is available and then use the network connection to search Windows Update or your designated intranet site for updates that apply to them.

After you configure this policy setting to Enabled, select one of the following three options in the Configure Automatic Updates Properties dialog box to specify how the service will work:

- 2 - Notify for download and auto install *(Notify before downloading any updates)*
- 3 - Auto download and notify for install *(Download the updates automatically and notify when they are ready to be installed.) (Default setting)*
- 4 - Auto download and schedule the install *(Automatically download updates and install them on the schedule specified below.))*
- 5 - Allow local admin to choose setting *(Leave decision on above choices up to the local Administrators (Not Recommended))*

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

Note: The sub-setting "*Configure automatic updating:*" has 4 possible values – all of them are valid depending on specific organizational needs, however if feasible we suggest using a value of `4 - Auto download and schedule the install`. This suggestion is not a scored requirement.

Note #2: Organizations that utilize a 3rd-party solution for patching may choose to exempt themselves from this setting, and instead configure it to `Disabled` so that the native Windows Update mechanism does not interfere with the 3rd-party patching process.

Rationale:

Although each version of Windows is thoroughly tested before release, it is possible that problems will be discovered after the products are shipped. The Configure Automatic Updates setting can help you ensure that the computers in your environment will always have the most recent critical operating system updates and service packs installed.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update\Configure
Automatic Updates
```

Note: This Group Policy path is provided by the Group Policy template `WindowsUpdate.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Impact:

Critical operating system updates and service packs will be installed as necessary.

Assessment:

Ensure 'NoAutoUpdate' is 'Windows: Registry Value' to '0' -- More

References:

- **CCE-IDv5:** CCE-35111-4 -- More

CIS Controls V7.0:

- **Control 3: Continuous Vulnerability Management:** -- More
- **Control 3: Continuous Vulnerability Management:** -- More

CIS Controls V6.1:

- **Control 4: Continuous Vulnerability Assessment and Remedia:** -- More

Back to Summary

18.9.101.3 (L1) Ensure 'Configure Automatic Updates: Scheduled install day' is set to '0 - Every day'

Pass

Description:

This policy setting specifies when computers in your environment will receive security updates from Windows Update or WSUS.

The recommended state for this setting is: `0 - Every day`.

Note: This setting is only applicable if `4 - Auto download and schedule the install` is selected in Rule 18.9.101.2. 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.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `0 - Every day`:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update\Configure
Automatic Updates: Scheduled install day
```

Note: This Group Policy path is provided by the Group Policy template `WindowsUpdate.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Impact:

If `4 - Auto download and schedule the install` is selected in Rule 18.9.101.2, critical operating system updates and service packs will automatically download every day (at 3:00 A.M., by default).

Assessment:

Ensure 'ScheduledInstallDay' is 'Windows: Registry Value' to '0' -- More

References:

- **CCE-IDv5:** CCE-35111-4 -- More

CIS Controls V7.0:

- **Control 3: Continuous Vulnerability Management:** -- More
- **Control 3: Continuous Vulnerability Management:** -- More

CIS Controls V6.1:

- **Control 4: Continuous Vulnerability Assessment and Remedia:** -- More

Back to Summary

18.9.101.4 (L1) Ensure 'No auto-restart with logged on users for scheduled automatic updates installations' is set to 'Disabled'

Fail

Description:

This policy setting specifies that Automatic Updates will wait for computers to be restarted by the users who are logged on to them to complete a scheduled installation.

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

Note: This setting applies only when you configure Automatic Updates to perform scheduled update installations. If you configure the Configure Automatic Updates setting to Disabled, this setting has no effect.

