CIS Benchmarks

Security Configuration Assessment Report for DESKTOP-JGURJJH

Target IP Address: 10.0.2.15

CIS Microsoft Windows 10 Enterprise Benchmark v4.0.0

Level 1 (L1)
Tuesday, August 12 2025 18:08:19
Assessment Duration: 2 minutes, 30 seconds

Report generated by the Center for Internet Security's Configuration Assessment Tool (CIS-CAT Pro Assessor) v4.56.0.
For further information, please visit The Center for Internet Security or our Product Support page.

Content generated on 08/12/2025 18:10 PM. Content last obtained on 07/28/2025 16:08 PM.

Summary

Description	Tests						Scoring		
	Pass	Fail	Error	Unkn.	Man.	Exc.	Score	Max	Percent
1 Account Policies	**4**	**6**	**0**	**0**	**1**	**0**	**4.0**	**10.0**	**40%**
1.1 Password Policy	2	5	0	0	0	0	2.0	7.0	29%
1.2 Account Lockout Policy	2	1	0	0	1	0	2.0	3.0	67%
2 Local Policies	**67**	**31**	**0**	**0**	**1**	**0**	**67.0**	**98.0**	**68%**
2.1 Audit Policy	0	0	0	0	0	0	0.0	0.0	0%
2.2 User Rights Assignment	27	10	0	0	0	0	27.0	37.0	73%
2.3 Security Options	40	21	0	0	1	0	40.0	61.0	66%
2.3.1 Accounts	2	3	0	0	0	0	2.0	5.0	40%
2.3.2 Audit	1	1	0	0	0	0	1.0	2.0	50%
2.3.3 DCOM	0	0	0	0	0	0	0.0	0.0	0%
2.3.4 Devices	0	0	0	0	0	0	0.0	0.0	0%
2.3.5 Domain controller	0	0	0	0	0	0	0.0	0.0	0%
2.3.6 Domain member	6	0	0	0	0	0	6.0	6.0	100%
2.3.7 Interactive logon	4	3	0	0	0	0	4.0	7.0	57%
2.3.8 Microsoft network client	2	1	0	0	0	0	2.0	3.0	67%
2.3.9 Microsoft network server	4	1	0	0	0	0	4.0	5.0	80%
2.3.10 Network access	10	2	0	0	0	0	10.0	12.0	83%
2.3.11 Network security	3	8	0	0	1	0	3.0	11.0	27%
2.3.12 Recovery console	0	0	0	0	0	0	0.0	0.0	0%
2.3.13 Shutdown	0	0	0	0	0	0	0.0	0.0	0%
2.3.14 System cryptography	0	0	0	0	0	0	0.0	0.0	0%
2.3.15 System objects	2	0	0	0	0	0	2.0	2.0	100%
2.3.16 System settings	0	0	0	0	0	0	0.0	0.0	0%
2.3.17 User Account Control	6	2	0	0	0	0	6.0	8.0	75%
3 Event Log	**0**	**0**	**0**	**0**	**0**	**0**	**0.0**	**0.0**	**0%**
4 Restricted Groups	**0**	**0**	**0**	**0**	**0**	**0**	**0.0**	**0.0**	**0%**
5 System Services	**11**	**10**	**0**	**0**	**0**	**0**	**11.0**	**21.0**	**52%**
6 Registry	**0**	**0**	**0**	**0**	**0**	**0**	**0.0**	**0.0**	**0%**
7 File System	**0**	**0**	**0**	**0**	**0**	**0**	**0.0**	**0.0**	**0%**
8 Wired Network (IEEE 802.3) Policies	**0**	**0**	**0**	**0**	**0**	**0**	**0.0**	**0.0**	**0%**
9 Windows Defender Firewall with Advanced Security (formerly Windows Firewall with Advanced Security)	**0**	**23**	**0**	**0**	**0**	**0**	**0.0**	**23.0**	**0%**
9.1 Domain Profile	0	7	0	0	0	0	0.0	7.0	0%
9.2 Private Profile	0	7	0	0	0	0	0.0	7.0	0%
9.3 Public Profile	0	9	0	0	0	0	0.0	9.0	0%
10 Network List Manager Policies	**0**	**0**	**0**	**0**	**0**	**0**	**0.0**	**0.0**	**0%**
11 Wireless Network (IEEE 802.11) Policies	**0**	**0**	**0**	**0**	**0**	**0**	**0.0**	**0.0**	**0%**
12 Public Key Policies	**0**	**0**	**0**	**0**	**0**	**0**	**0.0**	**0.0**	**0%**
13 Software Restriction Policies	**0**	**0**	**0**	**0**	**0**	**0**	**0.0**	**0.0**	**0%**
14 Network Access Protection NAP Client Configuration	**0**	**0**	**0**	**0**	**0**	**0**	**0.0**	**0.0**	**0%**
15 Application Control Policies	**0**	**0**	**0**	**0**	**0**	**0**	**0.0**	**0.0**	**0%**
16 IP Security Policies	**0**	**0**	**0**	**0**	**0**	**0**	**0.0**	**0.0**	**0%**
17 Advanced Audit Policy Configuration	**13**	**14**	**0**	**0**	**0**	**0**	**13.0**	**27.0**	**48%**
17.1 Account Logon	1	0	0	0	0	0	1.0	1.0	100%
17.2 Account Management	3	0	0	0	0	0	3.0	3.0	100%
17.3 Detailed Tracking	1	1	0	0	0	0	1.0	2.0	50%
17.4 DS Access	0	0	0	0	0	0	0.0	0.0	0%
17.5 Logon/Logoff	3	3	0	0	0	0	3.0	6.0	50%
17.6 Object Access	0	4	0	0	0	0	0.0	4.0	0%
17.7 Policy Change	2	3	0	0	0	0	2.0	5.0	40%
17.8 Privilege Use	0	1	0	0	0	0	0.0	1.0	0%
17.9 System	3	2	0	0	0	0	3.0	5.0	60%
18 Administrative Templates (Computer)	**13**	**169**	**0**	**0**	**0**	**0**	**13.0**	**182.0**	**7%**
18.1 Control Panel	0	3	0	0	0	0	0.0	3.0	0%
18.1.1 Personalization	0	2	0	0	0	0	0.0	2.0	0%
18.1.2 Regional and Language Options	0	1	0	0	0	0	0.0	1.0	0%
18.1.2.1 Handwriting personalization	0	0	0	0	0	0	0.0	0.0	0%
18.2 Desktop	0	0	0	0	0	0	0.0	0.0	0%
18.3 LAPS (legacy)	0	0	0	0	0	0	0.0	0.0	0%
18.4 MS Security Guide	0	8	0	0	0	0	0.0	8.0	0%
18.5 MSS (Legacy)	3	5	0	0	0	0	3.0	8.0	38%
18.6 Network	4	7	0	0	0	0	4.0	11.0	36%
18.6.1 Background Intelligent Transfer Service (BITS)	0	0	0	0	0	0	0.0	0.0	0%

Description	Tests						Scoring		
	Pass	Fail	Error	Unkn.	Man.	Exc.	Score	Max	Percent
18.6.2 BranchCache	0	0	0	0	0	0	0.0	0.0	0%
18.6.3 DirectAccess Client Experience Settings	0	0	0	0	0	0	0.0	0.0	0%
18.6.4 DNS Client	0	3	0	0	0	0	0.0	3.0	0%
18.6.5 Fonts	0	0	0	0	0	0	0.0	0.0	0%
18.6.6 Hotspot Authentication	0	0	0	0	0	0	0.0	0.0	0%
18.6.7 Lanman Server	0	0	0	0	0	0	0.0	0.0	0%
18.6.8 Lanman Workstation	0	1	0	0	0	0	0.0	1.0	0%
18.6.9 Link-Layer Topology Discovery	0	0	0	0	0	0	0.0	0.0	0%
18.6.10 Microsoft Peer-to-Peer Networking Services	0	0	0	0	0	0	0.0	0.0	0%
18.6.10.1 Peer Name Resolution Protocol	0	0	0	0	0	0	0.0	0.0	0%
18.6.11 Network Connections	3	0	0	0	0	0	3.0	3.0	100%
18.6.11.1 Windows Defender Firewall (formerly Windows Firewall)	0	0	0	0	0	0	0.0	0.0	0%
18.6.12 Network Connectivity Status Indicator	0	0	0	0	0	0	0.0	0.0	0%
18.6.13 Network Isolation	0	0	0	0	0	0	0.0	0.0	0%
18.6.14 Network Provider	0	1	0	0	0	0	0.0	1.0	0%
18.6.15 Offline Files	0	0	0	0	0	0	0.0	0.0	0%
18.6.16 QoS Packet Scheduler	0	0	0	0	0	0	0.0	0.0	0%
18.6.17 SNMP	0	0	0	0	0	0	0.0	0.0	0%
18.6.18 SSL Configuration Settings	0	0	0	0	0	0	0.0	0.0	0%
18.6.19 TCPIP Settings	0	0	0	0	0	0	0.0	0.0	0%
18.6.19.1 IPv6 Transition Technologies	0	0	0	0	0	0	0.0	0.0	0%
18.6.19.2 Parameters	0	0	0	0	0	0	0.0	0.0	0%
18.6.20 Windows Connect Now	0	0	0	0	0	0	0.0	0.0	0%
18.6.21 Windows Connection Manager	1	1	0	0	0	0	1.0	2.0	50%
18.6.22 Wireless Display	0	0	0	0	0	0	0.0	0.0	0%
18.6.23 WLAN Service	0	1	0	0	0	0	0.0	1.0	0%
18.6.23.1 WLAN Media Cost	0	0	0	0	0	0	0.0	0.0	0%
18.6.23.2 WLAN Settings	0	1	0	0	0	0	0.0	1.0	0%
18.7 Printers	0	12	0	0	0	0	0.0	12.0	0%
18.8 Start Menu and Taskbar	0	0	0	0	0	0	0.0	0.0	0%
18.8.1 Notifications	0	0	0	0	0	0	0.0	0.0	0%
18.9 System	1	38	0	0	0	0	1.0	39.0	3%
18.9.1 Access-Denied Assistance	0	0	0	0	0	0	0.0	0.0	0%
18.9.2 App-V	0	0	0	0	0	0	0.0	0.0	0%
18.9.3 Audit Process Creation	0	1	0	0	0	0	0.0	1.0	0%
18.9.4 Credentials Delegation	0	2	0	0	0	0	0.0	2.0	0%
18.9.5 Device Guard	0	0	0	0	0	0	0.0	0.0	0%
18.9.6 Device Health Attestation Service	0	0	0	0	0	0	0.0	0.0	0%
18.9.7 Device Installation	0	1	0	0	0	0	0.0	1.0	0%
18.9.7.1 Device Installation Restrictions	0	0	0	0	0	0	0.0	0.0	0%
18.9.8 Disk NV Cache	0	0	0	0	0	0	0.0	0.0	0%
18.9.9 Disk Quotas	0	0	0	0	0	0	0.0	0.0	0%
18.9.10 Display	0	0	0	0	0	0	0.0	0.0	0%
18.9.11 Distributed COM	0	0	0	0	0	0	0.0	0.0	0%
18.9.12 Driver Installation	0	0	0	0	0	0	0.0	0.0	0%
18.9.13 Early Launch Antimalware	0	1	0	0	0	0	0.0	1.0	0%
18.9.14 Enhanced Storage Access	0	0	0	0	0	0	0.0	0.0	0%
18.9.15 File Classification Infrastructure	0	0	0	0	0	0	0.0	0.0	0%
18.9.16 File Share Shadow Copy Provider	0	0	0	0	0	0	0.0	0.0	0%
18.9.17 Filesystem (formerly NTFS Filesystem)	0	0	0	0	0	0	0.0	0.0	0%
18.9.18 Folder Redirection	0	0	0	0	0	0	0.0	0.0	0%
18.9.19 Group Policy	1	5	0	0	0	0	1.0	6.0	17%
18.9.19.1 Logging and tracing	0	0	0	0	0	0	0.0	0.0	0%
18.9.20 Internet Communication Management	0	2	0	0	0	0	0.0	2.0	0%
18.9.20.1 Internet Communication settings	0	2	0	0	0	0	0.0	2.0	0%
18.9.21 iSCSI	0	0	0	0	0	0	0.0	0.0	0%
18.9.22 KDC	0	0	0	0	0	0	0.0	0.0	0%
18.9.23 Kerberos	0	0	0	0	0	0	0.0	0.0	0%
18.9.24 Kernel DMA Protection	0	0	0	0	0	0	0.0	0.0	0%
18.9.25 LAPS	0	8	0	0	0	0	0.0	8.0	0%
18.9.26 Local Security Authority	0	1	0	0	0	0	0.0	1.0	0%
18.9.27 Locale Services	0	0	0	0	0	0	0.0	0.0	0%
18.9.28 Logon	0	7	0	0	0	0	0.0	7.0	0%
18.9.29 Mitigation Options	0	0	0	0	0	0	0.0	0.0	0%
18.9.30 Net Logon	0	0	0	0	0	0	0.0	0.0	0%
18.9.31 OS Policies	0	0	0	0	0	0	0.0	0.0	0%
18.9.32 PIN Complexity	0	0	0	0	0	0	0.0	0.0	0%

Description	Tests						Scoring		
	Pass	Fail	Error	Unkn.	Man.	Exc.	Score	Max	Percent
18.9.33 Power Management	0	4	0	0	0	0	0.0	4.0	0%
18.9.33.1 Button Settings	0	0	0	0	0	0	0.0	0.0	0%
18.9.33.2 Energy Saver Settings	0	0	0	0	0	0	0.0	0.0	0%
18.9.33.3 Hard Disk Settings	0	0	0	0	0	0	0.0	0.0	0%
18.9.33.4 Notification Settings	0	0	0	0	0	0	0.0	0.0	0%
18.9.33.5 Power Throttling Settings	0	0	0	0	0	0	0.0	0.0	0%
18.9.33.6 Sleep Settings	0	4	0	0	0	0	0.0	4.0	0%
18.9.34 Recovery	0	0	0	0	0	0	0.0	0.0	0%
18.9.35 Remote Assistance	0	2	0	0	0	0	0.0	2.0	0%
18.9.36 Remote Procedure Call	0	2	0	0	0	0	0.0	2.0	0%
18.9.37 Removable Storage Access	0	0	0	0	0	0	0.0	0.0	0%
18.9.38 Scripts	0	0	0	0	0	0	0.0	0.0	0%
18.9.39 Security Account Manager	0	0	0	0	0	0	0.0	0.0	0%
18.9.40 Server Manager	0	0	0	0	0	0	0.0	0.0	0%
18.9.41 Service Control Manager Settings	0	0	0	0	0	0	0.0	0.0	0%
18.9.42 Shutdown	0	0	0	0	0	0	0.0	0.0	0%
18.9.43 Shutdown Options	0	0	0	0	0	0	0.0	0.0	0%
18.9.44 Storage Health	0	0	0	0	0	0	0.0	0.0	0%
18.9.45 Storage Sense	0	0	0	0	0	0	0.0	0.0	0%
18.9.46 System Restore	0	0	0	0	0	0	0.0	0.0	0%
18.9.47 Troubleshooting and Diagnostics	0	0	0	0	0	0	0.0	0.0	0%
18.9.47.1 Application Compatibility Diagnostics	0	0	0	0	0	0	0.0	0.0	0%
18.9.47.2 Corrupted File Recovery	0	0	0	0	0	0	0.0	0.0	0%
18.9.47.3 Disk Diagnostic	0	0	0	0	0	0	0.0	0.0	0%
18.9.47.4 Fault Tolerant Heap	0	0	0	0	0	0	0.0	0.0	0%
18.9.47.5 Microsoft Support Diagnostic Tool	0	0	0	0	0	0	0.0	0.0	0%
18.9.47.6 MSI Corrupted File Recovery	0	0	0	0	0	0	0.0	0.0	0%
18.9.47.7 Scheduled Maintenance	0	0	0	0	0	0	0.0	0.0	0%
18.9.47.8 Scripted Diagnostics	0	0	0	0	0	0	0.0	0.0	0%
18.9.47.9 Windows Boot Performance Diagnostics	0	0	0	0	0	0	0.0	0.0	0%
18.9.47.10 Windows Memory Leak Diagnosis	0	0	0	0	0	0	0.0	0.0	0%
18.9.47.11 Windows Performance PerfTrack	0	0	0	0	0	0	0.0	0.0	0%
18.9.48 Trusted Platform Module Services	0	0	0	0	0	0	0.0	0.0	0%
18.9.49 User Profiles	0	0	0	0	0	0	0.0	0.0	0%
18.9.50 Windows File Protection	0	0	0	0	0	0	0.0	0.0	0%
18.9.51 Windows Time Service	0	2	0	0	0	0	0.0	2.0	0%
18.9.51.1 Time Providers	0	2	0	0	0	0	0.0	2.0	0%
18.10 Windows Components	5	96	0	0	0	0	5.0	101.0	5%
18.10.1 ActiveX Installer Service	0	0	0	0	0	0	0.0	0.0	0%
18.10.2 Add features to Windows 10 (formerly Windows Anytime Upgrade)	0	0	0	0	0	0	0.0	0.0	0%
18.10.3 App and Device Inventory	0	0	0	0	0	0	0.0	0.0	0%
18.10.4 App Package Deployment	0	2	0	0	0	0	0.0	2.0	0%
18.10.5 App Privacy	0	1	0	0	0	0	0.0	1.0	0%
18.10.6 App runtime	0	1	0	0	0	0	0.0	1.0	0%
18.10.7 Application Compatibility	0	0	0	0	0	0	0.0	0.0	0%
18.10.8 AutoPlay Policies	0	3	0	0	0	0	0.0	3.0	0%
18.10.9 Biometrics	0	1	0	0	0	0	0.0	1.0	0%
18.10.9.1 Facial Features	0	1	0	0	0	0	0.0	1.0	0%
18.10.10 BitLocker Drive Encryption	0	0	0	0	0	0	0.0	0.0	0%
18.10.10.1 Fixed Data Drives	0	0	0	0	0	0	0.0	0.0	0%
18.10.10.2 Operating System Drives	0	0	0	0	0	0	0.0	0.0	0%
18.10.10.3 Removable Data Drives	0	0	0	0	0	0	0.0	0.0	0%
18.10.11 Camera	0	0	0	0	0	0	0.0	0.0	0%
18.10.12 Chat	0	0	0	0	0	0	0.0	0.0	0%
18.10.13 Cloud Content	0	2	0	0	0	0	0.0	2.0	0%
18.10.14 Connect	0	1	0	0	0	0	0.0	1.0	0%
18.10.15 Credential User Interface	0	3	0	0	0	0	0.0	3.0	0%
18.10.16 Data Collection and Preview Builds	0	7	0	0	0	0	0.0	7.0	0%
18.10.17 Delivery Optimization	0	1	0	0	0	0	0.0	1.0	0%
18.10.18 Desktop App Installer	0	5	0	0	0	0	0.0	5.0	0%
18.10.19 Desktop Gadgets	0	0	0	0	0	0	0.0	0.0	0%
18.10.20 Desktop Window Manager	0	0	0	0	0	0	0.0	0.0	0%
18.10.21 Device and Driver Compatibility	0	0	0	0	0	0	0.0	0.0	0%
18.10.22 Device Registration (formerly Workplace Join)	0	0	0	0	0	0	0.0	0.0	0%
18.10.23 Digital Locker	0	0	0	0	0	0	0.0	0.0	0%
18.10.24 Edge UI	0	0	0	0	0	0	0.0	0.0	0%
18.10.25 Event Forwarding	0	0	0	0	0	0	0.0	0.0	0%

Description	Tests						Scoring		
	Pass	Fail	Error	Unkn.	Man.	Exc.	Score	Max	Percent
18.10.26 Event Log Service	3	5	0	0	0	0	3.0	8.0	38%
18.10.26.1 Application	1	1	0	0	0	0	1.0	2.0	50%
18.10.26.2 Security	1	1	0	0	0	0	1.0	2.0	50%
18.10.26.3 Setup	0	2	0	0	0	0	0.0	2.0	0%
18.10.26.4 System	1	1	0	0	0	0	1.0	2.0	50%
18.10.27 Event Logging	0	0	0	0	0	0	0.0	0.0	0%
18.10.28 Event Viewer	0	0	0	0	0	0	0.0	0.0	0%
18.10.29 File Explorer (formerly Windows Explorer)	0	4	0	0	0	0	0.0	4.0	0%
18.10.29.1 Previous Versions	0	0	0	0	0	0	0.0	0.0	0%
18.10.30 File History	0	0	0	0	0	0	0.0	0.0	0%
18.10.31 Find My Device	0	0	0	0	0	0	0.0	0.0	0%
18.10.32 Handwriting	0	0	0	0	0	0	0.0	0.0	0%
18.10.33 HomeGroup	0	0	0	0	0	0	0.0	0.0	0%
18.10.34 Human Presence	0	0	0	0	0	0	0.0	0.0	0%
18.10.35 Internet Explorer	0	1	0	0	0	0	0.0	1.0	0%
18.10.36 Internet Information Services	0	0	0	0	0	0	0.0	0.0	0%
18.10.37 Location and Sensors	0	0	0	0	0	0	0.0	0.0	0%
18.10.38 Maintenance Scheduler	0	0	0	0	0	0	0.0	0.0	0%
18.10.39 Maps	0	0	0	0	0	0	0.0	0.0	0%
18.10.40 MDM	0	0	0	0	0	0	0.0	0.0	0%
18.10.41 Messaging	0	0	0	0	0	0	0.0	0.0	0%
18.10.42 Microsoft account	0	1	0	0	0	0	0.0	1.0	0%
18.10.43 Microsoft Defender Antivirus (formerly Windows Defender and Windows Defender Antivirus)	0	19	0	0	0	0	0.0	19.0	0%
18.10.43.1 Client Interface	0	0	0	0	0	0	0.0	0.0	0%
18.10.43.2 Device Control	0	0	0	0	0	0	0.0	0.0	0%
18.10.43.3 Exclusions	0	0	0	0	0	0	0.0	0.0	0%
18.10.43.4 Features	0	1	0	0	0	0	0.0	1.0	0%
18.10.43.5 MAPS	0	1	0	0	0	0	0.0	1.0	0%
18.10.43.6 Microsoft Defender Exploit Guard (formerly Windows Defender Exploit Guard)	0	3	0	0	0	0	0.0	3.0	0%
18.10.43.6.1 Attack Surface Reduction	0	2	0	0	0	0	0.0	2.0	0%
18.10.43.6.2 Controlled Folder Access	0	0	0	0	0	0	0.0	0.0	0%
18.10.43.6.3 Network Protection	0	1	0	0	0	0	0.0	1.0	0%
18.10.43.7 MpEngine	0	1	0	0	0	0	0.0	1.0	0%
18.10.43.8 Network Inspection System	0	0	0	0	0	0	0.0	0.0	0%
18.10.43.9 Quarantine	0	0	0	0	0	0	0.0	0.0	0%
18.10.43.10 Real-time Protection	0	5	0	0	0	0	0.0	5.0	0%
18.10.43.11 Remediation	0	1	0	0	0	0	0.0	1.0	0%
18.10.43.11.1 Behavioral Network Blocks	0	1	0	0	0	0	0.0	1.0	0%
18.10.43.11.1.1 Brute-Force Protection	0	1	0	0	0	0	0.0	1.0	0%
18.10.43.11.1.2 Remote Encryption Protection	0	0	0	0	0	0	0.0	0.0	0%
18.10.43.12 Reporting	0	0	0	0	0	0	0.0	0.0	0%
18.10.43.13 Scan	0	5	0	0	0	0	0.0	5.0	0%
18.10.43.14 Security Intelligence Updates (formerly Signature Updates)	0	0	0	0	0	0	0.0	0.0	0%
18.10.43.15 Threats	0	0	0	0	0	0	0.0	0.0	0%
18.10.44 Microsoft Defender Application Guard (formerly Windows Defender Application Guard)	0	0	0	0	0	0	0.0	0.0	0%
18.10.45 Microsoft Defender Exploit Guard (formerly Windows Defender Exploit Guard)	0	0	0	0	0	0	0.0	0.0	0%
18.10.46 Microsoft Edge	0	0	0	0	0	0	0.0	0.0	0%
18.10.47 Microsoft Secondary Authentication Factor	0	0	0	0	0	0	0.0	0.0	0%
18.10.48 Microsoft User Experience Virtualization	0	0	0	0	0	0	0.0	0.0	0%
18.10.49 NetMeeting	0	0	0	0	0	0	0.0	0.0	0%
18.10.50 News and interests	0	0	0	0	0	0	0.0	0.0	0%
18.10.51 OneDrive (formerly SkyDrive)	0	1	0	0	0	0	0.0	1.0	0%
18.10.52 Online Assistance	0	0	0	0	0	0	0.0	0.0	0%
18.10.53 OOBE	0	0	0	0	0	0	0.0	0.0	0%
18.10.54 Portable Operating System	0	0	0	0	0	0	0.0	0.0	0%
18.10.55 Presentation Settings	0	0	0	0	0	0	0.0	0.0	0%
18.10.56 Push To Install	0	0	0	0	0	0	0.0	0.0	0%
18.10.57 Remote Desktop Services (formerly Terminal Services)	0	8	0	0	0	0	0.0	8.0	0%
18.10.57.1 RD Licensing (formerly TS Licensing)	0	0	0	0	0	0	0.0	0.0	0%
18.10.57.2 Remote Desktop Connection Client	0	1	0	0	0	0	0.0	1.0	0%
18.10.57.2.1 RemoteFX USB Device Redirection	0	0	0	0	0	0	0.0	0.0	0%
18.10.57.3 Remote Desktop Session Host (formerly Terminal Server)	0	7	0	0	0	0	0.0	7.0	0%
18.10.57.3.1 Application Compatibility	0	0	0	0	0	0	0.0	0.0	0%

Description	Tests						Scoring		
	Pass	Fail	Error	Unkn.	Man.	Exc.	Score	Max	Percent
18.10.57.3.2 Connections	0	0	0	0	0	0	0.0	0.0	0%
18.10.57.3.3 Device and Resource Redirection	0	1	0	0	0	0	0.0	1.0	0%
18.10.57.3.4 Licensing	0	0	0	0	0	0	0.0	0.0	0%
18.10.57.3.5 Printer Redirection	0	0	0	0	0	0	0.0	0.0	0%
18.10.57.3.6 Profiles	0	0	0	0	0	0	0.0	0.0	0%
18.10.57.3.7 RD Connection Broker (formerly TS Connection Broker)	0	0	0	0	0	0	0.0	0.0	0%
18.10.57.3.8 Remote Session Environment	0	0	0	0	0	0	0.0	0.0	0%
18.10.57.3.9 Security	0	5	0	0	0	0	0.0	5.0	0%
18.10.57.3.10 Session Time Limits	0	0	0	0	0	0	0.0	0.0	0%
18.10.57.3.11 Temporary folders	0	1	0	0	0	0	0.0	1.0	0%
18.10.58 RSS Feeds	0	2	0	0	0	0	0.0	2.0	0%
18.10.59 Search	0	4	0	0	0	0	0.0	4.0	0%
18.10.59.1 OCR	0	0	0	0	0	0	0.0	0.0	0%
18.10.60 Security Center	0	0	0	0	0	0	0.0	0.0	0%
18.10.61 Shutdown Options	0	0	0	0	0	0	0.0	0.0	0%
18.10.62 Smart Card	0	0	0	0	0	0	0.0	0.0	0%
18.10.63 Software Protection Platform	0	0	0	0	0	0	0.0	0.0	0%
18.10.64 Sound Recorder	0	0	0	0	0	0	0.0	0.0	0%
18.10.65 Speech	0	0	0	0	0	0	0.0	0.0	0%
18.10.66 Store	0	2	0	0	0	0	0.0	2.0	0%
18.10.67 Sync your settings	0	0	0	0	0	0	0.0	0.0	0%
18.10.68 Tablet PC	0	0	0	0	0	0	0.0	0.0	0%
18.10.69 Task Scheduler	0	0	0	0	0	0	0.0	0.0	0%
18.10.70 Tenant Restrictions	0	0	0	0	0	0	0.0	0.0	0%
18.10.71 Text Input	0	0	0	0	0	0	0.0	0.0	0%
18.10.72 Widgets	0	1	0	0	0	0	0.0	1.0	0%
18.10.73 Windows Calendar	0	0	0	0	0	0	0.0	0.0	0%
18.10.74 Windows Color System	0	0	0	0	0	0	0.0	0.0	0%
18.10.75 Windows Customer Experience Improvement Program	0	0	0	0	0	0	0.0	0.0	0%
18.10.76 Windows Defender SmartScreen	0	1	0	0	0	0	0.0	1.0	0%
18.10.76.1 Enhanced Phishing Protection	0	0	0	0	0	0	0.0	0.0	0%
18.10.76.2 Explorer	0	1	0	0	0	0	0.0	1.0	0%
18.10.77 Windows Error Reporting	0	0	0	0	0	0	0.0	0.0	0%
18.10.78 Windows Game Recording and Broadcasting	0	1	0	0	0	0	0.0	1.0	0%
18.10.79 Windows Hello for Business (formerly Microsoft Passport for Work)	0	0	0	0	0	0	0.0	0.0	0%
18.10.80 Windows Ink Workspace	0	1	0	0	0	0	0.0	1.0	0%
18.10.81 Windows Installer	0	2	0	0	0	0	0.0	2.0	0%
18.10.82 Windows Logon Options	0	2	0	0	0	0	0.0	2.0	0%
18.10.83 Windows Media Digital Rights Management	0	0	0	0	0	0	0.0	0.0	0%
18.10.84 Windows Media Player	0	0	0	0	0	0	0.0	0.0	0%
18.10.85 Windows Messenger	0	0	0	0	0	0	0.0	0.0	0%
18.10.86 Windows Mobility Center	0	0	0	0	0	0	0.0	0.0	0%
18.10.87 Windows PowerShell	0	0	0	0	0	0	0.0	0.0	0%
18.10.88 Windows Reliability Analysis	0	0	0	0	0	0	0.0	0.0	0%
18.10.89 Windows Remote Management (WinRM)	0	6	0	0	0	0	0.0	6.0	0%
18.10.89.1 WinRM Client	0	3	0	0	0	0	0.0	3.0	0%
18.10.89.2 WinRM Service	0	3	0	0	0	0	0.0	3.0	0%
18.10.90 Windows Remote Shell	0	0	0	0	0	0	0.0	0.0	0%
18.10.91 Windows Sandbox	0	2	0	0	0	0	0.0	2.0	0%
18.10.92 Windows Security (formerly Windows Defender Security Center)	0	1	0	0	0	0	0.0	1.0	0%
18.10.92.1 Account protection	0	0	0	0	0	0	0.0	0.0	0%
18.10.92.2 App and browser protection	0	1	0	0	0	0	0.0	1.0	0%
18.10.93 Windows Update	2	5	0	0	0	0	2.0	7.0	29%
18.10.93.1 Legacy Policies	0	1	0	0	0	0	0.0	1.0	0%
18.10.93.2 Manage end user experience	2	1	0	0	0	0	2.0	3.0	67%
18.10.93.3 Manage updates offered from Windows Server Update Service	0	0	0	0	0	0	0.0	0.0	0%
18.10.93.4 Manage updates offered from Windows Update (formerly Defer Windows Updates and Windows Update for Business)	0	3	0	0	0	0	0.0	3.0	0%
19 Administrative Templates (User)	**0**	**9**	**0**	**0**	**0**	**0**	**0.0**	**9.0**	**0%**
19.1 Control Panel	0	0	0	0	0	0	0.0	0.0	0%
19.2 Desktop	0	0	0	0	0	0	0.0	0.0	0%
19.3 Network	0	0	0	0	0	0	0.0	0.0	0%
19.4 Shared Folders	0	0	0	0	0	0	0.0	0.0	0%
19.5 Start Menu and Taskbar	0	1	0	0	0	0	0.0	1.0	0%
19.5.1 Notifications	0	1	0	0	0	0	0.0	1.0	0%
19.6 System	0	0	0	0	0	0	0.0	0.0	0%
19.6.1 Ctrl+Alt+Del Options	0	0	0	0	0	0	0.0	0.0	0%

Description	Tests						Scoring		
	Pass	Fail	Error	Unkn.	Man.	Exc.	Score	Max	Percent
19.6.2 Display	0	0	0	0	0	0	0.0	0.0	0%
19.6.3 Driver Installation	0	0	0	0	0	0	0.0	0.0	0%
19.6.4 Folder Redirection	0	0	0	0	0	0	0.0	0.0	0%
19.6.5 Group Policy	0	0	0	0	0	0	0.0	0.0	0%
19.6.6 Internet Communication Management	0	0	0	0	0	0	0.0	0.0	0%
19.6.6.1 Internet Communication settings	0	0	0	0	0	0	0.0	0.0	0%
19.7 Windows Components	0	8	0	0	0	0	0.0	8.0	0%
19.7.1 Account Notifications	0	0	0	0	0	0	0.0	0.0	0%
19.7.2 Add features to Windows 8 / 8.1 / 10 (formerly Windows Anytime Upgrade)	0	0	0	0	0	0	0.0	0.0	0%
19.7.3 App runtime	0	0	0	0	0	0	0.0	0.0	0%
19.7.4 Application Compatibility	0	0	0	0	0	0	0.0	0.0	0%
19.7.5 Attachment Manager	0	2	0	0	0	0	0.0	2.0	0%
19.7.6 AutoPlay Policies	0	0	0	0	0	0	0.0	0.0	0%
19.7.7 Calculator	0	0	0	0	0	0	0.0	0.0	0%
19.7.8 Cloud Content	0	3	0	0	0	0	0.0	3.0	0%
19.7.9 Credential User Interface	0	0	0	0	0	0	0.0	0.0	0%
19.7.10 Data Collection and Preview Builds	0	0	0	0	0	0	0.0	0.0	0%
19.7.11 Desktop Gadgets	0	0	0	0	0	0	0.0	0.0	0%
19.7.12 Desktop Window Manager	0	0	0	0	0	0	0.0	0.0	0%
19.7.13 Digital Locker	0	0	0	0	0	0	0.0	0.0	0%
19.7.14 Edge UI	0	0	0	0	0	0	0.0	0.0	0%
19.7.15 File Explorer (formerly Windows Explorer)	0	0	0	0	0	0	0.0	0.0	0%
19.7.16 File Revocation	0	0	0	0	0	0	0.0	0.0	0%
19.7.17 IME	0	0	0	0	0	0	0.0	0.0	0%
19.7.18 Instant Search	0	0	0	0	0	0	0.0	0.0	0%
19.7.19 Internet Explorer	0	0	0	0	0	0	0.0	0.0	0%
19.7.20 Location and Sensors	0	0	0	0	0	0	0.0	0.0	0%
19.7.21 Microsoft Edge	0	0	0	0	0	0	0.0	0.0	0%
19.7.22 Microsoft Management Console	0	0	0	0	0	0	0.0	0.0	0%
19.7.23 Microsoft User Experience Virtualization	0	0	0	0	0	0	0.0	0.0	0%
19.7.24 Multitasking	0	0	0	0	0	0	0.0	0.0	0%
19.7.25 NetMeeting	0	0	0	0	0	0	0.0	0.0	0%
19.7.26 Network Sharing	0	1	0	0	0	0	0.0	1.0	0%
19.7.27 OOBE	0	0	0	0	0	0	0.0	0.0	0%
19.7.28 Presentation Settings	0	0	0	0	0	0	0.0	0.0	0%
19.7.29 Remote Desktop Services (formerly Terminal Services)	0	0	0	0	0	0	0.0	0.0	0%
19.7.30 RSS Feeds	0	0	0	0	0	0	0.0	0.0	0%
19.7.31 Search	0	0	0	0	0	0	0.0	0.0	0%
19.7.32 Snipping Tool	0	0	0	0	0	0	0.0	0.0	0%
19.7.33 Sound Recorder	0	0	0	0	0	0	0.0	0.0	0%
19.7.34 Store	0	0	0	0	0	0	0.0	0.0	0%
19.7.35 Tablet PC	0	0	0	0	0	0	0.0	0.0	0%
19.7.36 Task Scheduler	0	0	0	0	0	0	0.0	0.0	0%
19.7.37 Windows AI	0	0	0	0	0	0	0.0	0.0	0%
19.7.38 Windows Calendar	0	0	0	0	0	0	0.0	0.0	0%
19.7.39 Windows Color System	0	0	0	0	0	0	0.0	0.0	0%
19.7.40 Windows Copilot	0	1	0	0	0	0	0.0	1.0	0%
19.7.41 Windows Defender SmartScreen	0	0	0	0	0	0	0.0	0.0	0%
19.7.42 Windows Error Reporting	0	0	0	0	0	0	0.0	0.0	0%
19.7.43 Windows Hello for Business (formerly Microsoft Passport for Work)	0	0	0	0	0	0	0.0	0.0	0%
19.7.44 Windows Installer	0	1	0	0	0	0	0.0	1.0	0%
19.7.45 Windows Logon Options	0	0	0	0	0	0	0.0	0.0	0%
19.7.46 Windows Media Player	0	0	0	0	0	0	0.0	0.0	0%
19.7.46.1 Networking	0	0	0	0	0	0	0.0	0.0	0%
19.7.46.2 Playback	0	0	0	0	0	0	0.0	0.0	0%
Total	**108**	**262**	**0**	**0**	**2**	**0**	**108.0**	**370.0**	**29%**

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

The 'Exc' column only applies to Exceptions that are generated using CIS-CAT Pro Dashboard and is not utilized by CIS-CAT Pro Assessor.

Profiles

This benchmark contains 10 profiles.The **Level 1 (L1)** profile was used for this assessment.

Title	Description
Level 1 (L1)	This profile is for Corporate/Enterprise Environments and is considered general use.