Rationale:

Some security updates require that the computer be restarted to complete an installation. If the computer cannot restart automatically, then the most recent update will not completely install and no new updates will download to the computer until it is restarted. Without the auto-restart functionality, users who are not security-conscious may choose to indefinitely delay the restart, therefore keeping the computer in a less secure state.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update\No
auto-restart with logged on users for scheduled automatic updates installations
```

Note: This Group Policy path is provided by the Group Policy template `WindowsUpdate.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *No auto-restart for scheduled Automatic Updates installations*, but it was renamed starting with the Windows 7 & Server 2008 R2 Administrative Templates.

Impact:

None - this is the default behavior.

Assessment:

Ensure 'NoAutoRebootWithLoggedOnUsers' is 'Windows: Registry Value' to '0' -- Less

Check:	All Must Pass
Registry Key:	HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate\AU
Registry Value:	NoAutoRebootWithLoggedOnUsers

CIS-CAT Expected...	CIS-CAT Collected...
the registry key's *type* to be set to **reg_dword**	reg_dword
the registry key's *value* to be set to **0**	1

References:

- **CCE-IDv5:** CCE-33813-7 -- More

CIS Controls V7.0:

- **Control 3: Continuous Vulnerability Management:** -- More
- **Control 3: Continuous Vulnerability Management:** -- More

CIS Controls V6.1:

- **Control 4: Continuous Vulnerability Assessment and Remedia:** -- More

Back to Summary

19 Administrative Templates (User)

This section contains user-based recommendations from Group Policy Administrative Templates (ADMX).

19.1 Control Panel

This section contains recommendations for Control Panel settings.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.1.1 Add or Remove Programs

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

This Group Policy section is provided by the Group Policy template `AddRemovePrograms.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.1.2 Display

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

This Group Policy section is provided by the Group Policy template `ControlPanelDisplay.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.1.3 Personalization (formerly Desktop Themes)

This section contains recommendations for personalization settings.

This Group Policy section is provided by the Group Policy template `ControlPanelDisplay.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note: This section was initially named *Desktop Themes* but was renamed by Microsoft to *Personalization* starting with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates.

19.1.3.1 (L1) Ensure 'Enable screen saver' is set to 'Enabled'

Fail

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.

Remediation:

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

```
User Configuration\Policies\Administrative Templates\Control Panel\Personalization\Enable screen saver
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `ControlPanelDisplay.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Impact:

A screen saver runs, provided that the following two conditions hold: First, a valid screen saver on the client is specified through the *Force specific screen saver* setting (Rule 19.1.3.2) or through Control Panel on the client computer. Second, the *Screen saver timeout* setting (Rule 19.1.3.4) is set to a nonzero value through the setting or through Control Panel.

Assessment:

Ensure 'ScreenSaveActive' is 'Windows: Registry Value' to '1', -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_USERS\S-1-5-21-358118824-3846515562-1363085019-1040\Software\Policies\Microsoft\Windows\Control Panel\Desktop:ScreenSaveActive — does not exist

References:

- **CCE-IDv5:** CCE-33164-5 -- More

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

19.1.3.2 (L1) Ensure 'Force specific screen saver: Screen saver executable name' is set to 'Enabled: scrnsave.scr'

Fail

Description:

This policy setting specifies the screen saver for the user's desktop.

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

Note: If the specified screen saver is not installed on a computer to which this setting applies, the setting is ignored.

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.

Remediation:

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

```
User Configuration\Policies\Administrative Templates\Control Panel\Personalization\Force specific screen
saver
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `ControlPanelDisplay.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Impact:

The system displays the specified screen saver on the user's desktop. The drop-down list of screen savers in the Screen Saver dialog in the Personalization or Display Control Panel will be disabled, preventing users from changing the screen saver.

Assessment:

Ensure 'SCRNSAVE.EXE' is 'Windows: User Registry Value' to 'scrnsave.scr' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_USERS\S-1-5-21-358118824-3846515562-1363085019-1040\Software\Policies\Microsoft\Windows\Control Panel\Desktop:SCRNSAVE.EXE	does not exist

References:

- **CCE-IDv5:** CCE-33105-8 -- More

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

19.1.3.3 (L1) Ensure 'Password protect the screen saver' is set to 'Enabled'

Fail

Description:

This setting determines whether screen savers used on the computer are password protected.

The recommended state for this setting is: `Enabled`.

Rationale:

If a user forgets to lock their computer when they walk away, it is possible that a passerby will hijack it. Configuring a timed screen saver with password lock will help to protect against these hijacks.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
User Configuration\Policies\Administrative Templates\Control Panel\Personalization\Password protect the
screen saver
```