Title	Description
	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. Show Profile XML
Level 1 (L1) + BitLocker (BL)	This profile extends the Level 1 (L1) profile and includes BitLocker-related recommendations. Show Profile XML
Level 1 (L1) + Next Generation (NG)	This profile extends the Level 1 (L1) profile and includes Next Generation-related recommendations. Show Profile XML
Level 1 (L1) + BitLocker (BL) + Next Generation (NG)	This profile extends the Level 1 (L1) profile and includes BitLocker and Next Generation-related recommendations. Show Profile XML
Level 2 (L2)	This profile extends the Level 1 (L1) profile and is intended for High Security/Sensitive Data Environment with limited functionality. 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. Show Profile XML
Level 2 (L2) + BitLocker (BL)	This profile extends the Level 2 (L2) profile and includes BitLocker-related recommendations. Show Profile XML
Level 2 (L2) + Next Generation (NG)	This profile extends the Level 2 (L2) profile and includes Next Generation-related recommendations. Show Profile XML
Level 2 (L2) + BitLocker (BL) + Next Generation (NG)	This profile extends the Level 2 (L2) profile and includes BitLocker and Next Generation-related recommendations. Show Profile XML
BitLocker (BL)	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. Show Profile XML
Next Generation (NG)	This profile contains advanced Windows security features that have specific configuration dependencies, and may not be compatible with all systems. It therefore requires special attention to detail and testing before implementation. If your environment supports these features, they are highly recommended as they have tangible security benefits. This profile is intended to be an optional "add-on" to the Level 1 (L1) or Level 2 (L2) profiles. Show Profile XML

⇧

Assessment Results

☑ Display Only Essential Hygiene (CIS Critical Security Controls V8- IG-1) ☑ Display Only Failures
More

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	1.1.3 (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'	Fail
1.0	1.1.6 (L1) Ensure 'Relax minimum password length limits' is set to 'Enabled'	Fail
	1.2 Account Lockout Policy	
	2 Local Policies	
	2.1 Audit Policy	
	2.2 User Rights Assignment	

w	Benchmark Item	Result
	2.3 Security Options	
	2.3.1 Accounts	
1.0	2.3.1.4 (L1) Configure 'Accounts: Rename administrator account'	Fail
1.0	2.3.1.5 (L1) Configure 'Accounts: Rename guest account'	Fail
	2.3.2 Audit	
	2.3.3 DCOM	
	2.3.4 Devices	
	2.3.5 Domain controller	
	2.3.6 Domain member	
	2.3.7 Interactive logon	
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	
	2.3.9 Microsoft network server	
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	
	2.3.11 Network security	
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
	2.3.12 Recovery console	
	2.3.13 Shutdown	
	2.3.14 System cryptography	
	2.3.15 System objects	
	2.3.16 System settings	
	2.3.17 User Account Control	
	3 Event Log	
	4 Restricted Groups	
	5 System Services	
	6 Registry	
	7 File System	
	8 Wired Network (IEEE 802.3) Policies	
	9 Windows Defender Firewall with Advanced Security (formerly Windows Firewall with Advanced Security)	
	9.1 Domain Profile	
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: Settings: Display a notification' is set to 'No'	Fail
1.0	9.1.4 (L1) Ensure 'Windows Firewall: Domain: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\domainfw.log'	Fail
1.0	9.1.5 (L1) Ensure 'Windows Firewall: Domain: Logging: Size limit (KB)' is set to '16,384 KB or greater'	Fail
1.0	9.1.6 (L1) Ensure 'Windows Firewall: Domain: Logging: Log dropped packets' is set to 'Yes'	Fail
1.0	9.1.7 (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
1.0	9.2.3 (L1) Ensure 'Windows Firewall: Private: Settings: Display a notification' is set to 'No'	Fail
1.0	9.2.4 (L1) Ensure 'Windows Firewall: Private: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\privatefw.log'	Fail
1.0	9.2.5 (L1) Ensure 'Windows Firewall: Private: Logging: Size limit (KB)' is set to '16,384 KB or greater'	Fail
1.0	9.2.6 (L1) Ensure 'Windows Firewall: Private: Logging: Log dropped packets' is set to 'Yes'	Fail
1.0	9.2.7 (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: Settings: Display a notification' is set to 'No'	Fail
1.0	9.3.4 (L1) Ensure 'Windows Firewall: Public: Settings: Apply local firewall rules' is set to 'No'	Fail
1.0	9.3.5 (L1) Ensure 'Windows Firewall: Public: Settings: Apply local connection security rules' is set to 'No'	Fail
1.0	9.3.6 (L1) Ensure 'Windows Firewall: Public: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\publicfw.log'	Fail
1.0	9.3.7 (L1) Ensure 'Windows Firewall: Public: Logging: Size limit (KB)' is set to '16,384 KB or greater'	Fail
1.0	9.3.8 (L1) Ensure 'Windows Firewall: Public: Logging: Log dropped packets' is set to 'Yes'	Fail
1.0	9.3.9 (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	

w	Benchmark Item	Result
	16 IP Security Policies	
	17 Advanced Audit Policy Configuration	
	17.1 Account Logon	
	17.2 Account Management	
	17.3 Detailed Tracking	
	17.4 DS Access	
	17.5 Logon/Logoff	
	17.6 Object Access	
	17.7 Policy Change	
	17.8 Privilege Use	
	17.9 System	
	18 Administrative Templates (Computer)	
	18.1 Control Panel	
	18.1.1 Personalization	
	18.1.2 Regional and Language Options	
	18.1.2.1 Handwriting personalization	
1.0	18.1.2.2 (L1) Ensure 'Allow users to enable online speech recognition services' is set to 'Disabled'	Fail
	18.2 Desktop	
	18.3 LAPS (legacy)	
	18.4 MS Security Guide	
1.0	18.4.7 (L1) Ensure 'NetBT NodeType configuration' is set to 'Enabled: P-node (recommended)'	Fail
	18.5 MSS (Legacy)	
1.0	18.5.5 (L1) Ensure 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' is set to 'Disabled'	Fail
1.0	18.5.10 (L1) Ensure 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires' is set to 'Enabled: 5 or fewer seconds'	Fail
1.0	18.5.13 (L1) Ensure 'MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning' is set to 'Enabled: 90% or less'	Fail
	18.6 Network	
	18.6.1 Background Intelligent Transfer Service (BITS)	
	18.6.2 BranchCache	
	18.6.3 DirectAccess Client Experience Settings	
	18.6.4 DNS Client	
	18.6.5 Fonts	
	18.6.6 Hotspot Authentication	
	18.6.7 Lanman Server	
	18.6.8 Lanman Workstation	
	18.6.9 Link-Layer Topology Discovery	
	18.6.10 Microsoft Peer-to-Peer Networking Services	
	18.6.10.1 Peer Name Resolution Protocol	
	18.6.11 Network Connections	
	18.6.11.1 Windows Defender Firewall (formerly Windows Firewall)	
	18.6.12 Network Connectivity Status Indicator	
	18.6.13 Network Isolation	
	18.6.14 Network Provider	
	18.6.15 Offline Files	
	18.6.16 QoS Packet Scheduler	
	18.6.17 SNMP	
	18.6.18 SSL Configuration Settings	
	18.6.19 TCPIP Settings	
	18.6.19.1 IPv6 Transition Technologies	
	18.6.19.2 Parameters	
	18.6.20 Windows Connect Now	
	18.6.21 Windows Connection Manager	
1.0	18.6.21.1 (L1) Ensure 'Minimize the number of simultaneous connections to the Internet or a Windows Domain' is set to 'Enabled: 3 = Prevent Wi-Fi when on Ethernet'	Fail
	18.6.22 Wireless Display	
	18.6.23 WLAN Service	
	18.6.23.1 WLAN Media Cost	
	18.6.23.2 WLAN Settings	
	18.7 Printers	
1.0	18.7.1 (L1) Ensure 'Allow Print Spooler to accept client connections' is set to 'Disabled'	Fail
	18.8 Start Menu and Taskbar	
	18.8.1 Notifications	
	18.9 System	
	18.9.1 Access-Denied Assistance	
	18.9.2 App-V	
	18.9.3 Audit Process Creation	

w	Benchmark Item	Result
	18.9.4 Credentials Delegation	
	18.9.5 Device Guard	
	18.9.6 Device Health Attestation Service	
	18.9.7 Device Installation	
	18.9.7.1 Device Installation Restrictions	
	18.9.8 Disk NV Cache	
	18.9.9 Disk Quotas	
	18.9.10 Display	
	18.9.11 Distributed COM	
	18.9.12 Driver Installation	
	18.9.13 Early Launch Antimalware	
	18.9.14 Enhanced Storage Access	
	18.9.15 File Classification Infrastructure	
	18.9.16 File Share Shadow Copy Provider	
	18.9.17 Filesystem (formerly NTFS Filesystem)	
	18.9.18 Folder Redirection	
	18.9.19 Group Policy	
	18.9.19.1 Logging and tracing	
1.0	18.9.19.2 (L1) Ensure 'Configure registry policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE'	Fail
1.0	18.9.19.3 (L1) Ensure 'Configure registry policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE'	Fail
1.0	18.9.19.4 (L1) Ensure 'Configure security policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE'	Fail
1.0	18.9.19.5 (L1) Ensure 'Configure security policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE'	Fail
	18.9.20 Internet Communication Management	
	18.9.20.1 Internet Communication settings	
	18.9.21 iSCSI	
	18.9.22 KDC	
	18.9.23 Kerberos	
	18.9.24 Kernel DMA Protection	
	18.9.25 LAPS	
1.0	18.9.25.4 (L1) Ensure 'Password Settings: Password Complexity' is set to 'Enabled: Large letters + small letters + numbers + special characters'	Fail
1.0	18.9.25.5 (L1) Ensure 'Password Settings: Password Length' is set to 'Enabled: 15 or more'	Fail
1.0	18.9.25.6 (L1) Ensure 'Password Settings: Password Age (Days)' is set to 'Enabled: 30 or fewer'	Fail
	18.9.26 Local Security Authority	
	18.9.27 Locale Services	
	18.9.28 Logon	
1.0	18.9.28.1 (L1) Ensure 'Block user from showing account details on sign-in' is set to 'Enabled'	Fail
	18.9.29 Mitigation Options	
	18.9.30 Net Logon	
	18.9.31 OS Policies	
	18.9.32 PIN Complexity	
	18.9.33 Power Management	
	18.9.33.1 Button Settings	
	18.9.33.2 Energy Saver Settings	
	18.9.33.3 Hard Disk Settings	
	18.9.33.4 Notification Settings	
	18.9.33.5 Power Throttling Settings	
	18.9.33.6 Sleep Settings	
	18.9.34 Recovery	
	18.9.35 Remote Assistance	
	18.9.36 Remote Procedure Call	
	18.9.37 Removable Storage Access	
	18.9.38 Scripts	
	18.9.39 Security Account Manager	
	18.9.40 Server Manager	
	18.9.41 Service Control Manager Settings	
	18.9.42 Shutdown	
	18.9.43 Shutdown Options	
	18.9.44 Storage Health	
	18.9.45 Storage Sense	
	18.9.46 System Restore	
	18.9.47 Troubleshooting and Diagnostics	
	18.9.47.1 Application Compatibility Diagnostics	
	18.9.47.2 Corrupted File Recovery	

w	Benchmark Item	Result
	18.9.47.3 Disk Diagnostic	
	18.9.47.4 Fault Tolerant Heap	
	18.9.47.5 Microsoft Support Diagnostic Tool	
	18.9.47.6 MSI Corrupted File Recovery	
	18.9.47.7 Scheduled Maintenance	
	18.9.47.8 Scripted Diagnostics	
	18.9.47.9 Windows Boot Performance Diagnostics	
	18.9.47.10 Windows Memory Leak Diagnosis	
	18.9.47.11 Windows Performance PerfTrack	
	18.9.48 Trusted Platform Module Services	
	18.9.49 User Profiles	
	18.9.50 Windows File Protection	
	18.9.51 Windows Time Service	
	18.9.51.1 Time Providers	
	18.10 Windows Components	
	18.10.1 ActiveX Installer Service	
	18.10.2 Add features to Windows 10 (formerly Windows Anytime Upgrade)	
	18.10.3 App and Device Inventory	
	18.10.4 App Package Deployment	
	18.10.5 App Privacy	
	18.10.6 App runtime	
	18.10.7 Application Compatibility	
	18.10.8 AutoPlay Policies	
1.0	18.10.8.1 (L1) Ensure 'Disallow Autoplay for non-volume devices' is set to 'Enabled'	Fail
1.0	18.10.8.2 (L1) Ensure 'Set the default behavior for AutoRun' is set to 'Enabled: Do not execute any autorun commands'	Fail
1.0	18.10.8.3 (L1) Ensure 'Turn off Autoplay' is set to 'Enabled: All drives'	Fail
	18.10.9 Biometrics	
	18.10.9.1 Facial Features	
	18.10.10 BitLocker Drive Encryption	
	18.10.10.1 Fixed Data Drives	
	18.10.10.2 Operating System Drives	
	18.10.10.3 Removable Data Drives	
	18.10.11 Camera	
	18.10.12 Chat	
	18.10.13 Cloud Content	
	18.10.14 Connect	
	18.10.15 Credential User Interface	
	18.10.16 Data Collection and Preview Builds	
	18.10.17 Delivery Optimization	
1.0	18.10.17.1 (L1) Ensure 'Download Mode' is NOT set to 'Enabled: Internet'	Fail
	18.10.18 Desktop App Installer	
	18.10.19 Desktop Gadgets	
	18.10.20 Desktop Window Manager	
	18.10.21 Device and Driver Compatibility	
	18.10.22 Device Registration (formerly Workplace Join)	
	18.10.23 Digital Locker	
	18.10.24 Edge UI	
	18.10.25 Event Forwarding	
	18.10.26 Event Log Service	
	18.10.26.1 Application	
1.0	18.10.26.1.2 (L1) Ensure 'Application: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'	Fail
	18.10.26.2 Security	
1.0	18.10.26.2.2 (L1) Ensure 'Security: Specify the maximum log file size (KB)' is set to 'Enabled: 196,608 or greater'	Fail
	18.10.26.3 Setup	
1.0	18.10.26.3.1 (L1) Ensure 'Setup: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'	Fail
1.0	18.10.26.3.2 (L1) Ensure 'Setup: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'	Fail
	18.10.26.4 System	
1.0	18.10.26.4.2 (L1) Ensure 'System: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'	Fail
	18.10.27 Event Logging	
	18.10.28 Event Viewer	
	18.10.29 File Explorer (formerly Windows Explorer)	
	18.10.29.1 Previous Versions	
	18.10.30 File History	
	18.10.31 Find My Device	
	18.10.32 Handwriting	
	18.10.33 HomeGroup	

w	Benchmark Item	Result
	18.10.34 Human Presence	
	18.10.35 Internet Explorer	
1.0	18.10.35.1 (L1) Ensure 'Disable Internet Explorer 11 as a standalone browser' is set to 'Enabled: Always'	Fail
	18.10.36 Internet Information Services	
	18.10.37 Location and Sensors	
	18.10.38 Maintenance Scheduler	
	18.10.39 Maps	
	18.10.40 MDM	
	18.10.41 Messaging	
	18.10.42 Microsoft account	
	18.10.43 Microsoft Defender Antivirus (formerly Windows Defender and Windows Defender Antivirus)	
	18.10.43.1 Client Interface	
	18.10.43.2 Device Control	
	18.10.43.3 Exclusions	
	18.10.43.4 Features	
1.0	18.10.43.4.1 (L1) Ensure 'Enable EDR in block mode' is set to 'Enabled'	Fail
	18.10.43.5 MAPS	
	18.10.43.6 Microsoft Defender Exploit Guard (formerly Windows Defender Exploit Guard)	
	18.10.43.6.1 Attack Surface Reduction	
	18.10.43.6.2 Controlled Folder Access	
	18.10.43.6.3 Network Protection	
	18.10.43.7 MpEngine	
1.0	18.10.43.7.1 (L1) Ensure 'Enable file hash computation feature' is set to 'Enabled'	Fail
	18.10.43.8 Network Inspection System	
	18.10.43.9 Quarantine	
	18.10.43.10 Real-time Protection	
1.0	18.10.43.10.1 (L1) Ensure 'Configure real-time protection and Security Intelligence Updates during OOBE' is set to 'Enabled'	Fail
1.0	18.10.43.10.2 (L1) Ensure 'Scan all downloaded files and attachments' is set to 'Enabled'	Fail
1.0	18.10.43.10.3 (L1) Ensure 'Turn off real-time protection' is set to 'Disabled'	Fail
	18.10.43.11 Remediation	
	18.10.43.11.1 Behavioral Network Blocks	
	18.10.43.11.1.1 Brute-Force Protection	
1.0	18.10.43.11.1.1.2 (L1) Ensure 'Configure Remote Encryption Protection Mode' is set to 'Enabled: Audit' or higher	Fail
	18.10.43.11.1.2 Remote Encryption Protection	
	18.10.43.12 Reporting	
	18.10.43.13 Scan	
1.0	18.10.43.13.1 (L1) Ensure 'Scan excluded files and directories during quick scans' is set to 'Enabled: 1'	Fail
1.0	18.10.43.13.4 (L1) Ensure 'Trigger a quick scan after X days without any scans' is set to 'Enabled: 7'	Fail
1.0	18.10.43.13.5 (L1) Ensure 'Turn on e-mail scanning' is set to 'Enabled'	Fail
	18.10.43.14 Security Intelligence Updates (formerly Signature Updates)	
	18.10.43.15 Threats	
1.0	18.10.43.16 (L1) Ensure 'Configure detection for potentially unwanted applications' is set to 'Enabled: Block'	Fail
1.0	18.10.43.17 (L1) Ensure 'Control whether exclusions are visible to local users' is set to 'Enabled'	Fail
	18.10.44 Microsoft Defender Application Guard (formerly Windows Defender Application Guard)	
	18.10.45 Microsoft Defender Exploit Guard (formerly Windows Defender Exploit Guard)	
	18.10.46 Microsoft Edge	
	18.10.47 Microsoft Secondary Authentication Factor	
	18.10.48 Microsoft User Experience Virtualization	
	18.10.49 NetMeeting	
	18.10.50 News and interests	
	18.10.51 OneDrive (formerly SkyDrive)	
	18.10.52 Online Assistance	
	18.10.53 OOBE	
	18.10.54 Portable Operating System	
	18.10.55 Presentation Settings	
	18.10.56 Push To Install	
	18.10.57 Remote Desktop Services (formerly Terminal Services)	
	18.10.57.1 RD Licensing (formerly TS Licensing)	
	18.10.57.2 Remote Desktop Connection Client	
	18.10.57.2.1 RemoteFX USB Device Redirection	
	18.10.57.3 Remote Desktop Session Host (formerly Terminal Server)	
	18.10.57.3.1 Application Compatibility	
	18.10.57.3.2 Connections	
	18.10.57.3.3 Device and Resource Redirection	
	18.10.57.3.4 Licensing	
	18.10.57.3.5 Printer Redirection	

w	Benchmark Item	Result
	18.10.57.3.6 Profiles	
	18.10.57.3.7 RD Connection Broker (formerly TS Connection Broker)	
	18.10.57.3.8 Remote Session Environment	
	18.10.57.3.9 Security	
	18.10.57.3.10 Session Time Limits	
	18.10.57.3.11 Temporary folders	
1.0	18.10.57.3.11.1 (L1) Ensure 'Do not delete temp folders upon exit' is set to 'Disabled'	Fail
	18.10.58 RSS Feeds	
	18.10.59 Search	
	18.10.59.1 OCR	
	18.10.60 Security Center	
	18.10.61 Shutdown Options	
	18.10.62 Smart Card	
	18.10.63 Software Protection Platform	
	18.10.64 Sound Recorder	
	18.10.65 Speech	
	18.10.66 Store	
1.0	18.10.66.2 (L1) Ensure 'Turn off Automatic Download and Install of updates' is set to 'Disabled'	Fail
	18.10.67 Sync your settings	
	18.10.68 Tablet PC	
	18.10.69 Task Scheduler	
	18.10.70 Tenant Restrictions	
	18.10.71 Text Input	
	18.10.72 Widgets	
	18.10.73 Windows Calendar	
	18.10.74 Windows Color System	
	18.10.75 Windows Customer Experience Improvement Program	
	18.10.76 Windows Defender SmartScreen	
	18.10.76.1 Enhanced Phishing Protection	
	18.10.76.2 Explorer	
	18.10.77 Windows Error Reporting	
	18.10.78 Windows Game Recording and Broadcasting	
	18.10.79 Windows Hello for Business (formerly Microsoft Passport for Work)	
	18.10.80 Windows Ink Workspace	
	18.10.81 Windows Installer	
	18.10.82 Windows Logon Options	
	18.10.83 Windows Media Digital Rights Management	
	18.10.84 Windows Media Player	
	18.10.85 Windows Messenger	
	18.10.86 Windows Mobility Center	
	18.10.87 Windows PowerShell	
	18.10.88 Windows Reliability Analysis	
	18.10.89 Windows Remote Management (WinRM)	
	18.10.89.1 WinRM Client	
	18.10.89.2 WinRM Service	
	18.10.90 Windows Remote Shell	
	18.10.91 Windows Sandbox	
	18.10.92 Windows Security (formerly Windows Defender Security Center)	
	18.10.92.1 Account protection	
	18.10.92.2 App and browser protection	
	18.10.93 Windows Update	
	18.10.93.1 Legacy Policies	
1.0	18.10.93.1.1 (L1) Ensure 'No auto-restart with logged on users for scheduled automatic updates installations' is set to 'Disabled'	Fail
	18.10.93.2 Manage end user experience	
1.0	18.10.93.2.3 (L1) Ensure 'Remove access to “Pause updates” feature' is set to 'Enabled'	Fail
	18.10.93.3 Manage updates offered from Windows Server Update Service	
	18.10.93.4 Manage updates offered from Windows Update (formerly Defer Windows Updates and Windows Update for Business)	
1.0	18.10.93.4.2 (L1) Ensure 'Select when Preview Builds and Feature Updates are received' is set to 'Enabled: 180 or more days'	Fail
1.0	18.10.93.4.3 (L1) Ensure 'Select when Quality Updates are received' is set to 'Enabled: 0 days'	Fail
	19 Administrative Templates (User)	
	19.1 Control Panel	
	19.2 Desktop	
	19.3 Network	
	19.4 Shared Folders	
	19.5 Start Menu and Taskbar	
	19.5.1 Notifications	

w	Benchmark Item	Result
	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 Account Notifications	
	19.7.2 Add features to Windows 8 / 8.1 / 10 (formerly Windows Anytime Upgrade)	
	19.7.3 App runtime	
	19.7.4 Application Compatibility	
	19.7.5 Attachment Manager	
1.0	19.7.5.2 (L1) Ensure 'Notify antivirus programs when opening attachments' is set to 'Enabled'	Fail
	19.7.6 AutoPlay Policies	
	19.7.7 Calculator	
	19.7.8 Cloud Content	
	19.7.9 Credential User Interface	
	19.7.10 Data Collection and Preview Builds	
	19.7.11 Desktop Gadgets	
	19.7.12 Desktop Window Manager	
	19.7.13 Digital Locker	
	19.7.14 Edge UI	
	19.7.15 File Explorer (formerly Windows Explorer)	
	19.7.16 File Revocation	
	19.7.17 IME	
	19.7.18 Instant Search	
	19.7.19 Internet Explorer	
	19.7.20 Location and Sensors	
	19.7.21 Microsoft Edge	
	19.7.22 Microsoft Management Console	
	19.7.23 Microsoft User Experience Virtualization	
	19.7.24 Multitasking	
	19.7.25 NetMeeting	
	19.7.26 Network Sharing	
	19.7.27 OOBE	
	19.7.28 Presentation Settings	
	19.7.29 Remote Desktop Services (formerly Terminal Services)	
	19.7.30 RSS Feeds	
	19.7.31 Search	
	19.7.32 Snipping Tool	
	19.7.33 Sound Recorder	
	19.7.34 Store	
	19.7.35 Tablet PC	
	19.7.36 Task Scheduler	
	19.7.37 Windows AI	
	19.7.38 Windows Calendar	
	19.7.39 Windows Color System	
	19.7.40 Windows Copilot	
	19.7.41 Windows Defender SmartScreen	
	19.7.42 Windows Error Reporting	
	19.7.43 Windows Hello for Business (formerly Microsoft Passport for Work)	
	19.7.44 Windows Installer	
	19.7.45 Windows Logon Options	
	19.7.46 Windows Media Player	
	19.7.46.1 Networking	
	19.7.46.2 Playback	

⇧

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 stand-alone systems is 0 passwords, but the default setting when joined to a domain is 24 passwords. To maintain the effectiveness of this policy setting, use the Minimum password age setting to prevent users from repeatedly changing their password.

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

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

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

Rationale:

The longer a 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:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** https://www.cisecurity.org/white-papers/cis-password-policy-guide/
- **URL:** https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/password-policy
- **URL:** GRID: MS-00000001

CIS Controls V7.0:

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

CIS Critical Security Controls V8.0:

- **Control 5: Account Management:** -- 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)).`

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

Rationale:

Users may have favorite passwords that they like to use because they are easy to remember and they believe that their password choice is secure from compromise. Unfortunately, passwords are compromised and if an attacker is targeting a specific individual's user account, with foreknowledge of data about that user, reuse of old passwords can cause a security breach. To address password reuse a combination of security settings is required. Using this policy setting with the Enforce password history setting prevents the easy reuse of old passwords. For example, if you configure the Enforce password history setting to ensure that users cannot reuse any of their last 12 passwords, they could change their password 13 times in a few minutes and reuse the password they started with, unless you also configure the Minimum password age setting to a number that is greater than 0. You must configure this policy setting to a number that is greater than 0 for the Enforce password history setting to be effective.

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:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** https://www.cisecurity.org/white-papers/cis-password-policy-guide/
- **URL:** https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/password-policy
- **URL:** GRID: MS-00000003

CIS Controls V7.0:

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

CIS Critical Security Controls V8.0:

- **Control 5: Account Management:** -- 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

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

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

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

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

Rationale:

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

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

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** https://www.cisecurity.org/white-papers/cis-password-policy-guide/
- **URL:** https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/password-policy
- **URL:** GRID: MS-00000004

CIS Controls V7.0:

- **Control 4: Controlled Use of Administrative Privileges:** -- More
- **Control 16: Account Monitoring and Control:** -- More
  >

CIS Critical Security Controls V8.0:

- **Control 5: Account Management:** -- More
  >

Back to Summary

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

Description:

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

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

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

Each additional character in a password increases its complexity exponentially. For instance, a seven-character, all lower-case alphabetic password would have 26 to the power of 7 (approximately 8 x 10 to the power of 9 or 8 billion) possible combinations. At 1,000,000 attempts per second (a capability of many password-cracking utilities), it would only take 133 minutes to crack. A seven-character alphabetic password with case sensitivity has 52 to the power of 7 combinations. A seven-character case-sensitive alphanumeric password without punctuation has 627 combinations. An eight-character password has 26 to the power of 8 (or 2 x 10 to the power of 11) possible combinations. Although this might seem to be a large number, at 1,000,000 attempts per second it would take only 59 hours to try all possible passwords. Remember, these times will significantly increase for passwords that use ALT characters and other special keyboard characters such as "!" or "@". Proper use of the password settings can help make it difficult to mount a brute force attack.

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

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

Rationale:

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

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:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** https://www.cisecurity.org/white-papers/cis-password-policy-guide/
- **URL:** https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/password-policy
- **URL:** GRID: MS-00000005

CIS Controls V7.0:

- **Control 4: Controlled Use of Administrative Privileges:** -- More
- **Control 16: Account Monitoring and Control:** -- More

>

CIS Critical Security Controls V8.0:

- **Control 5: Account Management:** -- More
>

Back to Summary

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

Description:

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

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

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

Rationale:

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

Remediation:

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

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

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

Impact:

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

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

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

CIS Controls V7.0:

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

CIS Critical Security Controls V8.0:

- **Control 5: Account Management:** -- More
>

Back to Summary

1.2 Account Lockout Policy

This section contains recommendations for account lockout policy.

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.

2.3 Security Options

This section contains recommendations for security options.

2.3.1 Accounts

This section contains recommendations related to default accounts.

2.3.1.4 (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:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/accounts-rename-administrator-account
- **URL:** GRID: MS-00000056

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More
  >

Back to Summary

2.3.1.5 (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:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/accounts-rename-guest-account
- **URL:** GRID: MS-00000057

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

2.3.2 Audit

This section contains recommendations related to auditing controls.

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.

2.3.5 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.

2.3.7 Interactive logon

This section contains recommendations related to interactive logons.

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:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/interactive-logon-smart-card-removal-behavior
- **URL:** GRID: MS-00000080

CIS Controls V7.0:

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

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

2.3.8 Microsoft network client

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

2.3.9 Microsoft network server

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

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:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/microsoft-network-server-server-spn-target-name-validation-level
- **URL:** GRID: MS-00000088

CIS Controls V7.0:

- **Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

2.3.10 Network access

This section contains recommendations related to network access.

2.3.11 Network security

This section contains recommendations related to network security.

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` .

Note: If a hybrid environment is used, and PKU2U is `Disabled` , Remote Desktop connections from a hybrid joined system to a hybrid joined system will fail.

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:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-allow-pku2u-authentication-requests-to-this-computer-to-use-online-identities
- **URL:** GRID: MS-00000105

CIS Controls V7.0:

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

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- 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.

2.3.16 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.

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.

6 Registry

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

7 File System

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

8 Wired Network (IEEE 802.3) Policies

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

9 Windows Defender Firewall with Advanced Security (formerly Windows Firewall with Advanced Security)

This section contains recommendations for configuring the Windows Firewall.

Note: In older versions of Microsoft Windows, this section was named *Windows Firewall with Advanced Security* , but it was renamed to *Windows Defender Firewall with Advanced Security* starting with Windows 10 Release 1709.

9.1 Domain Profile

This section contains recommendations for the Domain Profile of the Windows Firewall.

9.1.1 (L1) Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)' 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 Defender Firewall with
Advanced Security\Windows Defender Firewall with Advanced Security\Windows Defender Firewall
Properties\Domain Profile\Firewall state
```

Impact:

None - this is the default behavior.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/best-practices-configuring
- **URL:** GRID: MS-00000173

CIS Controls V7.0:

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

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- 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 Defender Firewall with
Advanced Security\Windows Defender Firewall with Advanced Security\Windows Defender Firewall
Properties\Domain Profile\Inbound connections
```

Impact:

None - this is the default behavior.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/best-practices-configuring
- **URL:** GRID: MS-00000174

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More
- **Control 11: Secure Configuration for Network Devices, such as Firewalls, Routers and Switches:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

9.1.3 (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 Defender Firewall with
Advanced Security\Windows Defender Firewall with Advanced Security\Windows Defender 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:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/best-practices-configuring
- **URL:** GRID: MS-00000175

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More
- **Control 11: Secure Configuration for Network Devices, such as Firewalls, Routers and Switches:** -- More
  >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More
  >

Back to Summary

9.1.4 (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 Windows Firewall events are not recorded it may be difficult or impossible for Administrators to analyze system issues or unauthorized activities of malicious users.

Microsoft stores all firewall events as one file on the system (`pfirewall.log`). To improve logging, separate each firewall profile (domain, private, public) into its own distinct log file (`domainfw.log` , `privatefw.log` , `publicfw.log`) for better organization and identification of specific issues within each profile.

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 Defender Firewall with
Advanced Security\Windows Defender Firewall with Advanced Security\Windows Defender Firewall
Properties\Domain Profile\Logging Customize\Name
```

Impact:

The log file will be stored in the specified file.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/best-practices-configuring
- **URL:** GRID: MS-00000176

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More
- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More
  >

CIS Critical Security Controls V8.0:

- **Control 8: Audit Log Management:** -- More
  >

Back to Summary

9.1.5 (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 Defender Firewall with
Advanced Security\Windows Defender Firewall with Advanced Security\Windows Defender 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:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** GRID: MS-00000177

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More
- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More

>

CIS Critical Security Controls V8.0:

- **Control 8: Audit Log Management:** -- More
>

Back to Summary

9.1.6 (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 Defender Firewall with
Advanced Security\Windows Defender Firewall with Advanced Security\Windows Defender Firewall
Properties\Domain Profile\Logging Customize\Log dropped packets
```

Impact:

Information about dropped packets will be recorded in the firewall log file.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** GRID: MS-00000178

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More
- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More
>

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More
- **Control 8: Audit Log Management:** -- More
>

Back to Summary

9.1.7 (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 Defender Firewall with
Advanced Security\Windows Defender Firewall with Advanced Security\Windows Defender Firewall
Properties\Domain Profile\Logging Customize\Log successful connections
```

Impact:

Information about successful connections will be recorded in the firewall log file.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** GRID: MS-00000179

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More
- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More
  >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More
- **Control 8: Audit Log Management:** -- 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 Defender Firewall with
Advanced Security\Windows Defender Firewall with Advanced Security\Windows Defender Firewall
Properties\Private Profile\Firewall state
```

Impact:

None - this is the default behavior.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/best-practices-configuring

- **URL:** GRID: MS-00000180

CIS Controls V7.0:

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

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- 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 Defender Firewall with
Advanced Security\Windows Defender Firewall with Advanced Security\Windows Defender Firewall
Properties\Private Profile\Inbound connections
```

Impact:

None - this is the default behavior.

Assessment:

Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/best-practices-configuring
- **URL:** GRID: MS-00000181

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More
- **Control 11: Secure Configuration for Network Devices, such as Firewalls, Routers and Switches:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

9.2.3 (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 Defender Firewall with
Advanced Security\Windows Defender Firewall with Advanced Security\Windows Defender 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:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** GRID: MS-00000182

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More
- **Control 11: Secure Configuration for Network Devices, such as Firewalls, Routers and Switches:** -- More
  >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More
  >

Back to Summary

9.2.4 (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 Windows Firewall events are not recorded it may be difficult or impossible for Administrators to analyze system issues or unauthorized activities of malicious users.

Microsoft stores all firewall events as one file on the system (`pfirewall.log`). To improve logging, separate each firewall profile (domain, private, public) into its own distinct log file (`domainfw.log` , `privatefw.log` , `publicfw.log`) for better organization and identification of specific issues within each profile.

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 Defender Firewall with
Advanced Security\Windows Defender Firewall with Advanced Security\Windows Defender Firewall
Properties\Private Profile\Logging Customize\Name
```

Impact:

The log file will be stored in the specified file.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/best-practices-configuring
- **URL:** https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/configure-the-windows-firewall-log
- **URL:** GRID: MS-00000183

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More
- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More
  >

CIS Critical Security Controls V8.0:

- **Control 8: Audit Log Management:** -- More
  >

Back to Summary

9.2.5 (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 Defender Firewall with
Advanced Security\Windows Defender Firewall with Advanced Security\Windows Defender 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:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/configure-the-windows-firewall-log
- **URL:** GRID: MS-00000184

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More
- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More
  >

CIS Critical Security Controls V8.0:

- **Control 8: Audit Log Management:** -- More
  >

Back to Summary

9.2.6 (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 Defender Firewall with
Advanced Security\Windows Defender Firewall with Advanced Security\Windows Defender Firewall
Properties\Private Profile\Logging Customize\Log dropped packets
```

Impact:

Information about dropped packets will be recorded in the firewall log file.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/configure-the-windows-firewall-log
- **URL:** GRID: MS-00000185

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More
- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More
  >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More
- **Control 8: Audit Log Management:** -- More
  >

Back to Summary

9.2.7 (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 Defender Firewall with
Advanced Security\Windows Defender Firewall with Advanced Security\Windows Defender Firewall
Properties\Private Profile\Logging Customize\Log successful connections
```

Impact:

Information about successful connections will be recorded in the firewall log file.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/configure-the-windows-firewall-log
- **URL:** GRID: MS-00000186

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More
- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More
  >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More
- **Control 8: Audit Log Management:** -- 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 Defender Firewall with
Advanced Security\Windows Defender Firewall with Advanced Security\Windows Defender Firewall
Properties\Public Profile\Firewall state
```

Impact:

None - this is the default behavior.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/best-practices-configuring
- **URL:** GRID: MS-00000187

CIS Controls V7.0:

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

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- 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 Defender Firewall with
Advanced Security\Windows Defender Firewall with Advanced Security\Windows Defender Firewall
Properties\Public Profile\Inbound connections
```

Impact:

None - this is the default behavior.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/best-practices-configuring
- **URL:** GRID: MS-00000188

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More
- **Control 11: Secure Configuration for Network Devices, such as Firewalls, Routers and Switches:** -- More
  >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More
  >

Back to Summary

9.3.3 (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 Defender Firewall with
Advanced Security\Windows Defender Firewall with Advanced Security\Windows Defender 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:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** GRID: MS-00000189

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More
- **Control 11: Secure Configuration for Network Devices, such as Firewalls, Routers and Switches:** -- More
  >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More
  >

Back to Summary

9.3.4 (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 Defender Firewall with
Advanced Security\Windows Defender Firewall with Advanced Security\Windows Defender 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:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** GRID: MS-00000190

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More
- **Control 11: Secure Configuration for Network Devices, such as Firewalls, Routers and Switches:** -- More
  >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More
  >

Back to Summary

9.3.5 (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 Defender Firewall with
Advanced Security\Windows Defender Firewall with Advanced Security\Windows Defender 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:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** GRID: MS-00000191

CIS Controls V7.0:

- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More
- **Control 11: Secure Configuration for Network Devices, such as Firewalls, Routers and Switches:** -- More
  >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More
  >

Back to Summary

9.3.6 (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 Windows Firewall events are not recorded it may be difficult or impossible for Administrators to analyze system issues or unauthorized activities of malicious users.

Microsoft stores all firewall events as one file on the system (`pfirewall.log`). To improve logging, separate each firewall profile (domain, private, public) into its own distinct log file (`domainfw.log` , `privatefw.log` , `publicfw.log`) for better organization and identification of specific issues within each profile.