Note: This Group Policy path is provided by the Group Policy template `ControlPanelDisplay.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Impact:

All screen savers are password protected. The "Password protected" checkbox on the Screen Saver dialog in the Personalization or Display Control Panel will be disabled, preventing users from changing the password protection setting.

Assessment:

Ensure 'ScreenSaverIsSecure' is 'Windows:User Registry Value' to '1' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_USERS\S-1-5-21-358118824-3846515562-1363085019-1040\Software\Policies\Microsoft\Windows\Control
Panel\Desktop:ScreenSaverIsSecure                                                              does not exist
```

References:

- **CCE-IDv5:** CCE-32938-3 -- More

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

19.1.3.4 (L1) Ensure 'Screen saver timeout' is set to 'Enabled: 900 seconds or fewer, but not 0'

Fail

Description:

This setting specifies how much user idle time must elapse before the screen saver is launched.

The recommended state for this setting is: `Enabled: 900 seconds or fewer, but not 0`.

Note: This setting has no effect under the following circumstances:

- The wait time is set to zero.
- The "Enable Screen Saver" setting is disabled.
- A valid screen existing saver is not selected manually or via the "Screen saver executable name" setting

Rationale:

If a user forgets to lock their computer when they walk away, it is possible that a passerby will hijack it. Configuring a timed screen saver with password lock will help to protect against these hijacks.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: 900 or fewer, but not 0`:

```
User Configuration\Policies\Administrative Templates\Control Panel\Personalization\Screen saver timeout
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `ControlPanelDisplay.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Impact:

The screen saver will automatically activate when the computer has been left unattended for the amount of time specified, and the users will not be able to change the timeout value.

Assessment:

All of the following tests or sub-groups must pass:

Ensure 'ScreenSaveTimeOut' is 'Windows: User Registry Value' is less than or equal to '900' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_USERS\S-1-5-21-358118824-3846515562-1363085019-1040\Software\Policies\Microsoft\Windows\Control Panel\Desktop:ScreenSaveTimeOut does not exist

Ensure 'ScreenSaveTimeOut' is 'Windows: User Registry Value' not equal to '0' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_USERS\S-1-5-21-358118824-3846515562-1363085019-1040\Software\Policies\Microsoft\Windows\Control Panel\Desktop:ScreenSaveTimeOut does not exist

References:

- **CCE-IDv5:** CCE-33168-6 -- More

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

19.2 Desktop

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.3 Network

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.4 Shared Folders

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `SharedFolders.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.5 Start Menu and Taskbar

This section contains recommendations for Start Menu and Taskbar settings.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.5.1 Notifications

This section contains recommendations for Notification settings.

This Group Policy section is provided by the Group Policy template `WPN.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

19.5.1.1 (L1) Ensure 'Turn off toast notifications on the lock screen' is set to 'Enabled'

Fail

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.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
User Configuration\Policies\Administrative Templates\Start Menu and Taskbar\Notifications\Turn off toast
notifications on the lock screen
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WPN.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Impact:

Applications will not be able to raise toast notifications on the lock screen.