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 Defender Firewall with
Advanced Security\Windows Defender Firewall with Advanced Security\Windows Defender Firewall
Properties\Public Profile\Logging Customize\Name
```

Impact:

The log file will be stored in the specified file.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/configure-the-windows-firewall-log
- **URL:** GRID: MS-00000192

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More
- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More
  >

CIS Critical Security Controls V8.0:

- **Control 8: Audit Log Management:** -- More
  >

Back to Summary

9.3.7 (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 Defender Firewall with
Advanced Security\Windows Defender Firewall with Advanced Security\Windows Defender 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:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** GRID: MS-00000193

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More
- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More
  >

CIS Critical Security Controls V8.0:

- **Control 8: Audit Log Management:** -- More
  >

Back to Summary

9.3.8 (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 Defender Firewall with
Advanced Security\Windows Defender Firewall with Advanced Security\Windows Defender Firewall
Properties\Public Profile\Logging Customize\Log dropped packets
```

Impact:

Information about dropped packets will be recorded in the firewall log file.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** GRID: MS-00000194

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More
- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More
  >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More
- **Control 8: Audit Log Management:** -- More
  >

Back to Summary

9.3.9 (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 Defender Firewall with
Advanced Security\Windows Defender Firewall with Advanced Security\Windows Defender Firewall
Properties\Public Profile\Logging Customize\Log successful connections
```

Impact:

Information about successful connections will be recorded in the firewall log file.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** GRID: MS-00000195

CIS Controls V7.0:

- **Control 6: Maintenance, Monitoring and Analysis of Audit Logs:** -- More
- **Control 9: Limitation and Control of Network Ports, Protocols, and Services:** -- More
  >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More
- **Control 8: Audit Log Management:** -- 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.

17.2 Account Management

This section contains recommendations for configuring the Account Management audit policy.

17.3 Detailed Tracking

This section contains recommendations for configuring the Detailed Tracking audit policy.

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.

17.6 Object Access

This section contains recommendations for configuring the Object Access audit policy.

17.7 Policy Change

This section contains recommendations for configuring the Policy Change audit policy.

17.8 Privilege Use

This section contains recommendations for configuring the Privilege Use audit policy.

17.9 System

This section contains recommendations for configuring the System audit policy.

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).

18.1.2 Regional and Language Options

This section contains recommendation settings for Regional and Language Options.

This Group Policy section is provided by the Group Policy template `Globalization.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.1.2.1 Handwriting personalization

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

This Group Policy section is provided by the Group Policy template `Globalization.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.1.2.2 (L1) Ensure 'Allow users to enable online speech recognition services' is set to 'Disabled' 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 users to enable online speech recognition services
```

Note: This Group Policy path is provided by the Group Policy template `Globalization.admx/adml` that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *Allow input personalization* , but it was renamed to *Allow users to enable online speech recognition services* starting with the Windows 10 R1809 & Server 2019 Administrative Templates.

Impact:

Automatic learning of speech, inking, and typing stops and users cannot change its value via PC Settings.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** GRID: MS-00000233

CIS Controls V7.0:

- **Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

18.2 Desktop

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

This Group Policy section is provided by the Group Policy template `Desktop.admx/adml` that is included with the Microsoft Windows 11 Release 22H2 Administrative Templates v1.0 (or newer).

18.3 LAPS (legacy)

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

18.4 MS Security Guide

This section contains recommendations for configuring additional settings from the MS Security Guide.

This Group Policy section is provided by the Group Policy template `SecGuide.admx/adml` that is available for download from the Microsoft Security Compliance Toolkit and Baselines website. Regardless of Windows Operating System version, download the latest Windows 11 Security Baseline to obtain the template.

18.4.7 (L1) Ensure 'NetBT NodeType configuration' is set to 'Enabled: P-node (recommended)' Fail

Description:

This setting determines which method NetBIOS over TCP/IP (NetBT) uses to register and resolve names. The available methods are:

- The B-node (broadcast) method only uses broadcasts.
- The P-node (point-to-point) method only uses name queries to a name server (WINS).
- The M-node (mixed) method broadcasts first, then queries a name server (WINS) if broadcast failed.
- The H-node (hybrid) method queries a name server (WINS) first, then broadcasts if the query failed.

The recommended state for this setting is: `Enabled: P-node (recommended)` (point-to-point).

Note: Resolution through LMHOSTS or DNS follows these methods. If the `NodeType` registry value is present, it overrides any `DhcpNodeType` registry value. If neither `NodeType` nor `DhcpNodeType` is present, the computer uses B-node (broadcast) if there are no WINS servers configured for the network, or H-node (hybrid) if there is at least one WINS server configured.

Rationale:

In order to help mitigate the risk of NetBIOS Name Service (NBT-NS) poisoning attacks, setting the node type to P-node (point-to-point) will prevent the system from sending out NetBIOS broadcasts.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: P-node (recommended)` :

```
Computer Configuration\Policies\Administrative Templates\MS Security Guide\NetBT NodeType configuration
```

Note: This change does not take effect until the computer has been restarted.

Note #2: This Group Policy path does not exist by default. An additional Group Policy template (`SecGuide.admx/adml`) is required - it is available from Microsoft at this link . Please note that this setting is **only** available in the *Security baseline (FINAL) for Windows 10 v1903 and Windows Server v1903* (or newer) release of `SecGuide.admx/adml` , so if you previously downloaded this template, you may need to update it from a newer Microsoft baseline to get this new *NetBT NodeType configuration* setting.

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:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-cifs/45170055-a0cd-4910-9228-801d5bf7ac84
- **URL:** GRID: MS-00000247

CIS Controls V7.0:

- **Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

18.5 MSS (Legacy)

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

This Group Policy section is provided by the Group Policy template `MSS-legacy.admx/adml` that is available for download from the Microsoft Security Compliance Toolkit and Baselines website. Regardless of Windows Operating System version, download the latest Windows 11 Security Baseline to obtain the template.

18.5.5 (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:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** https://techcommunity.microsoft.com/t5/microsoft-security-baselines/the-mss-settings/ba-p/701055
- **URL:** GRID: MS-00000253

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More
- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More
  >

Back to Summary

18.5.10 (L1) Ensure 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires' 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
```

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:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** https://techcommunity.microsoft.com/t5/microsoft-security-baselines/the-mss-settings/ba-p/701055
- **URL:** GRID: MS-00000258

CIS Controls V7.0:

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

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

18.5.13 (L1) Ensure 'MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning' is set to 'Enabled: 90% or less'

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:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** https://techcommunity.microsoft.com/t5/microsoft-security-baselines/the-mss-settings/ba-p/701055
- **URL:** GRID: MS-00000261

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 Critical Security Controls V8.0:

- **Control 8: Audit Log Management:** -- More
  >

Back to Summary

18.6 Network

This section contains recommendations for network settings.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.6.1 Background Intelligent Transfer Service (BITS)

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

This Group Policy section is provided by the Group Policy template `Bits.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.6.2 BranchCache

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

This Group Policy section is provided by the Group Policy template `PeerToPeerCaching.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.6.3 DirectAccess Client Experience Settings

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

This Group Policy section is provided by the Group Policy template `nca.admx/adml` that is included with the Microsoft 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.6.4 DNS Client

This section contains recommendations related to DNS Client.

This Group Policy section is provided by the Group Policy template `DnsClient.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.6.5 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).

18.6.6 Hotspot Authentication

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

This Group Policy section is provided by the Group Policy template `hotspotauth.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.6.7 Lanman Server

This section is 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).

18.6.8 Lanman Workstation

This section contains recommendations related to Lanman Workstation.

This Group Policy section is provided by the Group Policy template `LanmanWorkstation.admx/adml` that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

18.6.9 Link-Layer Topology Discovery

This section contains recommendations for Link-Layer Topology Discovery settings.

This Group Policy section is provided by the Group Policy template `LinkLayerTopologyDiscovery.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.6.10 Microsoft Peer-to-Peer Networking Services

This section contains recommendations for Microsoft Peer-to-Peer Networking Services settings.

This Group Policy section is provided by the Group Policy template `P2P-pnrp.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.6.10.1 Peer Name Resolution Protocol

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

This Group Policy section is provided by the Group Policy template `P2P-pnrp.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.6.11 Network Connections

This section contains recommendations for Network Connections settings.

This Group Policy section is provided by the Group Policy template `NetworkConnections.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.6.11.1 Windows Defender Firewall (formerly Windows Firewall)

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

This Group Policy section is provided by the Group Policy template `WindowsFirewall.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note: This section was initially named *Windows Firewall* but was renamed by Microsoft to *Windows Defender Firewall* starting with the Microsoft Windows 10 Release 1709 Administrative Templates.

18.6.12 Network Connectivity Status Indicator

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

This Group Policy section is provided by the Group Policy template `NCSI.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.6.13 Network Isolation

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

This Group Policy section is provided by the Group Policy template `NetworkIsolation.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.6.14 Network Provider

This section contains recommendations for Network Provider settings.

This Group Policy section is provided by the Group Policy template `NetworkProvider.admx/adml` that is included with the MS15-011 / MSKB 3000483 security update and the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

18.6.15 Offline Files

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

This Group Policy section is provided by the Group Policy template `OfflineFiles.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.6.16 QoS Packet Scheduler

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

This Group Policy section is provided by the Group Policy template `QOS.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.6.17 SNMP

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

This Group Policy section is provided by the Group Policy template `Snmp.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.6.18 SSL Configuration Settings

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

This Group Policy section is provided by the Group Policy template `CipherSuiteOrder.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.6.19 TCPIP Settings

This section contains TCP/IP configuration settings.

This Group Policy section is provided by the Group Policy template `tcpip.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.6.19.1 IPv6 Transition Technologies

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

This Group Policy section is provided by the Group Policy template `tcpip.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.6.19.2 Parameters

This section contains TCP/IP parameter configuration settings.

This Group Policy section is provided by the Group Policy template `tcpip.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.6.20 Windows Connect Now

This section contains recommendations for Windows Connect Now settings.

This Group Policy section is provided by the Group Policy template `WindowsConnectNow.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.6.21 Windows Connection Manager

This section contains recommendations for Windows Connection Manager settings.

This Group Policy section is provided by the Group Policy template `WCM.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.6.21.1 (L1) Ensure 'Minimize the number of simultaneous connections to the Internet or a Windows Domain' is set to 'Enabled: 3 = Prevent Wi-Fi when on Ethernet' 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: 3 = Prevent Wi-Fi when on Ethernet.`

Rationale:

Preventing bridged network connections can help prevent a user unknowingly allowing traffic to route between internal and external networks, which risks exposure to sensitive internal data.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: 3 = Prevent Wi-Fi when on Ethernet`:

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

Note: This Group Policy path is provided by the Group Policy template `WCM.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates. It was updated with a new *Minimize Policy Options* sub-setting starting with the Windows 10 Release 1903 Administrative Templates.

Impact:

While connected to an Ethernet connection, Windows won't allow use of a WLAN (automatically *or* manually) until Ethernet is disconnected. However, if a cellular data connection is available, it will always stay connected for services that require it, but no Internet traffic will be routed over cellular if an Ethernet or WLAN connection is present.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** GRID: MS-00000278

CIS Controls V7.0:

- **Control 15: Wireless Access Control:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

18.6.22 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).

18.6.23 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).

18.6.23.1 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).

18.6.23.2 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).

18.7 Printers

This section contains recommendations for printer settings.

This Group Policy section is provided by the Group Policy template `Printing.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.7.1 (L1) Ensure 'Allow Print Spooler to accept client connections' is set to 'Disabled' Fail

Description:

This policy setting controls whether the Print Spooler service will accept client connections.

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

Note: The Print Spooler service must be restarted for changes to this policy to take effect.

Rationale:

Disabling the ability for the Print Spooler service to accept client connections mitigates **remote** attacks against the PrintNightmare vulnerability (CVE-2021-34527) and other **remote** Print Spooler attacks. However, this recommendation *does not* mitigate against **local** attacks on the Print Spooler service.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Printers\Allow Print Spooler to accept client connections
```

Note: This Group Policy path is provided by the Group Policy template `printing2.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Impact:

Provided that the Print Spooler service is not disabled, users will continue to be able to print *from their workstation* . However, the workstation's Print Spooler service will not accept client connections or allow users to share printers. Note that all printers that were already shared will continue to be shared.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527
- **URL:** GRID: MS-00000281

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More
- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

18.8 Start Menu and Taskbar

This section contains recommendations for Start Menu and Taskbar.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.8.1 Notifications

This section contains recommendations for Start Menu and Taskbar Notifications.

This Group Policy section is provided by the Group Policy template `WPN.admx/adml` that is included with the Microsoft 10 Release 1803 Administrative Templates (or newer).

18.9 System

This section contains recommendations for System settings.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.1 Access-Denied Assistance

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

This Group Policy section is provided by the Group Policy template `srm-fci.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.9.2 App-V

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

This Group Policy section is provided by the Group Policy template `appv.admx/adml` that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

18.9.3 Audit Process Creation

This section contains settings related to auditing of process creation events.

This Group Policy section is provided by the Group Policy template `AuditSettings.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.9.4 Credentials Delegation

This section contains settings related to Credential Delegation.

This Group Policy section is provided by the Group Policy template `CredSsp.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.5 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).

18.9.6 Device Health Attestation Service

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

This Group Policy section is provided by the Group Policy template `TPM.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

18.9.7 Device Installation

This section contains recommendations related to device installation.

This Group Policy section is provided by the Group Policy template `DeviceInstallation.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.7.1 Device Installation Restrictions

This section 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.

18.9.8 Disk NV Cache

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

This Group Policy section is provided by the Group Policy template `DiskNVCache.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.9 Disk Quotas

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

This Group Policy section is provided by the Group Policy template `DiskQuota.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.10 Display

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

This Group Policy section is provided by the Group Policy template `Display.admx/adml` that is included with the Microsoft Windows 10 Release 1703 Administrative Templates (or newer).

18.9.11 Distributed COM

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

This Group Policy section is provided by the Group Policy template `DCOM.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.12 Driver Installation

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

This Group Policy section is provided by the Group Policy template `DeviceInstallation.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.13 Early Launch Antimalware

This section contains recommendations for configuring boot-start driver initialization settings.

This Group Policy section is provided by the Group Policy template `EarlyLaunchAM.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.9.14 Enhanced Storage Access

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

This Group Policy section is provided by the Group Policy template `EnhancedStorage.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.9.15 File Classification Infrastructure

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

This Group Policy section is provided by the Group Policy template `srm-fci.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.9.16 File Share Shadow Copy Provider

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

This Group Policy section is provided by the Group Policy templates `FileServerVSSProvider.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.9.17 Filesystem (formerly NTFS Filesystem)

This section is 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.

18.9.18 Folder Redirection

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

This Group Policy section is provided by the Group Policy template `FolderRedirection.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.19 Group Policy

This section contains recommendations for configuring group policy-related settings.

This Group Policy section is provided by the Group Policy template `GroupPolicy.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.19.1 Logging and tracing

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

This Group Policy section is provided by the Group Policy template `GroupPolicyPreferences.admx/adml` that is included with the Microsoft Windows Server 2008 (non-R2) Administrative Templates (or newer).

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

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

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

Rationale:

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

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** https://learn.microsoft.com/en-us/previous-versions/ms813374(v=msdn.10)?redirectedfrom=MSDN
- **URL:** GRID: MS-00000312

CIS Controls V7.0:

- **Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

18.9.19.3 (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 registry policies even if the registry policies have not changed.

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

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

Rationale:

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

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** https://learn.microsoft.com/en-us/previous-versions/ms813374(v=msdn.10)?redirectedfrom=MSDN
- **URL:** GRID: MS-00000313

CIS Controls V7.0:

- **Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

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

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

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

Rationale:

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

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`, then set the `Do not apply during periodic background processing` option to `FALSE` (unchecked):

```
Computer Configuration\Policies\Administrative Templates\System\Group Policy\Configure security policy processing
```

Note: This Group Policy path is provided by the Group Policy template `GroupPolicy.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Impact:

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** https://learn.microsoft.com/en-us/previous-versions/ms813374(v=msdn.10)?redirectedfrom=MSDN
- **URL:** GRID: MS-00000314

CIS Controls V7.0:

- **Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

18.9.19.5 (L1) Ensure 'Configure security 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 security policies even if the security policies have not changed.

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

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

Rationale:

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

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`, then set the `Process even if the Group Policy objects have not changed` option to `TRUE` (checked):

```
Computer Configuration\Policies\Administrative Templates\System\Group Policy\Configure security policy processing
```

Note: This Group Policy path is provided by the Group Policy template `GroupPolicy.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

Impact:

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** https://learn.microsoft.com/en-us/previous-versions/ms813374(v=msdn.10)?redirectedfrom=MSDN
- **URL:** GRID: MS-00000315

CIS Controls V7.0:

- **Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

18.9.20 Internet Communication Management

This section contains recommendations related to Internet Communication Management.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.20.1 Internet Communication settings

This section contains recommendations related to Internet Communication settings.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.21 iSCSI

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

This Group Policy section is provided by the Group Policy template `iSCSI.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.22 KDC

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

This Group Policy section is provided by the Group Policy template `KDC.admx/adml` that is included with the Microsoft Windows Server 2008 (non-R2) Administrative Templates (or newer).

18.9.23 Kerberos

This section contains recommendations for Kerberos settings.

This Group Policy section is provided by the Group Policy template `Kerberos.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.24 Kernel DMA Protection

This section contains recommendations related to Kernel DMA Protection.

This Group Policy section is provided by the Group Policy template `DmaGuard.admx/adml` that is included with the Microsoft Windows 10 Release 1809 and Server 2019 Administrative Templates (or newer).

18.9.25 LAPS

This section contains recommendations for Windows Local Administrator Password Solution (LAPS) settings.

This Group Policy section is provided by the Group Policy template `LAPS.admx/adml` that is included with the Microsoft Windows 11 Release 22H2 Administrative Templates v3.0 (or newer).

18.9.25.4 (L1) Ensure 'Password Settings: Password Complexity' is set to 'Enabled: Large letters + small letters + numbers + special characters'

Fail

Description:

This policy setting configures the Windows LAPS Password Settings policy for password complexity.

Each additional character in a password increases its complexity exponentially. For instance, a seven-character, all lower-case alphabetic password would have 26 to the power of 7 (approximately 8 x 10 to the power of 9 or 8 billion) possible combinations. At 1,000,000 attempts per second (a capability of many password-cracking utilities), it would only take 133 minutes to crack. A seven-character alphabetic password with case sensitivity has 52 to the power of 7 combinations. A seven-character case-sensitive alphanumeric password without punctuation has 627 combinations. An eight-character password has 26 to the power of 8 (or 2 x 10 to the power of 11) possible combinations. Although this might seem to be a large number, at 1,000,000 attempts per second it would take only 59 hours to try all possible passwords. Remember, these times will significantly increase for passwords that use ALT characters and other special keyboard characters such as "!" or "@". Proper use of the password settings can help make it difficult to mount a brute force attack.

The recommended state for this setting is: `Enabled: Large letters + small letters + numbers + special characters.`

Note: Organizations that utilize third-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations.

Note #2: Windows LAPS does not support standalone computers - they must be joined to an Active Directory domain or Entra ID (formerly Azure Active Directory).

Rationale:

Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or Member Servers when deploying them. This creates a serious attack surface security risk because if an attacker manages to compromise one system and learn the password to its local Administrator account, then they can leverage that account to instantly gain access to all other computers that also use that password for their local Administrator account.

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\System\LAPS\Password Settings
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `LAPS.admx/adml` that is included with the Microsoft Windows 11 Release 22H2 Administrative Templates v3.0 (or newer).

Impact:

None - this is the default behavior.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** https://learn.microsoft.com/en-us/windows-server/identity/laps/laps-management-policy-settings
- **URL:** GRID: MS-00000337

CIS Controls V7.0:

- **Control 4: Controlled Use of Administrative Privileges:** -- More >

CIS Critical Security Controls V8.0:

- **Control 5: Account Management:** -- More >

Back to Summary

18.9.25.5 (L1) Ensure 'Password Settings: Password Length' is set to 'Enabled: 15 or more'

Fail

Description:

This policy setting configures the Windows LAPS Password Settings policy for password length.

Each additional character in a password increases its complexity exponentially. For instance, a seven-character, all lower-case alphabetic password would have 26 to the power of 7 (approximately 8 x 10 to the power of 9 or 8 billion) possible combinations. At 1,000,000 attempts per second (a capability of many password-cracking utilities), it would only take 133 minutes to crack. A seven-character alphabetic password with case sensitivity has 52 to the power of 7 combinations. A seven-character case-sensitive alphanumeric password without punctuation has 627 combinations. An eight-character password has 26 to the power of 8 (or 2 x 10 to the power of 11) possible combinations. Although this might seem to be a large number, at 1,000,000 attempts per second it would take only 59 hours to try all possible passwords. Remember, these times will significantly increase for passwords that use ALT characters and other special keyboard characters such as "!" or "@". Proper use of the password settings can help make it difficult to mount a brute force attack.

The recommended state for this setting is: `Enabled: 15 or more`.

Note: Organizations that utilize third-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations.

Note #2: Windows LAPS does not support standalone computers - they must be joined to an Active Directory domain or Entra ID (formerly Azure Active Directory).

Rationale:

Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or Member Servers when deploying them. This creates a serious attack surface security risk because if 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\System\LAPS\Password Settings
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `LAPS.admx/adml` that is included with the Microsoft Windows 11 Release 22H2 Administrative Templates v3.0 (or newer).

Impact:

Windows LAPS-generated passwords will be required to have a length of 15 characters (or more, if selected).

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** https://learn.microsoft.com/en-us/windows-server/identity/laps/laps-management-policy-settings
- **URL:** GRID: MS-00000338

CIS Controls V7.0:

- **Control 4: Controlled Use of Administrative Privileges:** -- More >

CIS Critical Security Controls V8.0:

- **Control 5: Account Management:** -- More >

Back to Summary

18.9.25.6 (L1) Ensure 'Password Settings: Password Age (Days)' is set to 'Enabled: 30 or fewer'

Fail

Description:

This policy setting configures the Windows LAPS Password Settings policy for password age.

Because attackers can crack passwords, the more frequently the password is changed the less opportunity an attacker has to use a cracked password.

The recommended state for this setting is: `Enabled: 30 or fewer.`

Note: Organizations that utilize third-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations.

Note #2: Windows LAPS does not support standalone computers - they must be joined to an Active Directory domain or Entra ID (formerly Azure Active Directory).

Rationale:

Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or Member Servers when deploying them. This creates a serious attack surface security risk because if 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\System\LAPS\Password Settings
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `LAPS.admx/adml` that is included with the Microsoft Windows 11 Release 22H2 Administrative Templates v3.0 (or newer).

Impact:

None - this is the default behavior, unless set to fewer than 30 days.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** https://learn.microsoft.com/en-us/windows-server/identity/laps/laps-management-policy-settings
- **URL:** GRID: MS-00000339

CIS Controls V7.0:

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

CIS Critical Security Controls V8.0:

- **Control 5: Account Management:** -- More >

Back to Summary

18.9.26 Local Security Authority

This section contains recommendations for Local Security Authority settings.

This Group Policy section is provided by the Group Policy template `LocalSecurityAuthority.admx/adml` that is included with the Microsoft Windows 11 Release 22H2 Administrative Templates v1.0 (or newer).

18.9.27 Locale Services

This section contains recommendations for Locale Services settings.

This Group Policy section is provided by the Group Policy template `Globalization.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.28 Logon

This section contains recommendations related to the logon process and lock screen.

This Group Policy section is provided by the Group Policy template `Logon.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.28.1 (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 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:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** GRID: MS-00000345

CIS Controls V7.0:

- **Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers:** -- More >

CIS Critical Security Controls V8.0:

- **Control 4: Secure Configuration of Enterprise Assets and Software:** -- More >

Back to Summary

18.9.29 Mitigation Options

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

This Group Policy section is provided by the Group Policy template `GroupPolicy.admx/adml` that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

18.9.30 Net Logon

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

This Group Policy section is provided by the Group Policy template `Netlogon.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.31 OS Policies

This section contains recommendations related to OS Policies.

This Group Policy section is provided by the Group Policy template `OSPolicy.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

18.9.32 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).

18.9.33 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.

18.9.33.1 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.

18.9.33.2 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).

18.9.33.3 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.

18.9.33.4 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.

18.9.33.5 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).

18.9.33.6 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.

18.9.34 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).

18.9.35 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.

18.9.36 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.

18.9.37 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.

18.9.38 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.

18.9.39 Security Account Manager

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

This Group Policy section is provided by the Group Policy template `SAM.admx/adml` that is included with the Microsoft Windows 11 Release 21H2 Administrative Templates (or newer).

18.9.40 Server Manager

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

This Group Policy section is provided by the Group Policy template `ServerManager.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.41 Service Control Manager Settings

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

This Group Policy section is provided by the Group Policy template `ServiceControlManager.admx/adml` that is included with the Microsoft Windows 10 Release 1903 Administrative Templates (or newer).

18.9.42 Shutdown

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

This Group Policy section is provided by the Group Policy template `WinInit.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.9.43 Shutdown Options

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

This Group Policy section is provided by the Group Policy template `Winsrv.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.44 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).

18.9.45 Storage Sense

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

This Group Policy section is provided by the Group Policy template `StorageSense.admx/adml` that is included with the Microsoft Windows 10 Release 1903 Administrative Templates (or newer).

18.9.46 System Restore

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

This Group Policy section is provided by the Group Policy template `SystemRestore.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.47 Troubleshooting and Diagnostics

This section contains recommendations related to Troubleshooting and Diagnostics.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.47.1 Application Compatibility Diagnostics

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

This Group Policy section is provided by the Group Policy template `pca.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.47.2 Corrupted File Recovery

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

This Group Policy section is provided by the Group Policy template `FileRecovery.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.47.3 Disk Diagnostic

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

This Group Policy section is provided by the Group Policy template `DiskDiagnostic.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.47.4 Fault Tolerant Heap

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

This Group Policy section is provided by the Group Policy template `fthsvc.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.9.47.5 Microsoft Support Diagnostic Tool

This section contains recommendations related to the Microsoft Support Diagnostic Tool.

This Group Policy section is provided by the Group Policy template `MSDT.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.47.6 MSI Corrupted File Recovery

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

This Group Policy section is provided by the Group Policy template `Msi-FileRecovery.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.9.47.7 Scheduled Maintenance

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

This Group Policy section is provided by the Group Policy template `sdiagschd.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.9.47.8 Scripted Diagnostics

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

This Group Policy section is provided by the Group Policy template `sdiageng.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.9.47.9 Windows Boot Performance Diagnostics

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

This Group Policy section is provided by the Group Policy template `PerformanceDiagnostics.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.47.10 Windows Memory Leak Diagnosis

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

This Group Policy section is provided by the Group Policy template `LeakDiagnostic.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.47.11 Windows Performance PerfTrack

This section contains recommendations related to Windows Performance PerfTrack.

This Group Policy section is provided by the Group Policy template `PerformancePerftrack.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.9.48 Trusted Platform Module Services

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

This Group Policy section is provided by the Group Policy template `TPM.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.49 User Profiles

This section contains recommendations related to User Profiles.

This Group Policy section is provided by the Group Policy template `UserProfiles.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.50 Windows File Protection

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

This Group Policy section is provided by the Group Policy template `WindowsFileProtection.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.51 Windows Time Service

This section contains recommendations related to the Windows Time Service.

This Group Policy section is provided by the Group Policy template `W32Time.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.9.51.1 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.

18.10 Windows Components

This section contains recommendations for Windows Component settings.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.1 ActiveX Installer Service

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

This Group Policy section is provided by the Group Policy template `ActiveXInstallService.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.2 Add features to Windows 10 (formerly Windows Anytime Upgrade)

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

This Group Policy section is provided by the Group Policy template `WindowsAnytimeUpgrade.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Note: This section was initially named *Windows Anytime Upgrade* but was renamed by Microsoft to *Add features to Windows x* starting with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

18.10.3 App and Device Inventory

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

This Group Policy section is provided by the Group Policy template `AppDeviceInventory.admx/adml` that is included with the Microsoft Windows 11 Release 24H2 Administrative Templates (or newer).

18.10.4 App Package Deployment

This section contains recommendations for App Package Deployment settings.

This Group Policy section is provided by the Group Policy template `AppxPackageManager.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.10.5 App Privacy

This section contains recommendations for App Privacy settings.

This Group Policy section is provided by the Group Policy template `AppPrivacy.admx/adml` that is included with the Microsoft Windows 10 Release 1511 Administrative Templates (or newer).

18.10.6 App runtime

This section contains recommendations for App runtime settings.

This Group Policy section is provided by the Group Policy template `AppXRuntime.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.10.7 Application Compatibility

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

This Group Policy section is provided by the Group Policy template `AppCompat.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.8 AutoPlay Policies

This section contains recommendations for AutoPlay policies.

This Group Policy section is provided by the Group Policy template `AutoPlay.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.8.1 (L1) Ensure 'Disallow Autoplay for non-volume devices' is set to 'Enabled' Fail

Description:

This policy setting disallows AutoPlay for MTP devices like cameras or phones.

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

Rationale:

An attacker could use this feature to launch a program to damage a client computer or data on the computer.

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 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:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** GRID: MS-00000374

CIS Controls V7.0:

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

CIS Critical Security Controls V8.0:

- **Control 10: Malware Defenses:** -- More
  >

Back to Summary

18.10.8.2 (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 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:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** GRID: MS-00000375

CIS Controls V7.0:

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

CIS Critical Security Controls V8.0:

- **Control 10: Malware Defenses:** -- More
>

Back to Summary

18.10.8.3 (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:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** GRID: MS-00000376

CIS Controls V7.0:

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

CIS Critical Security Controls V8.0:

- **Control 10: Malware Defenses:** -- More
>

Back to Summary

18.10.9 Biometrics

This section contains recommendations related to Biometrics.

This Group Policy section is provided by the Group Policy template `Biometrics.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.10.9.1 Facial Features

This section contains recommendations related to Facial Feature Biometrics.

This Group Policy section is provided by the Group Policy template `Biometrics.admx/adml` that is included with the Microsoft Windows 10 Release 1511 Administrative Templates (or newer).

18.10.10 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.

18.10.10.1 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).

18.10.10.2 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).

18.10.10.3 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).

18.10.11 Camera

This section contains recommendations related to Camera.

This Group Policy section is provided by the Group Policy template `Camera.admx/adml` that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

18.10.12 Chat

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

This Group Policy section is provided by the Group Policy template `Taskbar.admx/adml` that is included with the Microsoft Windows 11 Release 21H2 Administrative Templates (or newer).

18.10.13 Cloud Content

This section contains recommendations related to Cloud Content.

This Group Policy section is provided by the Group Policy template `CloudContent.admx/adml` that is included with the Microsoft Windows 10 Release 1511 Administrative Templates (or newer).

18.10.14 Connect

This section contains recommendations related to Connect.

This Group Policy section is provided by the Group Policy template `WirelessDisplay.admx/adml` that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

18.10.15 Credential User Interface

This section contains recommendations related to the Credential User Interface.

This Group Policy section is provided by the Group Policy template `CredUI.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.16 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).

18.10.17 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).

18.10.17.1 (L1) Ensure 'Download Mode' is NOT set to 'Enabled: Internet' Fail

Description:

This policy setting specifies the download method that Delivery Optimization can use in downloads of Windows Updates, Apps and App updates. The following methods are supported:

- 0 = HTTP only, no peering.
- 1 = HTTP blended with peering behind the same NAT.
- 2 = HTTP blended with peering across a private group. Peering occurs on devices in the same Active Directory Site (if exist) or the same domain by default. When this option is selected, peering will cross NATs. To create a custom group use Group ID in combination with Mode 2.
- 3 = HTTP blended with Internet Peering.
- 99 = Simple download mode with no peering. Delivery Optimization downloads using HTTP only and does not attempt to contact the Delivery Optimization cloud services.
- 100 = Bypass mode. Do not use Delivery Optimization and use BITS instead.

The recommended state for this setting is any value EXCEPT: `Enabled: Internet (3)`.

Note: The default on all SKUs other than Enterprise, Enterprise LTSB or Education is `Enabled: Internet (3)`, so on other SKUs, be sure to set this to a different value.

Note #2: The option `100 = Bypass mode` is deprecated for Windows 11 and can cause some content downloads to fail.

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 (3)`:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Delivery Optimization\Download Mode
```

Note: This Group Policy path 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 (0)`, `Enabled: Simple (99)`, or `Enabled: Bypass (100)`, machines will not be able to download updates from other machines on the same LAN.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** https://learn.microsoft.com/en-us/windows/deployment/do/waas-delivery-optimization-reference#download-mode
- **URL:** GRID: MS-00000440

CIS Controls V7.0:

- **Control 3: Continuous Vulnerability Management:** -- More >

CIS Critical Security Controls V8.0:

- **Control 7: Continuous Vulnerability Management:** -- More

>

Back to Summary

18.10.18 Desktop App Installer

This section contains recommendations related to Desktop App Installer.

This Group Policy section is provided by the Group Policy template `DesktopAppInstaller.admx/adml` that is included with the Microsoft Windows 11 Release 22H2 Administrative Templates v1.0 (or newer).

18.10.19 Desktop Gadgets

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

This Group Policy section is provided by the Group Policy template `Sidebar.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.10.20 Desktop Window Manager

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

This Group Policy section is provided by the Group Policy template `DWM.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.21 Device and Driver Compatibility

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

This Group Policy section is provided by the Group Policy template `DeviceCompat.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.10.22 Device Registration (formerly Workplace Join)

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

This Group Policy section is provided by the Group Policy template `WorkplaceJoin.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Note: This section was initially named *Workplace Join* but was renamed by Microsoft to *Device Registration* starting with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates.

18.10.23 Digital Locker

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

This Group Policy section is provided by the Group Policy template `DigitalLocker.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.24 Edge UI

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

This Group Policy section is provided by the Group Policy template `EdgeUI.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.10.25 Event Forwarding

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

This Group Policy section is provided by the Group Policy template `EventForwarding.admx/adml` that is included with the Microsoft Windows Server 2008 (non-R2) Administrative Templates (or newer).

18.10.26 Event Log Service

This section contains recommendations for configuring the Event Log Service.

This Group Policy section is provided by the Group Policy template `EventLog.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.26.1 Application

This section contains recommendations for configuring the Application Event Log.

This Group Policy section is provided by the Group Policy template `EventLog.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.26.1.2 (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:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** GRID: MS-00000446

CIS Controls V7.0:

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

CIS Critical Security Controls V8.0:

- **Control 8: Audit Log Management:** -- More >

Back to Summary

18.10.26.2 Security

This section contains recommendations for configuring the Security Event Log.

This Group Policy section is provided by the Group Policy template `EventLog.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.26.2.2 (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:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** GRID: MS-00000448

CIS Controls V7.0:

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

CIS Critical Security Controls V8.0:

- **Control 8: Audit Log Management:** -- More >

Back to Summary

18.10.26.3 Setup

This section contains recommendations for configuring the Setup Event Log.

This Group Policy section is provided by the Group Policy template `EventLog.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.26.3.1 (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:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** GRID: MS-00000449

CIS Controls V7.0:

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

CIS Critical Security Controls V8.0:

- **Control 8: Audit Log Management:** -- More >

Back to Summary

18.10.26.3.2 (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:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** GRID: MS-00000451

CIS Controls V7.0:

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

CIS Critical Security Controls V8.0:

- **Control 8: Audit Log Management:** -- More >

Back to Summary

18.10.26.4 System

This section contains recommendations for configuring the System Event Log.

This Group Policy section is provided by the Group Policy template `EventLog.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.26.4.2 (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:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** GRID: MS-00000453

CIS Controls V7.0:

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

CIS Critical Security Controls V8.0:

- **Control 8: Audit Log Management:** -- More >

Back to Summary

18.10.27 Event Logging

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

This Group Policy section is provided by the Group Policy template `EventLogging.admx/adml` that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

18.10.28 Event Viewer

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

This Group Policy section is provided by the Group Policy template `EventViewer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.29 File Explorer (formerly Windows Explorer)

This section contains recommendations to control the availability of options such as menu items and tabs in dialog boxes.

This Group Policy section is provided by the Group Policy template `WindowsExplorer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note: This section was initially named *Windows Explorer* but was renamed by Microsoft to *File Explorer* starting with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

18.10.29.1 Previous Versions

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

This Group Policy section is provided by the Group Policy template `PreviousVersions.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.30 File History

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

This Group Policy section is provided by the Group Policy template `FileHistory.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.10.31 Find My Device

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

This Group Policy section is provided by the Group Policy template `FindMy.admx/adml` that is included with the Microsoft Windows 10 Release 1703 Administrative Templates (or newer).

18.10.32 Handwriting

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

This Group Policy section is provided by the Group Policy template `Handwriting.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

18.10.33 HomeGroup

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

This Group Policy section is provided by the Group Policy template `Sharing.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.10.34 Human Presence

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

This Group Policy section is provided by the Group Policy template `Sensors.admx/adml` that is included with the Microsoft Windows 11 Release 21H2 Administrative Templates (or newer).

18.10.35 Internet Explorer

This section contains recommendations related to Internet Explorer.

This Group Policy section is provided by the Group Policy template `InetRes.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

CIS publishes security guidance for Microsoft Internet Explorer in a separate benchmark from Windows. Additional details can be found in the CIS Microsoft Web Browser Benchmarks Community .

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

Description:

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

This setting performs the following actions when enabled:

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

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

Rationale:

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

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Internet Explorer\Disable Internet Explorer 11 as a standalone browser
```

Note: This Group Policy path is provided by the Group Policy template `InetRes.admx/adml` that is included with the Microsoft Windows 10 Release 21H1 Administrative Templates (or newer).

Impact:

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

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

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

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** https://learn.microsoft.com/en-us/deployedge/edge-ie-disable-ie11
- **URL:** https://techcommunity.microsoft.com/t5/windows-it-pro-blog/internet-explorer-11-desktop-app-retirement-faq/ba-p/2366549
- **URL:** GRID: MS-00000458

CIS Controls V7.0:

- **Control 7: Email and Web Browser Protections:** -- More >

CIS Critical Security Controls V8.0:

- **Control 9: Email and Web Browser Protections:** -- More >

Back to Summary

18.10.36 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.

18.10.37 Location and Sensors

This section contains settings for Locations and Sensors.

This Group Policy section is provided by the Group Policy template `Sensors.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.10.38 Maintenance Scheduler

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

This Group Policy section is provided by the Group Policy template `msched.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.10.39 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).

18.10.40 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).

18.10.41 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).

18.10.42 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).

18.10.43 Microsoft Defender Antivirus (formerly Windows Defender and Windows Defender Antivirus)

This section contains recommendations related to Microsoft Defender Antivirus.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note: This section was originally named *Windows Defender* but was renamed by Microsoft to *Windows Defender Antivirus* starting with the Microsoft Windows 10 Release 1703 Administrative Templates. It was renamed (again) to *Microsoft Defender Antivirus* starting with the Microsoft Windows 10 Release 2004 Administrative Templates.

18.10.43.1 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).

18.10.43.2 Device Control

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

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 11 Release 21H2 Administrative Templates (or newer).

18.10.43.3 Exclusions

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

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.10.43.4 Features

This section contains recommendations related to Features.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 11 Release 22H2 Administrative Templates v1.0 (or newer).

18.10.43.4.1 (L1) Ensure 'Enable EDR in block mode' is set to 'Enabled' Fail

Description:

This policy setting controls whether Microsoft Defender Antivirus Endpoint Detection and Response (EDR) is enabled in block mode (passive remediation).

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

Note: EDR in block mode is only available in Microsoft Defender for Endpoint Plan 2.

Note #2: This setting is available with Microsoft Defender Antivirus platform release v4.18.2202.X and newer.

Rationale:

When Microsoft Defender Antivirus is not the primary antivirus product and is running in passive mode, EDR in block mode provides added protection against malicious artifacts.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Features\Enable EDR in block mode
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 11 Release 24H2 Administrative Templates (or newer).