Assessment:

Ensure 'NoToastApplicationNotificationOnLockScreen' is 'Windows: User Registry Value' to '1' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_USERS\S-1-5-21-358118824-3846515562-1363085019-1040\Software\Policies\Microsoft\Windows\CurrentVersion      does not exist
\PushNotifications:NoToastApplicationNotificationOnLockScreen
```

References:

- **CCE-IDv5:** CCE-33727-9 -- More

CIS Controls V7.0:

- **Control 16: Account Monitoring and Control:** -- More

CIS Controls V6.1:

- **Control 16: Account Monitoring and Control:** -- More

Back to Summary

19.6 System

This section contains recommendations for System settings.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.6.1 Ctrl+Alt+Del Options

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `CtrlAltDel.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.6.2 Display

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Display.admx/adml` that is included with the Microsoft Windows 10 Release 1803 Administrative Templates (or newer).

19.6.3 Driver Installation

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `DeviceInstallation.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.6.4 Folder Redirection

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `FolderRedirection.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.6.5 Group Policy

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `GroupPolicy.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.6.6 Internet Communication Management

This section contains recommendations related to Internet Communication Management.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.6.6.1 Internet Communication settings

This section contains recommendations related to Internet Communication settings.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7 Windows Components

This section contains recommendations for Windows Component settings.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.1 Add features to Windows 8 / 8.1 / 10 (formerly Windows Anytime Upgrade)

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsAnytimeUpgrade.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Note: This section was initially named *Windows Anytime Upgrade* but was renamed by Microsoft to *Add features to Windows x* starting with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

19.7.2 App runtime

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `AppXRuntime.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

19.7.3 Application Compatibility

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `AppCompat.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.4 Attachment Manager

This section contains recommendations related to Attachment Manager.

This Group Policy section is provided by the Group Policy template `AttachmentManager.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.4.1 (L1) Ensure 'Do not preserve zone information in file attachments' is set to 'Disabled'

Fail

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.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
User Configuration\Policies\Administrative Templates\Windows Components\Attachment Manager\Do not
preserve zone information in file attachments
```

Note: This Group Policy path is provided by the Group Policy template `AttachmentManager.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Impact:

None - this is the default behavior.

Assessment:

Ensure 'SaveZoneInformation' is 'Windows: User Registry Value' to '2' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_USERS\S-1-5-21-358118824-3846515562-1363085019-1040\Software\Microsoft\Windows\CurrentVersion\Policies\Attachments:SaveZoneInformation does not exist

References:

- **CCE-IDv5:** CCE-34810-2 -- More

CIS Controls V6.1:

- **Control 7: Email and Web Browser Protections:** -- More

Back to Summary

19.7.4.2 (L1) Ensure 'Notify antivirus programs when opening attachments' is set to 'Enabled'

Fail

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.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
User Configuration\Policies\Administrative Templates\Windows Components\Attachment Manager\Notify
antivirus programs when opening attachments
```

Note: This Group Policy path is provided by the Group Policy template `AttachmentManager.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

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.

Assessment:

Ensure 'ScanWithAntiVirus' is 'Windows: User Registry Value' to '3' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_USERS\S-1-5-21-358118824-3846515562-1363085019-1040\Software\Microsoft\Windows\CurrentVersion\Policies\Attachments:ScanWithAntiVirus does not exist

References:

- **CCE-IDv5:** CCE-33799-8 -- More

CIS Controls V7.0:

- **Control 7: Email and Web Browser Protections:** -- More

CIS Controls V6.1:

- **Control 7: Email and Web Browser Protections:** -- More

Back to Summary

19.7.5 AutoPlay Policies

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `AutoPlay.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.6 Backup

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `UserDataBackup.admx/adml` that is included only with the Microsoft Windows Vista through Windows 8.0 & Server 2012 (non-R2) Administrative Templates, as well as the Microsoft Windows 10 RTM (Release 1507) and Windows 10 Release 1511 Administrative Templates.

19.7.7 Cloud Content

This section contains recommendations for Cloud Content.

This Group Policy section is provided by the Group Policy template `CloudContent.admx/adml` that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

19.7.7.1 (L1) Ensure 'Configure Windows spotlight on lock screen' is set to Disabled'

Fail

Description:

This policy setting lets you configure Windows Spotlight on the lock screen.

The recommended state for this setting is: `Disabled`.

Note: Per Microsoft TechNet, this policy setting only applies to Windows 10 Enterprise and Windows 10 Education editions.

Rationale:

Enabling this setting will help ensure your data is not shared with any third party. The Windows Spotlight feature collects data and uses that data to display suggested apps as well as images from the internet.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
User Configuration\Policies\Administrative Templates\Windows Components\Cloud Content\Configure Windows
spotlight on lock screen
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `CloudContent.admx/adml` that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

Impact:

Windows Spotlight will be turned off and users will no longer be able to select it as their lock screen.

Assessment:

Ensure 'ConfigureWindowsSpotlight' is 'Windows: User Registry Value' to '2' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_USERS\S-1-5-21-358118824-3846515562-1363085019-1040\Software\Policies\Microsoft\Windows \CloudContent:ConfigureWindowsSpotlight does not exist

References:

CIS Controls V6.1:

- **Control 13: Data Protection:** -- More

Back to Summary

19.7.7.2 (L1) Ensure 'Do not suggest third-party content in Windows spotlight' is set to 'Enabled'

Fail

Description:

This policy setting determines whether Windows will suggest apps and content from third-party software publishers.

The recommended state for this setting is: `Enabled`.

Rationale:

Enabling this setting will help ensure your data is not shared with any third party. The Windows Spotlight feature collects data and uses that data to display suggested apps as well as images from the internet.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
User Configuration\Policies\Administrative Templates\Windows Components\Cloud Content\Do not suggest
third-party content in Windows spotlight
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `CloudContent.admx/adml` that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

Impact:

Windows Spotlight on lock screen, Windows tips, Microsoft consumer features and other related features will no longer suggest apps and content from third-party software publishers. Users may still see suggestions and tips to make them more productive with Microsoft features and apps.

Assessment:

Ensure 'DisableThirdPartySuggestions' is 'Windows: User Registry Value' to '1' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_USERS\S-1-5-21-358118824-3846515562-1363085019-1040\Software\Policies\Microsoft\Windows \CloudContent:DisableThirdPartySuggestions does not exist

References:

CIS Controls V6.1:

- **Control 13: Data Protection:** -- More

Back to Summary

19.7.8 Credential User Interface

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `CredUI.admx/adml` that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

19.7.9 Data Collection and Preview Builds

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `DataCollection.admx/adml` that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

19.7.10 Desktop Gadgets

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Sidebar.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

19.7.11 Desktop Window Manager

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `DWM.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.12 Digital Locker

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `DigitalLocker.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.13 Edge UI

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `EdgeUI.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

19.7.14 File Explorer (formerly Windows Explorer)

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note: This section was initially named *Windows Explorer* but was renamed by Microsoft to *File Explorer* starting with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

19.7.15 File Revocation

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `FileRevocation.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

19.7.16 IME

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `EAIME.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

19.7.17 Import Video

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `CaptureWizard.admx/adml` that is only included with the Microsoft Windows Vista and Windows Server 2008 (non-R2) Administrative Templates.

19.7.18 Instant Search

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WordWheel.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.19 Internet Explorer

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `InetRes.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.20 Location and Sensors

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Sensors.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

19.7.21 Microsoft Edge

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `MicrosoftEdge.admx/adml` that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

19.7.22 Microsoft Management Console

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `MMC.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.23 Microsoft User Experience Virtualization

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `UserExperienceVirtualization.admx/adml` that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

19.7.24 NetMeeting

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Conf.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.25 Network Projector

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `NetworkProjection.admx/adml` that is only included with the Microsoft Windows Vista through the Windows 8.1 Update & Server 2012 R2 Update Administrative Templates.

19.7.26 Network Sharing

This section contains recommendations related to Network Sharing.

This Group Policy section is provided by the Group Policy template `Sharing.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.26.1 (L1) Ensure 'Prevent users from sharing files within their profile.' is set to 'Enabled'

Fail

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.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
User Configuration\Policies\Administrative Templates\Windows Components\Network Sharing\Prevent users
from sharing files within their profile.
```

Note: This Group Policy path is provided by the Group Policy template `Sharing.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

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.