Impact:

If Microsoft Defender Antivirus is running EDR will be enabled in block mode. If the system does not have Microsoft Defender Antivirus installed and running, then this setting will have no effect.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** GRID: MS-00000598
- **URL:** https://learn.microsoft.com/en-us/defender-endpoint/edr-in-block-mode

CIS Controls V7.0:

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

CIS Critical Security Controls V8.0:

- **Control 10: Malware Defenses:** -- More >

Back to Summary

18.10.43.5 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).

18.10.43.6 Microsoft Defender Exploit Guard (formerly Windows Defender Exploit Guard)

This section contains Microsoft Defender Exploit Guard settings.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

Note: This section was originally named *Windows Defender Exploit Guard* but was renamed by Microsoft to *Microsoft Defender Exploit Guard* starting with the Microsoft Windows 10 Release 2004 Administrative Templates.

18.10.43.6.1 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).

18.10.43.6.2 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).

18.10.43.6.3 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).

18.10.43.7 MpEngine

This section contains recommendations for MpEngine.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 10 Release 1703 Administrative Templates (or newer).

18.10.43.7.1 (L1) Ensure 'Enable file hash computation feature' is set to 'Enabled' Fail

Description:

This setting determines whether hash values are computed for files scanned by Microsoft Defender.

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

Rationale:

When running an antivirus solution such as Microsoft Defender Antivirus, it is important to ensure that it is configured to monitor for suspicious and known malicious activity. File hashes are a reliable way of detecting changes to files, and can speed up the scan process by skipping files that have not changed since they were last scanned and determined to be safe. A changed file hash can also be cause for additional scrutiny.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\MpEngine\Enable file hash computation feature
```

Note: This Group Policy path 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:

This setting could cause performance degradation during initial deployment and for users where new executable content is frequently being created (such as software developers), or where applications are frequently installed or updated.

For more information on this setting, please visit Security baseline (FINAL): Windows 10 and Windows Server, version 2004 - Microsoft Tech Community - 1543631 .

Note: The impact of this setting should be monitored closely during deployment to ensure user and system performance impact is within acceptable limits.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** GRID: MS-00000469

CIS Controls V7.0:

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

CIS Critical Security Controls V8.0:

- **Control 10: Malware Defenses:** -- More >

Back to Summary

18.10.43.8 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).

18.10.43.9 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).

18.10.43.10 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).

18.10.43.10.1 (L1) Ensure 'Configure real-time protection and Security Intelligence Updates during OOBE' is set to 'Enabled' — Fail

Description:

This policy setting configures whether Real-time Protection and Security Intelligence Updates are enabled during the Out of Box experience (OOBE).

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

Rationale:

Critical Windows zero-day patch updates should be applied during OOBE to help mitigate against malicious attacks.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Real-Time Protection\Configure real-time protection and Security Intelligence Updates during OOBE
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 11 Release 24H2 Administrative Templates (or newer).

Impact:

None - this is the default behavior.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** GRID: MS-00000600
- **URL:** https://learn.microsoft.com/en-us/windows-hardware/customize/desktop/windows-updates-during-oobe-in-windows-11
- **URL:** https://techcommunity.microsoft.com/blog/microsoft-security-baselines/windows-11-version-24h2-security-baseline/4252801

CIS Controls V7.0:

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

CIS Critical Security Controls V8.0:

- **Control 10: Malware Defenses:** -- More
  >

Back to Summary

18.10.43.10.2 (L1) Ensure 'Scan all downloaded files and attachments' is set to 'Enabled' — Fail

Description:

This policy setting configures scanning for all downloaded files and attachments.

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

Rationale:

When running an antivirus solution such as Microsoft Defender Antivirus, it is important to ensure that it is configured to heuristically monitor in real-time for suspicious and known malicious activity.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Real-Time Protection\Scan all downloaded files and attachments
```

Note: This Group Policy path 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:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** https://learn.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-antivirus/configure-real-time-protection-microsoft-defender-antivirus
- **URL:** GRID: MS-00000470

CIS Controls V7.0:

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

CIS Critical Security Controls V8.0:

- **Control 10: Malware Defenses:** -- More
  >

Back to Summary

18.10.43.10.3 (L1) Ensure 'Turn off real-time protection' is set to 'Disabled' Fail

Description:

This policy setting configures real-time protection prompts for known malware detection.

Microsoft Defender Antivirus alerts you when malware or potentially unwanted software attempts to install itself or to run on your computer.

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

Rationale:

When running an antivirus solution such as Microsoft Defender Antivirus, it is important to ensure that it is configured to heuristically monitor in real-time for suspicious and known malicious activity.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Real-Time Protection\Turn off real-time protection
```

Note: This Group Policy path 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:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** https://learn.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-antivirus/configure-real-time-protection-microsoft-defender-antivirus
- **URL:** https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-protection-features-microsoft-defender-antivirus?view=o365-worldwide
- **URL:** GRID: MS-00000471

CIS Controls V7.0:

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

CIS Critical Security Controls V8.0:

- **Control 10: Malware Defenses:** -- More
  >

Back to Summary

18.10.43.11 Remediation

This section contains settings related to Remediation.

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).

18.10.43.11.1 Behavioral Network Blocks

This section contains settings related to Behavioral Network Blocks.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 11 Release 24H2 Administrative Templates (or newer).

18.10.43.11.1.1 Brute-Force Protection

This section contains settings related to Brute-Force Protection.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 11 Release 24H2 Administrative Templates (or newer).

18.10.43.11.1.1.2 (L1) Ensure 'Configure Remote Encryption Protection Mode' is set to 'Enabled: Audit' or higher

Fail

Description:

This policy setting configures the Brute-Force Protection feature in Microsoft Defender Antivirus. Brute-Force Protection can detect and block attempts to forcibly initiate sign-ins and sessions.

The recommended state for this setting is: `Enabled: Audit` . Configuring this setting to `Block` also conforms to the benchmark.

Note: Configuring the value to either `Default` or `Off` does **not** conform to this benchmark.

Note #2: This setting's name is duplicated in the *Remote Encryption Protection* section, but they configure two different behaviors.

Rationale:

This feature assists with mitigating brute force attempts by detecting and blocking unauthorized sign-ins and sessions.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Remediation\Behavioral Network Blocks\Brute-Force Protection\Configure Remote Encryption Protection Mode
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 11 Release 24H2 Administrative Templates (or newer).

Impact:

Legitimate sign-ins and sessions could be detected or blocked by this feature if too many failed attempts are detected.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** GRID: MS-00000602

CIS Controls V7.0:

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

CIS Critical Security Controls V8.0:

- **Control 10: Malware Defenses:** -- More >

Back to Summary

18.10.43.11.1.2 Remote Encryption Protection

This section contains settings related to Remote Encryption Protection.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 11 Release 24H2 Administrative Templates (or newer).

18.10.43.12 Reporting

This section contains settings related to Microsoft Defender Reporting.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.10.43.13 Scan

This section contains settings related to Microsoft Defender scanning.

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

18.10.43.13.1 (L1) Ensure 'Scan excluded files and directories during quick scans' is set to 'Enabled: 1' Fail

Description:

This policy setting manages whether or not Microsoft Defender Antivirus scans excluded files and directories when running a Quick Scan.

The recommended state for this setting is: `Enabled: 1`.

Rationale:

The Real-time Protection feature excludes some files and directories for contextual reasons. This setting ensures that these are scanned during a Quick Scan.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: 1`:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Scan\Scan excluded files and directories during quick scans
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 11 Release 24H2 Administrative Templates (or newer).

Impact:

A Quick Scan could take longer when including the contextually excluded files and directories.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** GRID: MS-00000604
- **URL:** https://learn.microsoft.com/en-us/defender-endpoint/schedule-antivirus-scans

CIS Controls V7.0:

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

CIS Critical Security Controls V8.0:

- **Control 10: Malware Defenses:** -- More
  >

Back to Summary

18.10.43.13.4 (L1) Ensure 'Trigger a quick scan after X days without any scans' is set to 'Enabled: 7'

Fail

Description:

This policy setting configures the number of days after the last scan (of any type) before an aggressive Quick Scan is automatically triggered.

The recommended state for this setting is: `Enabled: 7` days.

Rationale:

Antivirus scans should be performed on a regular basis so that malicious software can be detected and remediated before malicious activity occurs.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: 7` days:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Scan\Trigger a quick scan after X days without any scans
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 11 Release 24H2 Administrative Templates (or newer).

Impact:

This setting should have no adverse effect on the system.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** GRID: MS-00000605

CIS Controls V7.0:

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

CIS Critical Security Controls V8.0:

- **Control 10: Malware Defenses:** -- More
  >

Back to Summary

18.10.43.13.5 (L1) Ensure 'Turn on e-mail scanning' is set to 'Enabled'

Fail

Description:

This policy setting configures e-mail scanning. When e-mail scanning is enabled, the engine will parse the mailbox and mail files, according to their specific format, in order to analyze the mail bodies and attachments. Several e-mail formats are currently supported, for example: pst (Outlook), dbx, mbx, mime (Outlook Express), binhex (Mac).

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

Rationale:

Incoming e-mails should be scanned by an antivirus solution such as Microsoft Defender Antivirus, as email attachments are a commonly used attack vector to infiltrate computers with malicious software.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Scan\Turn on e-mail scanning
```

Note: This Group Policy path 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 Microsoft Defender Antivirus will be enabled.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-advanced-scan-types-microsoft-defender-antivirus?view=o365-worldwide#settings-and-locations
- **URL:** GRID: MS-00000477

CIS Controls V7.0:

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

CIS Critical Security Controls V8.0:

- **Control 10: Malware Defenses:** -- More
  >

Back to Summary

18.10.43.14 Security Intelligence Updates (formerly Signature Updates)

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

This Group Policy section is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

Note: This section was initially named *Signature Updates* but was renamed by Microsoft to *Security Intelligence Updates* starting with the Microsoft Windows 10 Release 1903 Administrative Templates.

18.10.43.15 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).

18.10.43.16 (L1) Ensure 'Configure detection for potentially unwanted applications' is set to 'Enabled: Block'

Fail

Description:

This policy setting controls detection and action for Potentially Unwanted Applications (PUA), which are sneaky unwanted application bundlers or their bundled applications, that can deliver adware or malware.

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

For more information, see this link: Block potentially unwanted applications with Microsoft Defender Antivirus | Microsoft Docs

Rationale:

Potentially unwanted applications can increase the risk of your network being infected with malware, cause malware infections to be harder to identify, and can waste IT resources in cleaning up the applications. They should be blocked from installation.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Configure detection for potentially unwanted applications
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 10 Release 1809 & Server 2019 Administrative Templates (or newer).

Impact:

Applications that are identified by Microsoft as PUA will be blocked at download and install time.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/detect-block-potentially-unwanted-apps-microsoft-defender-antivirus?view=o365-worldwide
- **URL:** GRID: MS-00000462

CIS Controls V7.0:

- **Control 2: Inventory and Control of Software Assets:** -- More
- **Control 8: Malware Defenses:** -- More
  >

CIS Critical Security Controls V8.0:

- **Control 10: Malware Defenses:** -- More
  >

Back to Summary

18.10.43.17 (L1) Ensure 'Control whether exclusions are visible to local users' is set to 'Enabled'

Fail

Description:

This policy setting controls whether Microsoft Defender Antivirus exclusions are visible to local users on the system.

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

Rationale:

Only administrators should be able to view and manage Microsoft Defender Antivirus exclusions.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Control whether exclusions are visible to local users
```

Note: This Group Policy path is provided by the Group Policy template `WindowsDefender.admx/adml` that is included with the Microsoft Windows 11 Release 24H2 Administrative Templates (or newer).

Impact:

Local users will not be able to view Microsoft Defender Antivirus exclusions.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** GRID: MS-00000597

CIS Controls V7.0:

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

CIS Critical Security Controls V8.0:

- **Control 10: Malware Defenses:** -- More >

Back to Summary

18.10.44 Microsoft Defender Application Guard (formerly Windows Defender Application Guard)

This section contains settings related to Microsoft Defender Application Guard.

This Group Policy section is provided by the Group Policy template `AppHVSI.admx/adml` that is included with the Microsoft Windows 10 Release 1703 Administrative Templates (or newer).

Note: This section was originally named *Windows Defender Application Guard* but was renamed by Microsoft to *Microsoft Defender Application Guard* starting with the Microsoft Windows 10 Release 2004 Administrative Templates.

18.10.45 Microsoft Defender Exploit Guard (formerly Windows Defender Exploit Guard)

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

This Group Policy section is provided by the Group Policy template `ExploitGuard.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

Note: This section was originally named *Windows Defender Exploit Guard* , but was renamed by Microsoft to *Microsoft Defender Exploit Guard* starting with the Microsoft Windows 10 Release 2004 Administrative Templates.

18.10.46 Microsoft Edge

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

This Group Policy section is provided by the Group Policy template `MicrosoftEdge.admx/adml` that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

CIS publishes security guidance for Microsoft Edge in a separate benchmark from Windows. Additional details can be found in the CIS Microsoft Web Browser Benchmarks Community .

18.10.47 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).

18.10.48 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).

18.10.49 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.

18.10.50 News and interests

This section contains recommendations related to News and interests.

This Group Policy section is provided by the Group Policy template `Feeds.admx/adml` that is included with the Microsoft Windows 10 Release 21H1 Administrative Templates (or newer).

18.10.51 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.

18.10.52 Online Assistance

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

This Group Policy section is provided by the Group Policy template `HelpAndSupport.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.53 OOBE

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

This Group Policy section is provided by the Group Policy template `OOBE.admx/adml` that is included with the Microsoft Windows 10 Release 1809 and Server 2019 Administrative Templates (or newer).

18.10.54 Portable Operating System

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

This Group Policy section is provided by the Group Policy template `ExternalBoot.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.10.55 Presentation Settings

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

This Group Policy section is provided by the Group Policy template `MobilePCPresentationSettings.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.56 Push To Install

This section contains recommendations related to the Push To Install service.

This Group Policy section is provided by the Group Policy template `PushToInstall.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

18.10.57 Remote Desktop Services (formerly Terminal Services)

This section contains recommendations related to Remote Desktop Services.

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note: This section was initially named *Terminal Services* but was renamed by Microsoft to *Remote Desktop Services* starting with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates.

18.10.57.1 RD Licensing (formerly TS Licensing)

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

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note: This section was initially named *TS Licensing* but was renamed by Microsoft to *RD Licensing* starting with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates.

18.10.57.2 Remote Desktop Connection Client

This section contains recommendations for the Remote Desktop Connection Client.

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.57.2.1 RemoteFX USB Device Redirection

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

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.10.57.3 Remote Desktop Session Host (formerly Terminal Server)

This section contains recommendations for the Remote Desktop Session Host.

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note: This section was initially named *Terminal Server* but was renamed by Microsoft to *Remote Desktop Session Host* starting with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates.

18.10.57.3.1 Application Compatibility

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

This Group Policy section is provided by the Group Policy template `TerminalServer-Server.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.10.57.3.2 Connections

This section contains recommendations for Connections to the Remote Desktop Session Host.

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.57.3.3 Device and Resource Redirection

This section contains recommendations related to Remote Desktop Session Host Device and Resource Redirection.

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.57.3.4 Licensing

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

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.57.3.5 Printer Redirection

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

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.57.3.6 Profiles

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

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.57.3.7 RD Connection Broker (formerly TS Connection Broker)

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

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note: This section was initially named *TS Connection Broker* but was renamed by Microsoft to *RD Connection Broker* starting with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates.

18.10.57.3.8 Remote Session Environment

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

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.57.3.9 Security

This section contains recommendations related to Remote Desktop Session Host Security.

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.57.3.10 Session Time Limits

This section contains recommendations related to Remote Desktop Session Host Session Time Limits.

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.57.3.11 Temporary folders

This section contains recommendations related to Remote Desktop Session Host Session Temporary folders.

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.57.3.11.1 (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:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** GRID: MS-00000505

CIS Controls V7.0:

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

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More >

Back to Summary

18.10.58 RSS Feeds

This section contains recommendations related to RSS feeds.

This Group Policy section is provided by the Group Policy template `InetRes.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.59 Search

This section contains recommendations for Search settings.

This Group Policy section is provided by the Group Policy template `Search.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.59.1 OCR

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

This Group Policy section is provided by the Group Policy template `SearchOCR.admx/adml` that is only included with the Microsoft Windows 7 & Server 2008 R2 through the Windows 10 Release 1511 Administrative Templates.

18.10.60 Security Center

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

This Group Policy section is provided by the Group Policy template `SecurityCenter.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.61 Shutdown Options

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

This Group Policy section is provided by the Group Policy template `WinInit.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.62 Smart Card

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

This Group Policy section is provided by the Group Policy template `SmartCard.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.63 Software Protection Platform

This section contains recommendations related to the Software Protection Platform.

This Group Policy section is provided by the Group Policy template `AVSValidationGP.admx/adml` that is included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates (or newer).

18.10.64 Sound Recorder

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

This Group Policy section is provided by the Group Policy template `SoundRec.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.65 Speech

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

This Group Policy section is provided by the Group Policy template `Speech.admx/adml` that is included with the Microsoft Windows 10 Release 1703 Administrative Templates (or newer).

18.10.66 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).

18.10.66.2 (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 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:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** GRID: MS-00000517

CIS Controls V7.0:

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

CIS Critical Security Controls V8.0:

- **Control 7: Continuous Vulnerability Management:** -- More >

Back to Summary

18.10.67 Sync your settings

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

This Group Policy section is provided by the Group Policy template `SettingSync.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.10.68 Tablet PC

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

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.69 Task Scheduler

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

This Group Policy section is provided by the Group Policy template `TaskScheduler.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.70 Tenant Restrictions

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

This Group Policy section is provided by the Group Policy template `TenantRestrictions.admx/adml` that is included with the Microsoft Windows 11 Release 21H2 Administrative Templates (or newer).

18.10.71 Text Input

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

This Group Policy section is provided by the Group Policy template `TextInput.admx/adml` that is only included with the Microsoft Windows 10 RTM (Release 1507) Administrative Templates and Microsoft Windows 10 Release 1511 Administrative Templates.

18.10.72 Widgets

This section contains recommendations related to Widgets.

This Group Policy section is provided by the Group Policy template `NewsAndInterests.admx/adml` that is included with the Microsoft Windows 11 Release 21H2 Administrative Templates (or newer).

18.10.73 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.

18.10.74 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.

18.10.75 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.

18.10.76 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).

18.10.76.1 Enhanced Phishing Protection

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

This Group Policy section is provided by the Group Policy template `WebThreatDefense.admx/adml` that is included with the Microsoft Windows 11 Release 22H2 Administrative Templates v1.0 (or newer).

18.10.76.2 Explorer

This section contains recommendations for Explorer-related Windows Defender SmartScreen settings.

The Group Policy settings contained within this section are provided by the Group Policy template `WindowsExplorer.admx/adml` that is included with the Microsoft Windows 10 Release 1703 Administrative Templates (or newer).

18.10.77 Windows Error Reporting

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

This Group Policy section is provided by the Group Policy template `ErrorReporting.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.78 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).

18.10.79 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.

18.10.80 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).

18.10.81 Windows Installer

This section contains recommendations related to Windows Installer.

This Group Policy section is provided by the Group Policy template `MSI.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.82 Windows Logon Options

This section contains recommendations related to Windows Logon Options.

This Group Policy section is provided by the Group Policy template `WinLogon.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.83 Windows Media Digital Rights Management

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

This Group Policy section is provided by the Group Policy template `WindowsMediaDRM.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.84 Windows Media Player

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

This Group Policy section is provided by the Group Policy template `WindowsMediaPlayer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.85 Windows Messenger

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

This Group Policy section is provided by the Group Policy template `WindowsMessenger.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.86 Windows Mobility Center

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

This Group Policy section is provided by the Group Policy template `MobilePCMobilityCenter.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.87 Windows PowerShell

This section contains recommendations related to Windows PowerShell.

This Group Policy section is provided by the Group Policy template `PowerShellExecutionPolicy.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

18.10.88 Windows Reliability Analysis

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

This Group Policy section is provided by the Group Policy template `RacWmiProv.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

18.10.89 Windows Remote Management (WinRM)

This section contains recommendations related to Windows Remote Management (WinRM).

This Group Policy section is provided by the Group Policy template `WindowsRemoteManagement.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.89.1 WinRM Client

This section contains recommendations related to the Windows Remote Management (WinRM) client.

This Group Policy section is provided by the Group Policy template `WindowsRemoteManagement.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.89.2 WinRM Service

This section contains recommendations related to the Windows Remote Management (WinRM) service.

This Group Policy section is provided by the Group Policy template `WindowsRemoteManagement.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.90 Windows Remote Shell

This section contains settings related to Windows Remote Shell (WinRS).

This Group Policy section is provided by the Group Policy template `WindowsRemoteShell.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.91 Windows Sandbox

This section contains recommendations related to Windows Sandbox.

This Group Policy section is provided by the Group Policy template `WindowsSandbox.admx/adml` that is included with the Microsoft Windows 11 Release 21H2 Administrative Templates (or newer).

18.10.92 Windows Security (formerly Windows Defender Security Center)

This section contains recommendations related to the Windows Security Center console settings.

This Group Policy section is provided by the Group Policy template `WindowsDefenderSecurityCenter.admx/adml` that is included with the Microsoft Windows 10 Release 1709 Administrative Templates (or newer).

Note: This section was originally named *Windows Defender Security Center* but was renamed by Microsoft to *Windows Security* starting with the Microsoft Windows 10 Release 1809 & Server 2019 Administrative Templates.

18.10.92.1 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).

18.10.92.2 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).

18.10.93 Windows Update

This section contains recommendations related to Windows Update.

This Group Policy section is provided by the Group Policy template `WindowsUpdate.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

18.10.93.1 Legacy Policies

This section contains recommendations related to legacy Windows Update policies.

This Group Policy section is provided by the Group Policy template `WindowsUpdate.admx/adml` that is included with the Microsoft Windows 11 Release 21H2 Administrative Templates (or newer).

18.10.93.1.1 (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\Legacy Policies\No auto-restart with logged on users for scheduled automatic updates installations
```