Assessment:

Ensure 'NoInplaceSharing' is 'Windows: User Registry Value' to '1' -- Less

CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.

HKEY_USERS\S-1-5-21-358118824-3846515562-1363085019-1040\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer:NoInplaceSharing does not exist

References:

- **CCE-IDv5:** CCE-33490-4 -- More

CIS Controls V7.0:

- **Control 14: Controlled Access Based on the Need to Know:** -- More

CIS Controls V6.1:

- **Control 14: Controlled Access Based on the Need to Know:** -- More

Back to Summary

19.7.27 Presentation Settings

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `MobilePCPresentationSettings.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.28 Remote Desktop Services (formerly Terminal Services)

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note: This section was initially named *Terminal Services* but was renamed by Microsoft to *Remote Desktop Services* starting with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates.

19.7.29 RSS Feeds

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `InetRes.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.30 Search

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Search.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

19.7.31 Sound Recorder

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `SoundRec.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.32 Store

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WinStoreUI.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates and Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates, or by the Group Policy template `WindowsStore.admx/adml` that is included with the Microsoft Windows 10 Release 1511 Administrative Templates (or newer).

19.7.33 Tablet PC

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.34 Task Scheduler

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `TaskScheduler.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.35 Windows Calendar

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WinCal.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.36 Windows Color System

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsColorSystem.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.37 Windows Defender SmartScreen

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `SmartScreen.admx/adml` that is included with the Microsoft Windows 10 Release 1703 Administrative Templates (or newer).

19.7.38 Windows Error Reporting

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `ErrorReporting.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.39 Windows Hello for Business (formerly Microsoft Passport for Work)

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `Passport.admx/adml` that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

Note: This section was initially named *Microsoft Passport for Work* but was renamed by Microsoft to *Windows Hello for Business* starting with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates.

19.7.40 Windows Installer

This section contains recommendations related to Windows Installer.

This Group Policy section is provided by the Group Policy template `MSI.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.40.1 (L1) Ensure 'Always install with elevated privileges' is set to 'Disabled'

Fail

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.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
User Configuration\Policies\Administrative Templates\Windows Components\Windows Installer\Always install
with elevated privileges
```

Note: This Group Policy path is provided by the Group Policy template `MSI.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Impact:

None - this is the default behavior.

Assessment:

Ensure 'AlwaysInstallElevated' is 'Windows: User Registry Value' to '0' -- Less

```
CIS-CAT expected at least 1 matching registry item to be collected, and found 0 items.
HKEY_USERS\S-1-5-21-358118824-3846515562-1363085019-1040\Software\Policies\Microsoft\Windows
\Installer:AlwaysInstallElevated                                                      does not exist
```

References:

- **CCE-IDv5:** CCE-34788-0 -- More

CIS Controls V6.1:

- **Control 5: Controlled Use of Administrative Privileges:** -- More

Back to Summary

19.7.41 Windows Logon Options

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WinLogon.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.42 Windows Mail

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsMail.admx/adml` that is only included with the Microsoft Windows Vista through the Windows 10 Release 1703 Administrative Templates.

19.7.43 Windows Media Center

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `MediaCenter.admx/adml` that is only included with the Microsoft Windows Vista through Windows 10 Release 1511 Administrative Templates.

19.7.44 Windows Media Player

This section contains recommendations related to Windows Media Player.

This Group Policy section is provided by the Group Policy template `WindowsMediaPlayer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.44.1 Networking

This section is intentionally blank and exists to ensure the structure of Windows benchmarks is consistent.

This Group Policy section is provided by the Group Policy template `WindowsMediaPlayer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.44.2 Playback

This section contains recommendations related to Windows Media Player playback.

This Group Policy section is provided by the Group Policy template `WindowsMediaPlayer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

⇧