Note: This Group Policy path is provided by the Group Policy template `WindowsUpdate.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note #2: In older Microsoft Windows Administrative Templates, this setting was initially named *No auto-restart for scheduled Automatic Updates installations* , but it was renamed starting with the Windows 7 & Server 2008 R2 Administrative Templates.

Impact:

None - this is the default behavior.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** GRID: MS-00000549

CIS Controls V7.0:

- **Control 3: Continuous Vulnerability Management:** -- More >

CIS Critical Security Controls V8.0:

- **Control 7: Continuous Vulnerability Management:** -- More >

Back to Summary

18.10.93.2 Manage end user experience

This section contains recommendations related to managing Windows Update end user experience.

This Group Policy section is provided by the Group Policy template `WindowsUpdate.admx/adml` that is included with the Microsoft Windows 11 Release 21H2 Administrative Templates (or newer).

18.10.93.2.3 (L1) Ensure 'Remove access to “Pause updates” feature' is set to 'Enabled' Fail

Description:

This policy removes access to "Pause updates" feature.

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

Rationale:

In order to ensure security and system updates are applied, system administrators should control when updates are applied to systems.

Remediation:

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

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update\Manage end user experience\Remove access to “Pause updates” feature
```

Note: This Group Policy path may not exist by default. It is provided by the Group Policy template `WindowsUpdate.admx/adml` that is included with the Microsoft Windows 10 Release 1809 & Server 2019 Administrative Templates (or newer).

Impact:

Users will not be able to select the "Pause updates" option in Windows Update to prevent updates from being installed on a system.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** GRID: MS-00000571

CIS Controls V7.0:

- **Control 3: Continuous Vulnerability Management:** -- More >

CIS Critical Security Controls V8.0:

- **Control 7: Continuous Vulnerability Management:** -- More >

Back to Summary

18.10.93.3 Manage updates offered from Windows Server Update Service

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

This Group Policy section is provided by the Group Policy template `WindowsUpdate.admx/adml` that is included with the Microsoft Windows 11 Release 21H2 Administrative Templates (or newer).

18.10.93.4 Manage updates offered from Windows Update (formerly Defer Windows Updates and Windows Update for Business)

This section contains recommendations related to managing which updates are offered from Windows Update, and when.

This Group Policy section is provided by the Group Policy template `WindowsUpdate.admx/adml` that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

Note: This section was initially named *Defer Windows Updates* but was renamed by Microsoft to *Windows Update for Business* starting with the Microsoft Windows 10 Release 1709 Administrative Templates. It was renamed (again) to *Manage updates offered from Windows Update* starting with the Microsoft Windows 11 Release 21H2 Administrative Templates.

18.10.93.4.2 (L1) Ensure 'Select when Preview Builds and Feature Updates are received' is set to 'Enabled: 180 or more days' Fail

Description:

This policy setting determines when Preview Build or Feature Updates are received.

Defer Updates This enables devices to defer taking the next Feature Update available to your channel for up to 14 days for all the pre-release channels and up to 365 days for the Semi-Annual Channel. Or, if the device is updating from the Semi-Annual Channel, a version for the device to move to and/or stay on until the policy is updated or the device reaches end of service can be specified. Note: If you set both policies, the version specified will take precedence and the deferrals will not be in effect. Please see the Windows Release Information page for OS version information.

Pause Updates To prevent Feature Updates from being received on their scheduled time, you can temporarily pause Feature Updates. The pause will remain in effect for 35 days from the specified start date or until the field is cleared (Quality Updates will still be offered).

Note: If the "Allow Diagnostic Data" (formerly "Allow Telemetry") policy is set to 0, this policy will have no effect.

Note #2: Starting with Windows 10 R1607, Microsoft introduced a new Windows Update (WU) client behavior called **Dual Scan** , with an eye to cloud-based update management. In some cases, this Dual Scan feature can interfere with Windows Updates from Windows Server Update Services (WSUS) and/or manual WU updates. If you are using WSUS in your environment, you may need to set the above setting to `Not Configured`*or* configure the setting *Do not allow update deferral policies to cause scans against Windows Update* (added in the Windows 10 Release 1709 Administrative Templates) in order to prevent the Dual Scan feature from interfering. More information on Dual Scan is available at these links:

- Demystifying “Dual Scan” – WSUS Product Team Blog
- Improving Dual Scan on 1607 – WSUS Product Team Blog

Note #3: Prior to Windows 10 R1703, values above 180 days are not recognized by the OS. Starting with Windows 10 R1703, the maximum number of days you can defer is 365 days.

Rationale:

In a production environment, it is preferred to only use software and features that are publicly available, after they have gone through rigorous testing in beta.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled: 180 or more days`:

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update\Manage updates offered from Windows Update\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 they are publicly released to general public by Microsoft.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** GRID: MS-00000554

CIS Controls V7.0:

- **Control 2: Inventory and Control of Software Assets:** -- More >

CIS Critical Security Controls V8.0:

- **Control 7: Continuous Vulnerability Management:** -- More >

Back to Summary

18.10.93.4.3 (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 Diagnostic Data" (formerly "Allow Telemetry") policy is set to 0, this policy will have no effect.

Note #2: Starting with Windows 10 R1607, Microsoft introduced a new Windows Update (WU) client behavior called **Dual Scan** , with an eye to cloud-based update management. In some cases, this Dual Scan feature can interfere with Windows Updates from Windows Server Update Services (WSUS) and/or manual WU updates. If you are using WSUS in your environment, you may need to set the above setting to `Not Configured`*or* configure the setting *Do not allow update deferral policies to cause scans against Windows Update* (added in the Windows 10 Release 1709 Administrative Templates) in order to prevent the Dual Scan feature from interfering. More information on Dual Scan is available at these links:

- Demystifying “Dual Scan” – WSUS Product Team Blog
- Improving Dual Scan on 1607 – WSUS Product Team Blog

Rationale:

Quality Updates can contain important bug fixes and/or security patches, and should be installed as soon as possible.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled:0 days` :

```
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update\Manage updates offered from Windows Update\Select when Quality Updates are received
```

Note: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).

Impact:

None - this is the default behavior.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** GRID: MS-00000555

CIS Controls V7.0:

- **Control 3: Continuous Vulnerability Management:** -- More >

CIS Critical Security Controls V8.0:

- **Control 7: Continuous Vulnerability Management:** -- More >

Back to Summary

19 Administrative Templates (User)

This section contains recommendations for user-based settings that are present within the Administrative Templates (ADMX) for domain-joined user configurations. The settings included in this section are intended to harden the system and are applied on a per-user basis, reflected to each domain-joined interactive user's **HKEY_CURRENT_USER (HKCU)** registry hive. Each interactively logged-on user has its own **HKCU** hive, which is a context-sensitive, per-user, symbolic link to a subkey under **HKEY_USERS (HKU)** , where the user's Security Identifier (SID) is the subkey name (Ex: `HKU\S-1-5-21-123123123-123123123-1231231231-12312`). User SIDs for this scenario always begin with `S-1-5-21-*` for active directory domain-joined accounts.

The group policy engine applies user configuration settings to the **HKU***SID*** subkeys for interactive logons, including local console logons, remote desktop logons, and RunAs logons. User configuration settings are not applied to the built-in **NT AUTHORITY** service accounts (System, Network Service, and Local Service), nor to any other service logons. User configuration settings configured through active directory domain group policy objects (GPO) are not applied to local user accounts.

When validating user configuration settings for compliance, each recommendation should be checked against all currently-logged-on interactive users' hives:

- Audit all **HKEY_USERS** subkeys with key names beginning with `S-1-5-21-*` and do not end with **_Classes** .
- Do not audit subkeys named `.DEFAULT` , `S-1-5-18` , `S-1-5-19` , or `S-1-5-20` .
- Do not audit any **NT SERVICE** SIDs (`S-1-5-80-`).
- Do not load the hives of users that are not currently logged on (**NTUSER.DAT** files) as part of compliance verification.

A user configuration setting is considered in compliance if the correct configuration is found in all applicable user hives as described above. If there are multiple users logged on and the setting is correctly configured in some but not all the applicable user hives, the recommendation is not in full compliance.

If a system has no actively logged-on users, the recommendations in this section are not considered out of compliance. User accounts (`S-1-5-21-*`) that only log on as a service (service accounts), will not receive user configuration settings to its **HKU** registry hive since the group policy engine will not write to this type of account. Compliance findings for these accounts should be ignored.

Why CIS recommends not auditing all the **HKU** subkeys:

- Group policy applies user configuration settings only to **HKU** subkey hives associated with interactive logons. It never applies the settings to the **NT AUTHORITY** service account subkeys (`S-1-5-18` , `S-1-5-19` , `S-1-5-20` , or `.DEFAULT`) or the **NT SERVICE** subkeys (`S-1-5-80-*`).
  - The `HKU\S-1-5-18` is a symbolic link to **HKU\.DEFAULT** , so the key content is identical.
- The **HKU***SID***_Classes** subkey represents the subkey of the corresponding **HKU***SID***\SOFTWARE\Classes** , to which they are symbolically linked.

Why CIS recommends not loading the **NTUSER.DAT** file(s) to audit the hives of users that are not currently logged on:

- Unnecessary false positives of old user profiles that were last loaded before the new or updated GPO containing the user configuration settings were applied.
  - These accounts would be found out of compliance, with no supportable way to bring them into compliance other than the user logging on or deleting the old profiles.
  - These account settings being out of compliance should not cause issues if the user never logs on; and if they do, a group policy update should bring them into compliance.
- Risk of system issues if the user logs on while the scanning tool has the hive loaded, and then also when the scanning tool unloads the hive.
- Significant performance hit.

User configuration settings configured through active directory domain GPOs are not applied to local user accounts. Since these accounts begin with the SID `S-1-5-21-*` , a failure may occur with CIS-CAT and other third-party assessment tools.

To mitigate this, user recommendations (Section 19 of this benchmark) should be applied to local accounts separately. If this is not a concern for the organization, local accounts should be ignored. The above is also true when an account with a `S-1-5-21-*` SID logs on as a service.

19.1 Control Panel

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

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.2 Desktop

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

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.3 Network

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

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.4 Shared Folders

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

This Group Policy section is provided by the Group Policy template `SharedFolders.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.5 Start Menu and Taskbar

This section contains recommendations for Start Menu and Taskbar settings.

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.5.1 Notifications

This section contains recommendations for Notification settings.

This Group Policy section is provided by the Group Policy template `WPN.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

19.6 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 Account Notifications

This section contains recommendations for Account Notifications settings.

This Group Policy section is provided by the Group Policy template `AccountNotifications.admx/adml` that is included with the Microsoft Windows 11 Release 22H2 Administrative Templates v3.0 (or newer).

19.7.2 Add features to Windows 8 / 8.1 / 10 (formerly Windows Anytime Upgrade)

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

This Group Policy section is provided by the Group Policy template `WindowsAnytimeUpgrade.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

Note: This section was initially named *Windows Anytime Upgrade* but was renamed by Microsoft to *Add features to Windows x* starting with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

19.7.3 App runtime

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

This Group Policy section is provided by the Group Policy template `AppXRuntime.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

19.7.4 Application Compatibility

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

This Group Policy section is provided by the Group Policy template `AppCompat.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.5 Attachment Manager

This section contains recommendations related to Attachment Manager.

This Group Policy section is provided by the Group Policy template `AttachmentManager.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.5.2 (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:
Show Assessment Evidence

Show Rule Result XML

References:

- **URL:** GRID: MS-00000560

CIS Controls V7.0:

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

CIS Critical Security Controls V8.0:

- **Control 10: Malware Defenses:** -- More >

Back to Summary

19.7.6 AutoPlay Policies

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

This Group Policy section is provided by the Group Policy template `AutoPlay.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.7 Calculator

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

This Group Policy section is provided by the Group Policy template `Programs.admx/adml` that is included with the Microsoft Windows 10 Release 2004 Administrative Templates (or newer).

19.7.8 Cloud Content

This section contains recommendations for Cloud Content.

This Group Policy section is provided by the Group Policy template `CloudContent.admx/adml` that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

19.7.9 Credential User Interface

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

This Group Policy section is provided by the Group Policy template `CredUI.admx/adml` that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

19.7.10 Data Collection and Preview Builds

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

This Group Policy section is provided by the Group Policy template `DataCollection.admx/adml` that is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

19.7.11 Desktop Gadgets

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

This Group Policy section is provided by the Group Policy template `Sidebar.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

19.7.12 Desktop Window Manager

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

This Group Policy section is provided by the Group Policy template `DWM.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.13 Digital Locker

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

This Group Policy section is provided by the Group Policy template `DigitalLocker.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.14 Edge UI

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

This Group Policy section is provided by the Group Policy template `EdgeUI.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

19.7.15 File Explorer (formerly Windows Explorer)

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

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note: This section was initially named *Windows Explorer* but was renamed by Microsoft to *File Explorer* starting with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates.

19.7.16 File Revocation

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

This Group Policy section is provided by the Group Policy template `FileRevocation.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

19.7.17 IME

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

This Group Policy section is provided by the Group Policy template `EAIME.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

19.7.18 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 Multitasking

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

This Group Policy section is provided by the Group Policy template `Multitasking.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.25 NetMeeting

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

This Group Policy section is provided by the Group Policy template `Conf.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.26 Network Sharing

This section contains recommendations related to Network Sharing.

This Group Policy section is provided by the Group Policy template `Sharing.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.27 OOBE

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

This Group Policy section is provided by the Group Policy template `OOBE.admx/adml` that is included with the Microsoft Windows 10 Release 1809 and Server 2019 Administrative Templates (or newer).

19.7.28 Presentation Settings

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

This Group Policy section is provided by the Group Policy template `MobilePCPresentationSettings.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.29 Remote Desktop Services (formerly Terminal Services)

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

This Group Policy section is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Note: This section was initially named *Terminal Services* but was renamed by Microsoft to *Remote Desktop Services* starting with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates.

19.7.30 RSS Feeds

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

This Group Policy section is provided by the Group Policy template `InetRes.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.31 Search

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

This Group Policy section is provided by the Group Policy template `Search.admx/adml` that is included with the Microsoft Windows 7 & Server 2008 R2 Administrative Templates (or newer).

19.7.32 Snipping Tool

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

This Group Policy section is provided by the Group Policy template `Programs.admx/adml` that is included with the Microsoft Windows 11 Release 23H2 v2.0 Administrative Templates (or newer).

19.7.33 Sound Recorder

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

This Group Policy section is provided by the Group Policy template `SoundRec.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.34 Store

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

This Group Policy section is provided by the Group Policy template `WinStoreUI.admx/adml` that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates and Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates, or by the Group Policy template `WindowsStore.admx/adml` that is included with the Microsoft Windows 10 Release 1511 Administrative Templates (or newer).

19.7.35 Tablet PC

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

This Group Policy section is provided by the Group Policy template `Windows.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.36 Task Scheduler

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

This Group Policy section is provided by the Group Policy template `TaskScheduler.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.37 Windows AI

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

This Group Policy section is provided by the Group Policy template `WindowsCopilot.admx/adml` that is included with the Microsoft Windows 11 Release 24H2 Administrative Templates (or newer).

19.7.38 Windows Calendar

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

This Group Policy section is provided by the Group Policy template `WinCal.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.39 Windows Color System

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

This Group Policy section is provided by the Group Policy template `WindowsColorSystem.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.40 Windows Copilot

This section contains recommendations for Windows Copilot settings.

This Group Policy section is provided by the Group Policy template `WindowsCopilot.admx/adml` that is included with the Microsoft Windows 11 Release 23H2 Administrative Templates (or newer).

19.7.41 Windows Defender SmartScreen

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

This Group Policy section is provided by the Group Policy template `SmartScreen.admx/adml` that is included with the Microsoft Windows 10 Release 1703 Administrative Templates (or newer).

19.7.42 Windows Error Reporting

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

This Group Policy section is provided by the Group Policy template `ErrorReporting.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.43 Windows Hello for Business (formerly Microsoft Passport for Work)

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

This Group Policy section is provided by the Group Policy template `Passport.admx/adml` that is included with the Microsoft Windows 10 RTM (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.

19.7.44 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.

19.7.45 Windows Logon Options

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

This Group Policy section is provided by the Group Policy template `WinLogon.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.46 Windows Media Player

This section contains recommendations related to Windows Media Player.

This Group Policy section is provided by the Group Policy template `WindowsMediaPlayer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.46.1 Networking

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

This Group Policy section is provided by the Group Policy template `WindowsMediaPlayer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

19.7.46.2 Playback

This section contains recommendations related to Windows Media Player playback.

This Group Policy section is provided by the Group Policy template `WindowsMediaPlayer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

⇧